Scientific Journal of Electronical & Cyber Defence
Vol. 10, No. 4, Winter 2023, Serial No. 40

Compensating GPS Signal Deception Error by Using Wavelet Transform Based on PSO Algorithm in Receiver Acquisition Section

R. Soleimani Majd, S. Tohidi, S. M. R. Musavi Mirkalaei*

* Professor, Faculty of Electrical Engineering, Iran University of Science and Technology, Tehran, Iran

(Received: 30/11/2021, Accepted: 27/02/2022)

ABSTRACT

The spoofing attack is one of the most serious interferences in the Global Positioning System (GPS). By propagating a signal structurally similar to the original GPS signal, the spoofers try to influence the function of different parts of the receiver and force it to make a wrong positioning. This study focus on the acquisition stage. During the acquisition process, GPS receivers estimate the values of Doppler frequency and Pseudo Random Noise (PRN) code phase of the received signal, which are necessary for tracking the GPS satellite signals. One of the effects of the spoofing signal in the acquisition unit of the receiver is to increase the interactions in the Quadrate correlation taps (Q-correlation tap). In 2018, adding a denoising unit on the Q-correlation tap in the acquisition stage to reduce the interactions mentioned above was presented as a spoofing mitigation method. In this paper, the mentioned method is placed as the primary basis of the work. Here, by using powerful methods of evolutionary computing, the denoising unit added in the Q-correlation tap is tried to be optimally adjusted to mitigate the spoofing attack. Specifically, to achieve a more efficient denoising method for spoofing mitigation, the Particle Swarm Optimization (PSO) algorithm is proposed to determine the critical parameters of the Discrete Wavelet Transform (DWT) based on the Haar wavelet. In order to evaluate the proposed method, first, the noise reduction performance of the algorithm is measured on four benchmark signals, namely Blocks, Bumps, Heavy Sine, and Doppler. Then, compared to four traditional methods, namely, Rigrsure, Heursure, Sqtwolog, and Minimaxi, the developed de-nosing method outperformed the former methods by 47.3%, 38.4%, 47,3%, and 30%, respectively. Finally, the proposed algorithm was placed in the Q-correlation tap of the GPS receiver acquisition stage, and its performance in reducing the spoof effects was investigated. The results show that the proposed algorithm is 37.74% more efficient compared to the method that was considered the primary method.

Keywords: GPS Receiver, Spoofing Attack, Wavelet Transform, Particle Swarm Optimization, Noise Reduction.

*Corresponding Author Email: M_mosavi@iust.ac.ir

نشریه علمی "پدافند الکترونیکی و سایبری"
سال دهم، شماره ۴، زمستان ۱۴۰۱، ص ۳۱- ۱۹

علمی – پژوهشی

جبران‌سازی خطای فریب سیگنال GPS با به‌کارگیری تبدیل موجک مبتنی بر الگوریتم PSO در بخش اکتساب گیرنده

رضا سلیمانی مجد[۱]، سمیرا توحیدی[۲]، سید محمدرضا موسوی میرکلائی[۳*]

۱- دانشجوی کارشناسی، ۲- دانشجوی دکترا، ۳- استاد، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران، ایران

(دریافت: ۱۴۰۰/۰۹/۰۹، پذیرش: ۱۴۰۰/۱۲/۰۸)

چکیده

فریب یکی از خطرناک‌ترین اختلالات در سامانه موقعیت‌یابی جهانی (GPS) است. فریبنده‌ها با ارسال سیگنالی که از نظر ساختاری کاملاً مشابه با سیگنال اصلی GPS است، تلاش می‌کنند عملکرد بخش‌های مختلف گیرنده را تحت تأثیر قرار دهند و آن را مجبور به موقعیت‌یابی اشتباه نمایند. این تحقیق بر مرحله اکتساب تمرکز دارد. در طی فرایند اکتساب، گیرنده‌های GPS مقادیر فرکانس داپلر و فاز کد شبه تصادفی (PRN) سیگنال دریافتی را که برای ردیابی سیگنال‌های ماهواره‌ای GPS ضروری هستند، تخمین می‌زنند. یکی از تأثیرات سیگنال فریب در بخش اکتساب گیرنده، افزایش فعل‌وانفعالات در شاخه‌های همبستگی متعامد (Q) است. در سال ۲۰۱۸، اضافه نمودن واحد نویززدایی بر روی شاخه همبستگی Q در مرحله اکتساب جهت کاهش فعل‌وانفعالات مذکور به‌عنوان یک روش مقابل با فریب ارائه گردید. در این مقاله، روش مذکور به‌عنوان پایه اصلی کار قرار گرفته است. در اینجا تلاش می‌شود با بهره‌گیری از روش‌های قدرتمند پردازش تکاملی، واحد نویززدایی اضافه‌شده در شاخه همبستگی Q با هدف مقابله با حمله فریب، به‌صورت بهینه تنظیم شود. به‌طور خاص، به‌منظور دستیابی به الگوریتم نویززدایی مناسب‌تر برای مقابله با اثرات فریب، به‌کارگیری الگوریتم تکاملی ازدحام ذرات (PSO) جهت تعیین پارامترهای کلیدی تبدیل موجک گسسته (DWT) بر پایه موجک مادر هار پیشنهاد شده است. به‌منظور ارزیابی روش پیشنهادی، ابتدا عملکرد الگوریتم را در کاهش نویز در چهار پایگاه داده الگو بلوک‌ها، برجستگی، سینوسی سنگین و داپلر سنجیده و با چهار روش نویززدایی معمول Rigrsure، Heursure، Sqtwolog و Minimaxi مقایسه شده است که به ترتیب ۴۷/۳، ۳۸/۴، ۴۷/۳ و ۳۰ درصد کاهش نویزی بیشتر حاصل شد. در نهایت، الگوریتم پیشنهادی در شاخه Q واحد اکتساب گیرنده GPS قرار داده شد و عملکرد آن در کاهش اثرات فریب بررسی گردید. نتایج حاصله، نشان‌دهنده برتری ۳۷/۷۴ درصدی الگوریتم پیشنهادی در مقایسه با روش پایه است.

کلیدواژه‌ها: گیرنده GPS، حمله فریب، تبدیل موجک، الگوریتم بهینه‌سازی ازدحام ذرات، نویززدایی

۱- مقدمه

در دهه‌های اخیر، سامانه GPS[1] به علت کارایی بالا و سادگی کار با آن در حوزه‌های گسترده‌ای مورداستفاده قرار گرفته است [۱]. این سامانه شامل ۲۴ ماهواره است که در شش طبقه مداری در حال چرخش هستند و در چنان آرایش فلکی قرار گرفته‌اند که در هر نقطه از زمین، حداقل چهار ماهواره در هر ساعتی از شبانه‌روز در دسترس باشند. ضعیف بودن توان سیگنال‌های دریافتی از ماهواره‌های ارسال‌کننده در سطح زمین و راحتی دسترسی به ساختار سیگنال آن، باعث می‌شود در برابر حملات ناوبری، همچون حمله فریب آسیب‌پذیر شود. به همین دلیل، مسئله امنیت این سامانه بسیار اهمیت پیدا کرده و موضوع موردبحث در بسیاری از پژوهش‌ها است [۲].

در حال حاضر، حمله فریب به‌عنوان خطرناک‌ترین خطای عمدی GPS شناخته می‌شود. هدف فریبنده آن است که GPS به‌جای راه‌حل ناوبری صحیح، راه‌حلی غلط تولید کند. سیگنال جعلی به‌گونه‌ای طراحی می‌شود که بر سیگنال اصلی غلبه کند و کنترل گیرنده را بر عهده گیرد. به دلیل پایین بودن سطح توان سیگنال اصلی، یک تداخل کم‌توان به‌راحتی می‌تواند یک گیرنده GPS تجاری را در شعاع چند کیلومتری فریب دهد. هر سامانه فریب‌دهنده بسته به نوع آن، محدوده اثر مشخصی دارد که می‌تواند تنها در آن محدوده، گیرنده را منحرف کند. این حمله و همچنین مقابله با آن می‌تواند در هر یک از سطوح گیرنده از جمله بخش پردازش‌های آنالوگ، اکتساب، ردیابی، استخراج شبه‌فاصله و معادلات ناوبری صورت گیرد.

ازآنجاکه سیگنال GPS توان کمی دارد، به‌شدت می‌تواند تحت تأثیر نویز و اغتشاشات محیط قرار گیرد. به همین دلیل، نویززدایی اهمیت بسیاری در فرایند اکتساب و مقابله با حمله فریب دارد. در این مقاله، هدف ارائه روش نویززدایی جدیدی

* رایانامه نویسنده مسئول: M_mosavi@iust.ac.ir

[1] Global Positioning System

ناشر: دانشگاه جامع امام حسین (ع)

برای کاهش حمله فریب است که نسبت به روش‌های متداول عملکرد بهتری داشته باشد. تابه‌حال، روش‌های فراوانی در حوزه نویززدایی ارائه شده‌اند که برای نمونه می‌توان به فیلترهای خطی پایین‌گذر[1] [۳]، فیلتر کالمن[2] [۴] و فیلترهای وفقی[3] مبتنی بر شبکه عصبی[4] [۵] اشاره نمود؛ اما هر یک از این روش‌ها معایبی دارند. برای مثال، درصورتی‌که نویز محیط در فرکانس‌های پایین موجود باشد، فیلتر خطی پایین‌گذر نمی‌تواند عملکرد مناسبی داشته باشد [۶]. همچنین، روش‌های مبتنی بر زمان، همچون فیلتر میانه[5] نمی‌توانند مدل مناسبی برای تخمین سیگنال باشند [۷]. به همین دلیل، استفاده از حوزه زمان یا مکان به‌تنهایی جهت نویززدایی نتایج مناسب و قابل‌قبولی را ارائه نمی‌دهد [۸]. در نتیجه، ابزار ریاضی تبدیل موجک[6] (WT) که دانوهو[7] و جانستون[8] آن را در مراجع [۹ و ۱۰] معرفی کردند، ابزار مناسبی برای این منظور است. چراکه تبدیل موجک با ترکیب دو حوزه زمان و فرکانس می‌تواند سیگنال را در هر دو حوزه تحلیل نماید. همچنین به دلیل سادگی محاسباتی، این روش در بسیاری از علوم مهندس موردتوجه قرار گرفت [۱۱ و ۱۲]. گرچه، عملکرد تبدیل موجک نیز خود به پارامترهای مهمی همچون نوع موجک، سطح تجزیه، روش آستانه‌گذاری و روش انتخاب حدود آستانه وابسته است. از میان این پارامترها، روش آستانه‌گذاری و انتخاب حدود آستانه، دو پارامتر کلیدی در میزان کارایی تبدیل موجک به شمار می‌روند. در سال‌های گذشته، تحقیقات فراوانی با تمرکز بر روی این دو پارامتر جهت بهبود عملکرد تبدیل موجک صورت گرفته است [۱۳ و ۱۴].

در ادامه این مقاله، ابتدا به‌صورت مختصر حمله فریب و روش‌های متداول شناسایی و مقابله با آن بررسی می‌شود. سپس در بخش سوم و چهارم به ترتیب، مفاهیم مرتبط با تبدیل موجک گسسته و روش بهینه‌سازی PSO[9] شرح داده می‌شوند. در بخش پنجم، به معرفی روش پیشنهادی پرداخته می‌شود. بخش ششم، نتایج شبیه‌سازی روش پیشنهادی، روی داده‌های واقعی استخراج‌شده از گیرنده GPS ارائه می‌شوند و در بخش پایانی، نتیجه‌گیری بیان خواهد شد.

۲- مروری بر روش‌های مقابله با فریب

به‌منظور حل مشکل حمله فریب در سامانه GPS مطالعات گسترده‌ای انجام شده است [۱۵-۱۷]. به‌طورکلی، مقابله با حمله فریب در دو مرحله اساسی انجام می‌گیرد. در مرحله نخست می‌بایست حضور سیگنال فریب را تشخیص دهد. در قدم بعد، جبران‌سازی یا کاهش اثر سیگنال فریب صورت می‌گیرد.

یکی از رویکردهای شناسایی فریب، مبتنی بر بررسی تغییرات توان سیگنال GPS است. در شرایط مناسب جوی، فقط تغییرات یونسفر و حرکت ماهواره‌ها، تغییرات هموار تدریجی در توان سیگنال دریافتی به وجود می‌آورند. هنگامی‌که توان بزرگ فریب‌دهنده، گیرنده GPS را گمراه می‌کند، در مقدار نسبت حامل به نویز[10] (C/N_o) اندازه‌گیری شده تغییرات ناگهانی به وجود می‌آید. گیرنده ضدفریب با نظارت بر میزان نسبت سیگنال به نویز[11] (SNR)، هر تغییر غیرمعمولی را به‌عنوان احتمال فریب در نظر می‌گیرد [۱۸]. البته برخی از فریب‌دهنده‌های پیشرفته‌تر می‌توانند بدون آن‌که تغییر زیادی در توان سیگنال جعلی ایجاد کنند، گیرنده را تحت تأثیر خود قرار دهند.

دسته دوم روش‌های آشکارسازی فریب، روش‌های مبتنی بر زمان ورود[12] (TOA) است. در این روش‌ها، نظارت بر زمان دریافت سیگنال به‌عنوان معیار تشخیص فریب استفاده می‌شود. در واقع، درصورتی‌که انتقال بیت داده ناوبری در لحظاتی از زمان با فاصله‌گذاری کمتر یا بیشتر از ۲۰ms ثانیه رخ دهد، می‌توان به وجود حمله فریب پی برد [۱۹].

از دیگر شیوه‌های مقابله با فریب می‌توان به روش نظارت بر کیفیت سیگنال[13] (SQM) و نظارت بر تابع همبستگی اشاره کرد. حمله فریب باعث عدم تقارن‌های ناهنجار می‌گردد. بر این اساس، روش‌های SQM با تشخیص قله‌های غیرطبیعی در سیگنال و یا افزایش قله‌های هم‌بستگی، وجود فریب را اعلام می‌کنند. در سال‌های اخیر روش‌های جدید و قدرتمندی در این حوزه معرفی شده است. ازجمله این روش‌ها، معیار Q-SQM [۲۰] می‌باشد. این معیار، انرژی قرار گرفته شده بر شاخه‌های همبستگی متعامد را تحت نظر گرفته و تغییرات آن را اعلان حضور فریب می‌داند. تابع تغییر شکل [۲۱] نیز معیار قدرتمند دیگری است که در سال ۲۰۲۲ معرفی شده است. این معیار بر تغییر شکل تابع همبستگی نظارت دارد. نویسندگان در مرجع [۲۲] تغییر شکل تابع همبستگی را با استفاده از گشتاور وزن‌دار مرتبه دوم آن، اندازه‌گیری نمودند. بهره‌گیری از تابع درستنمایی بیشینه احتمال[14] جهت سنجش میزان ناهنجاری در تابع همبستگی گیرنده GPS [۲۳ و ۲۴] نیز از جمله روش‌های ارائه‌شده در این حوزه است.

همچنین، در روش‌هایی دیگر از مقایسه اطلاعات سامانه GPS با دیگر سامانه‌های ناوبری همچون واحد اندازه‌گیری

[1] Linear Low-Pass Filter
[2] Kalman Filter
[3] Adaptive Filters
[4] Neural Network
[5] Median Filter
[6] Wavelet Transform
[7] Donoho
[8] Johnstone
[9] Particle Swarm Optimization
[10] Carrier to Noise
[11] Signal to Noise Ratio
[12] Time of Arrival
[13] Signal Quality Monitoring
[14] Likelihood Function

اینرسی[1] (IMU) [۲۵] و یا مقایسه اطلاعات دریافتی از گیرنده‌های متفاوت [۲۶ و ۲۷] و آنتن‌های متعدد که به آن پردازش فضایی نیز گفته می‌شود [۲۸]، برای تشخیص و مقابله با حمله فریب استفاده می‌شود. البته این روش‌ها عمدتاً پیچیدگی نرم‌افزاری یا سخت‌افزاری سامانه را افزایش می‌دهند. به همین دلیل، در بسیاری از کاربردها از روش‌های ساده‌تری همچون تخمین‌گرها استفاده می‌شود. به‌عنوان مثال، در مرجع [۲۹] برای گیرنده دو حالت عملکردی طراحی شده است. در شرایط عادی، گیرنده اطلاعات دریافتی خود را معتبر می‌داند و در حالت هوشیار[2] اطلاعاتی را که از تخمین‌گر پیش‌بینی‌کننده خود دریافت می‌کند، برای مکان‌یابی به کار می‌گیرد و زمانی که علائم هشدار از بین رفت، اطلاعات قبلی خود را استفاده می‌نماید. تخمین‌گر موقعیت در این سامانه به کمک فیلتر کالمن[3] و حسگرهای داخلی طراحی شده است. فیلتر کالمن در مقایسه با دیگر تخمین‌گرها می‌تواند تخمین دقیق‌تری را ارائه دهد.

دسته آخر روش‌های مقابله با فریب که در این قسمت موردبررسی قرار گرفته است، روش‌های مبتنی بر نویززدایی موجک است. نویسندگان مرجع [۳۰] نشان دادند که سیگنال فریب موجب افزایش انفعالات شاخه Q[4] در بخش اکتساب و ردیابی گیرنده GPS می‌شود و به‌کارگیری الگوریتم نویززدایی موجک را جهت کاهش اثرات فریب ارائه دادند.

اکنون در این مقاله، مقابله با فریب با روش نویززدایی موجک [۳۰] مبنای کار قرار گرفته شده است و تلاش شده است با به‌کارگیری بهینه‌سازی تکاملی پارامترهای کلیدی موجک به نحوی تعیین شود که منجر به افزایش قدرت نویززدایی و درنتیجه افزایش قدرت مقابله با فریب مذکور شود.

۳- تبدیل موجک

تبدیل موجک یکی از ابزارهای پرکاربرد حوزه پردازش سیگنال است که می‌تواند اطلاعات حوزه زمان و فرکانس را هم‌زمان استخراج نماید. در واقع، مشکل اساسی تبدیل فوریه که از دست رفتن اطلاعات حوزه زمان است [۳۱]، در این تبدیل وجود ندارد. قبل از ارائه موجک، تبدیل فوریه زمان کوتاه[5] (STFT) برای بهبود مشکل بیان‌شده در تبدیل فوریه استاندارد ابداع شد. در این تبدیل از مفهومی به نام پنجره استفاده شد که در آن، سیگنال در محدوده زمانی خاصی از لحاظ فرکانسی بررسی می‌شود؛ اما STFT نیز محدودیت‌هایی دارد. اول این‌که به علت اصل عدم قطعیت، قادر نیستیم در یک پنجره دقت هر دو بعد را افزایش دهیم و دیگر آن‌که اندازه پنجره در تمام حوزه زمان و فرکانس ثابت است. این در حالی است که برای برخی کاربردهای پردازش سیگنال، مجبور به بررسی دقیق‌تر سیگنال در محدوده خاصی می‌باشیم [۳۲].

در تبدیل موجک برای فائق آمدن بر مشکلات بیان‌شده از پنجره‌هایی با ابعاد متغیر استفاده شده است. بدین‌صورت می‌تواند هم‌زمان اطلاعات حوزه فرکانس و حوزه زمان را با دقت مطلوب استخراج کند.

تبدیل موجک به‌طور هم‌زمان دو عمل جابجایی و تغییر مقیاس را بر روی موجک پایه‌ای که موجک مادر نام دارد، اعمال می‌نماید. به عبارتی، در تبدیل موجک، موجک مادر با میزان کشیدگی و فشردگی متفاوت در طول سیگنال جابجا می‌شود. محاسبه میزان شباهت سیگنال با موجک مادر در هر موقعیت و برای مقیاس‌های متفاوت، مقدار ضرایب تبدیل موجک را نتیجه می‌دهد. بسته به این‌که جابجایی موجک مادر در طول سیگنال به‌صورت پیوسته یا گسسته انجام گیرد، تبدیل موجک به دو دسته‌ی تبدیل پیوسته و گسسته تقسیم می‌شود که در ادامه به‌اختصار شرح داده می‌شوند.

۳-۱- تبدیل موجک پیوسته

در تبدیل موجک برای به دست آوردن ضرایب موجک، تابع موجک مادر در طول سیگنال جابجا می‌شود و با عملگر کانولوشن[6]، میزان شباهت سیگنال با آن سطح از تابع سنجیده می‌شود. اگر پله‌های جابجایی تابع موجک مادر به‌صورت پیوسته تغییر کند، تبدیل موجک پیوسته اجرا شده است. رابطه (۱) تبدیل موجک پیوسته را نشان می‌دهد [۳۱]:

$$T(a.b)=\frac{1}{\sqrt{a}}\int_{-\infty}^{+\infty}x(t)\psi^{*}\left(\frac{t-b}{a}\right)dt \qquad (۱)$$

که در آن، $x(t)$ سیگنال در حوزه زمان و ψ نماد موجک مادر است. پارامتر a نمایانگر سطح تبدیل یا میزان فراخ‌شدگی موجک مادر را نشان می‌دهد. طبیعتاً هر چه عدد a بزرگ‌تر باشد، مؤلفه‌های فرکانس پایین‌تر به دست می‌آید و هر چه a کوچک‌تر باشد، مؤلفه‌های فرکانس بالاتر به دست می‌آید. پارامتر b نیز میزان جابجایی را نشان می‌دهد.

۳-۲- تبدیل موجک گسسته

ازآنجاکه فرایند پردازش تبدیل موجک نسبتاً زمان‌بر و پیچیده است، در اغلب کاربردها، تبدیل گسسته به علت ساده‌تر بودن ترجیح داده می‌شود. همان‌طور که بیان شد، تبدیل موجک گسسته میزان جابجایی تابع موجک مادر در هر سطح، به‌صورت

[1] Inertial Measurement Unit
[2] Alert Mode
[3] Kalman Filter
[4] Quadrature Correlator Output
[5] Short-Time Fourier Transform
[6] Convolution

گسسته تغییر می‌کند. رابطه (۲) چگونگی محاسبه تبدیل موجک گسسته را نشان می‌دهد [۳۱]:

$$T_{m.n} = \int_{-\infty}^{+\infty} x(t) \frac{1}{a_0^{\frac{m}{2}}} \psi(a_0^{-m} t - n b_0)\, dt \qquad (۲)$$

عدد صحیح m نمایانگر سطح یا همان مقیاس تبدیل می‌باشد و b_0 میزان جابجایی است که با استفاده از پارامتر n گسسته-سازی شده است. مقدار a_0 در اغلب مسائل برای سادگی برابر با دو در نظر گرفته می‌شود. بدین ترتیب میزان جابجایی در هر سطح از رابطه (۳) به دست می‌آید [۳۱].

$$\Delta b = b_0 a_0^m \qquad (۳)$$

برای پیاده‌سازی تبدیل موجک گسسته در عمل، از بانک فیلتر استفاده می‌شود. بدین‌صورت که سیگنال اصلی از مجموعه-ای از فیلترهای بالاگذر و پایین‌گذر عبور داده می‌شود. به خروجی فیلتر بالاگذر و فیلتر پایین‌گذر، به ترتیب بخش تقریب و جزئیات گفته می‌شود. در هر بار گذر سیگنال از فیلتر فرایند نمونه‌برداری کاهشی[1] انجام می‌شود. همچنین، در فرایند تبدیل معکوس این روند به‌طور معکوس انجام می‌پذیرد که به آن نمونه‌برداری افزایشی[2] گفته می‌شود [۳۲].

۳-۳- نویززدایی به کمک تبدیل موجک

در نویززدایی به کمک تبدیل موجک، هدف، تغییر ضرایب موجک به نحوی است که ضرایب مربوط به نویز از میان ضرایب سیگنال اصلی کاسته شود. یکی دیگر از ویژگی‌های قابل‌توجه تبدیل موجک، قابلیت متمرکز کردن اطلاعات سیگنال است. بدین معنا که پس از اعمال تبدیل موجک بر روی سیگنال، بخش اعظمی از انرژی سیگنال در محدوده خاصی متمرکز شده که شامل اطلاعات اصلی سیگنال است. به همین دلیل، انرژی مربوط به نویز موجود در سیگنال، در طیف وسیعی با دامنه کم توزیع می‌شود؛ بنابراین، می‌توان با اطمینان زیادی ادعا کرد که ضرایب نویز در بخش جزئیات سیگنال پخش شده و با حذف آن می‌توان بدون آن‌که به اطلاعات اصلی سیگنال آسیبی وارد شود، نویز را حذف نمود. به‌طورکلی می‌توان نویززدایی را به سه مرحله تقسیم کرد [۳۳]:

مرحله ۱: تجزیه سیگنال به طول M در سطح N با انتخاب موجک مادر مناسب و اعمال تبدیل موجک.

مرحله ۲: انتخاب سطح آستانه مناسب و اعمال آستانه‌گذاری و تغییر ضرایب موجک.

مرحله ۳: بازسازی سیگنال به کمک تبدیل موجک معکوس.

در قدم اول، سیگنال از میان فیلترهای بالاگذر و پایین‌گذر عبور می‌کند و بخش‌های تقریب و جزئیات را نتیجه می‌دهند. این فرایند به تعداد سطح تجزیه (N بار) تکرار می‌شود. در قدم بعدی برای تغییر ضرایب موجک در بخش جزئیات، حدود آستانه باید تعیین گردد. انتخاب مقادیر کم برای حدود آستانه موجب می‌شود اثرات نویز به‌خوبی حذف نشود و درصورتی‌که مقادیر بزرگی به آن اختصاص داده شود، ممکن است منجر به از دست رفتن اطلاعات سیگنال اصلی نیز بشود. در بسیاری از کاربردها، برای انتخاب این حدود آستانه از توابع ریاضی و آماری استفاده می‌شود؛ اما در روشی که در این مقاله ارائه می‌شود، این مقادیر، از طریق الگوریتم بهینه‌سازی انتخاب می‌شوند. اکنون چگونگی محاسبه و انتخاب حدود آستانه در روش‌های معمول تشریح می‌شود.

پس از انتخاب سطوح آستانه، فرایند آستانه‌گذاری بر روی ضرایب موجک اعمال می‌شود. به‌طورکلی آستانه‌گذاری بر دو نوع است. آستانه‌گذاری سخت و نرم که معادلات آن‌ها به ترتیب در روابط **Error! Reference source not found.**۴) و **Error! Reference source not found.**۵) بیان شده‌اند. در آستانه-گذاری سخت داده‌هایی با مقدار کمتر از مقدار حد آستانه صفر شده و مقادیر بیشتر از حد آستانه بدون تغییر باقی می‌مانند [۳۴]:

$$w'_{j.k} = \begin{cases} w_{j.k} & |w_{j.k}| \geq t_j \\ 0 & |w_{j.k}| < t_j \end{cases} \qquad (۴)$$

که در آن، زیروند j نشان‌گر سطح موجک اعمالی است. در آستانه‌گذاری نرم، علاوه بر صفر کردن داده‌های زیر سطح آستانه، داده‌های بالای سطح آستانه نیز به مقدار سطح آستانه کاهش داده می‌شوند [۳۴]:

$$w'_{j.k} = \begin{cases} sgn(w_{j.k})(|w_{j.k}| - t_j) & |w_{j.k}| \geq t_j \\ 0 & |w_{j.k}| < t_j \end{cases} \qquad (۵)$$

در کاربردهایی که همواری داده دارای اهمیت بیشتری است، از آستانه‌گذاری نرم استفاده می‌شود، درحالی‌که آستانه‌گذاری سخت برای آشکارسازی لبه‌ها در پردازش تصویر بهتر عمل می-کند [۳۵]. در مرجع [۳۴] به‌منظور عملکرد بهتر آستانه‌گذاری نرم، روشی ارائه شد که آستانه‌گذاری وفقی نام دارد. در روش آستانه‌گذاری وفقی، ضرایب تبدیل موجک با توجه به اینکه در چه سطحی از تجزیه هستیم، تغییر می‌کند. به همین دلیل پارامتر j که نشان‌گر سطح تجزیه است، نیز در رابطه سطح آستانه دخیل شده است. رابطه دقیق آستانه‌گذاری وفقی مطابق رابطه (۶) است [۳۴]:

[1] Down-sampling
[2] Up-sampling

$$w'_{j.k} = \begin{cases} sgn(w_{j.k})\left(|w_{j.k}| - \dfrac{t_j}{\left(|w_{j.k}|^2 - t_j{}^2\right)^j + 1}\right) & |w_{j.k}| \geq t_j \\ 0 & |w_{j.k}| < t_j \end{cases} \quad (۶)$$

پس از اعمال آستانه‌گذاری، در مرحله بازسازی، ضرایب موجک که تغییر یافته‌اند به‌وسیله تبدیل موجک معکوس سرهم-بندی می‌شوند. در صورت انتخاب درست سطح آستانه، سیگنال بازسازی‌شده حامل نویز کمتری خواهد بود.

در ادامه چهار روش آستانه‌گذاری متداول با نام‌های: ۱) Sqtwolog ، ۲) Rigrsure، ۳) Heursure و ۴) Minimaxi که در این مقاله جهت مقایسه نتایج مورداستفاده قرار گرفته است، شرح داده می‌شوند.

- **Sqtwolog**

این روش ابتدا توسط دونوهو و جانستون [۳۶] ارائه شد که در آن مقدار سطح آستانه از طریق رابطه (۷) محاسبه می‌شود [۳۷]:

$$th_i = \sigma_j \sqrt{2\, log(N_j)} \quad (۷)$$

که در آن، $\mathbf{N_j}$ طول سیگنال نویزی و $\boldsymbol{\sigma_j}$ میانگین انحراف مطلق[1] است و از طریق رابطه (۸) محاسبه می‌شود [۲۶]:

$$th_i = \sigma_j \sqrt{2\, log(N_j)} \, \boldsymbol{\sigma_j} = \frac{\boldsymbol{MAD_j}}{\mathbf{0.6745}} = \frac{\boldsymbol{median}\,(|\boldsymbol{\omega}|)}{\mathbf{0.6745}} \quad (۸)$$

که در آن، $\boldsymbol{\omega}$ نشان‌دهنده ضرایب موجک در سطح j ام است.

- **Rigrsure**

در این روش، مقدار سطح آستانه از رابطه (۹) به دست می‌آید [۲۶]:

$$th_i = \sigma_j \sqrt{\omega_b} \quad (۹)$$

که در آن، $\boldsymbol{\omega_b}$ از مجذور ضرایب موجک محاسبه شده و ریسک حداقل[2] نام دارد و σ_j برابر با میزان انحراف از معیار سیگنال نویزی است.

- **Heursure**

این روش، تلفیقی از دو روش پیشین است. در حالت عادی و درصورتی‌که سیگنال نویزی SNR نسبتاً زیادی داشته باشد، از روش Rigrsure برای تخمین سطح آستانه استفاده می‌شود؛ اما ازآنجاکه روش Rigrsure برای سیگنال‌های با SNR کم، عملکرد ضعیفی دارد [۳۸]، در این موارد روش Sqtwolg جایگزین آن می‌شود.

- **Minimaxi**

مقدار سطح آستانه در این روش از رابطه (۱۰) محاسبه می‌گردد [۳۹]:

$$\boldsymbol{th_i} = \begin{cases} \boldsymbol{\sigma} \times (\mathbf{0.3936} + \mathbf{0.10829} \times \boldsymbol{log_2 N} & \boldsymbol{N > 32} \\ \mathbf{0} & \boldsymbol{N < 32} \end{cases} \quad (۱۰)$$

که در این رابطه، N و $\boldsymbol{\sigma}$ به ترتیب طول و انحراف از معیار سیگنال نویزی می‌باشند.

در مقاله مرجع [۴۰]، میزان تأثیر نویززدایی این چهار روش به کمک موجک مادر Haar با یکدیگر مقایسه شده است. مطابق نتایج گزارش شده، روش rigrsure عملکرد بهتری داشته است.

۴- الگوریتم هجوم ذرات

الگوریتم هجوم ذرات یا PSO یک روش یادگیری هوشمند بر مبنای محاسبات تکاملی است که ابتدا کندی[3] و ابرهارت[4] آن را در ۱۹۹۵ در مرجع [۴۱] معرفی کردند. این الگوریتم از مفاهیم زیست‌شناسی و جامعه‌شناسی حیواناتی همچون پرندگان و ماهی‌ها جهت یافتن بهترین مسیر بهره می‌گیرد [۴۲]. تاکنون شواهد و آزمایش‌های تجربی گوناگونی کارایی این روش را در بهینه‌سازی اثبات کرده‌اند. به همین دلیل، در بسیاری از مسائل مهندسی که مرتبط با فرایند بهینه‌سازی هستند، این روش بسیار موردتوجه قرار گرفته است [۴۳ و ۴۴].

الگوریتم PSO برای حل مسئله، ابتدا جمعیتی از ذرات به تعداد N در فضای D بعدی به‌صورت تصادفی در فضای جستجوی مسئله تشکیل می‌دهد. میزان شایستگی نقاط انتخاب شده به‌وسیله تابع هزینه مسئله تعیین می‌شود که با توجه به نوع مسئله و هدف آن (بیشینه یا کمینه‌سازی)، تابع هزینه متفاوتی در نظر گرفته می‌شود. هدف الگوریتم PSO، جابجایی این ذرات به نحوی است تا مختصات نقطه بهینه یا اکسترمم مسئله یافت شود. به‌طورکلی، روش PSO شامل دو مدل از معادله سرعت و موقعیت این ذرات است [۴۱]:

$$V_i(t+1) = w * V_i(t) + c_1 r_1 \left(P_{best(i)}(t) - X_i(t)\right) + c_2 r_2 (G_{best}(t) - X_i(t)) \quad (۱۱)$$

$$X_i(t+1) = X_i(t) + V_i(t+1) \quad (۱۲)$$

روابط **Error! Reference source not found.**۱۱) و **Error! Reference source not found.**۱۲) به ترتیب روابط مربوط به به‌روزرسانی سرعت و موقعیت ذرات می‌باشند که در آن C_1 و C_2 دو ثابت شتاب هستند و معمولاً برابر با مقدار ۲ در نظر

[1] Mean Absolute Deviation (MAD)
[2] Minimal risk
[3] James Kennedy
[4] Russell Eberhart

گرفته می‌شوند. مقادیر r_1 و r_2 نیز اعداد تصادفی هستند که در بازه [۰ ۱] انتخاب می‌شوند. $P_{best(i)}$ و G_{best}، به ترتیب مدلی از بهترین تجربه هر ذره و بهترین تجربه کل جمعیت است. این مقادیر در هر دوره از اجرای الگوریتم به‌روزرسانی می‌شوند. مقدار w نیز لختی حرکت را مدل‌سازی می‌نماید که در بعضی کاربردها برابر ۱ قرار داده می‌شود، ولی در مرجع [۴۵] روشی ارائه شد که مقادیر این وزن با نزدیک شدن الگوریتم به جواب بهینه، کاهش می‌یابد. برای محاسبه این مقدار در هر دوره، از رابطه (۱۳) استفاده می‌شود [۴۱]:

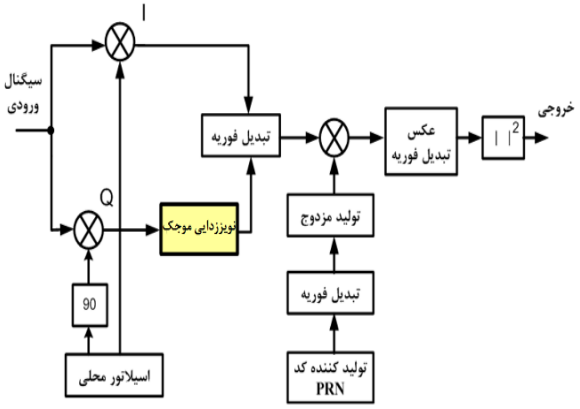
$$w(t+1) = w(t) * u^{-t} \qquad (۱۳)$$

که در آن، مقدار u می‌تواند در بازه [۱,۰۰۰۱,۱,۰۰۰۵] قرار گیرد. مزیت این روش در این است که سرعت ذرات با نزدیک به شدن به جواب کاهش می‌یابد و مانع از پراکنده شدن آن‌ها یا ناپایداری شود و به همین دلیل مسئله، همگرایی سریع‌تری دارد. همچنین، این روش به‌راحتی در نقاط اکسترمم محلی متوقف نشده و از آن‌ها عبور می‌کند.

۵- روش تلفیقی پیشنهادی

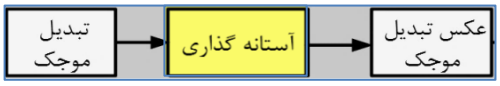
در این بخش از مقاله، روشی جدید برای نویززدایی سیگنال GPS در شاخه همبستگی Q واحد اکتساب به‌منظور مقابله با حمله فریب پیشنهاد می‌شود. همان‌طور که پیش‌تر اشاره شد، تبدیل موجک ابزاری مناسب برای کاهش نویز در سیگنال‌های غیرایستا، همچون سیگنال GPS است [۴۶ و ۴۷]. در روش پیشنهاد شده در این مقاله، از الگوریتم بهینه‌سازی PSO به جهت بهبود عملکرد تبدیل موجک استفاده می‌شود. سپس تبدیل موجک ارتقا یافته، مطابق روشی که در مرجع [۳۰] برای مقابله با فریب ارائه شده، به کار گرفته می‌شود. نویسندگان در مرجع [۳۰] نشان دادند که حمله فریب موجب افزایش فعل‌وانفعالات نویز مانندی در شاخه همبستگی Q گیرنده GPS خواهد شد. آنان در [۳۰] با به‌کارگیری الگوریتم نویززدایی موجک در بخش اکتساب گیرنده GPS، فعل‌وانفعالاتی را که به دلیل حضور سیگنال فریب بر روی این بازو ایجاد شده بود را کاهش دادند و از این طریق به مقابله با حمله فریب پرداختند. تفاوت اصلی روش پیشنهادی در این مقاله با مرجع [۳۰] در ارائه و به‌کارگیری تبدیل موجک ارتقا یافته جهت کاهش اثرات نویز مانند ناشی از حضور سیگنال فریب، در شاخه Q بخش اکتساب گیرنده GPS است.

بلوک دیاگرام کلی روش کاهش فریب مبتنی بر نویززدایی موجک در شکل (۱) آمده است. در اینجا اکتساب با روش جست‌وجوی فاز کد موازی انجام می‌پذیرد که پس از استخراج سیگنال‌های همبسته‌ساز، واحد نویززدایی روی سیگنال شاخه Q اعمال می‌شود.



شکل (۱). بلوک دیاگرام الگوریتم کاهش فریب با به‌کارگیری نویززدایی در واحد اکتساب

همان‌طور که در بخش (۳-۳) شرح داده شد، نویززدایی موجک دارای سه گام اساسی: ۱) تبدیل موجک، ۲) آستانه‌گذاری و ۳) عکس تبدیل موجک می‌باشد که در شکل (۲) نمایش داده شده است.



شکل (۲). مراحل نویززدایی موجک

اکنون روش پیشنهادی این مقاله جهت ارتقای نویززدایی موجک بر روی مرحله آستانه‌گذاری تمرکز دارد.

در روش پیشنهادی این مقاله، سطوح آستانه در تبدیل موجک با کمک بهینه‌سازی تکاملی به‌گونه‌ای انتخاب می‌شوند که عملکرد تبدیل موجک را نسبت به روش‌های نویززدایی متداول بهبود بخشد. در بسیاری از کاربردها، مقادیر سطوح آستانه با استفاده از توابع آماری متداولی همچون Minimaxi و Rigrsure انتخاب می‌شوند؛ اما در روش پیشنهادی این مقاله، انتخاب این سطوح آستانه بر عهده تابع بهینه‌سازی PSO قرار گرفته است. همان‌طور که پیش‌تر بیان شد، الگوریتم PSO برای بهینه‌سازی مسئله‌ای با تابع هزینه مشخص در فضای D بعدی استفاده می‌شود.

در بسیاری از کاربردهای پردازش سیگنال و نویززدایی، SNR به‌عنوان یکی از پرکاربردترین مشخصه‌های صحت سنجی الگوریتم نویززدایی مورداستفاده قرار می‌گیرد. مقدار این نسبت، از تقسیم میزان توان سیگنال به توان نویز محاسبه می‌شود. رابطه

(۱۴) چگونگی محاسبه این پارامتر را نشان می‌دهد [۳۴]:

$$SNR = 10 \times log(\frac{Power_{signal}}{Power_{noise}}) \quad (۱۴)$$

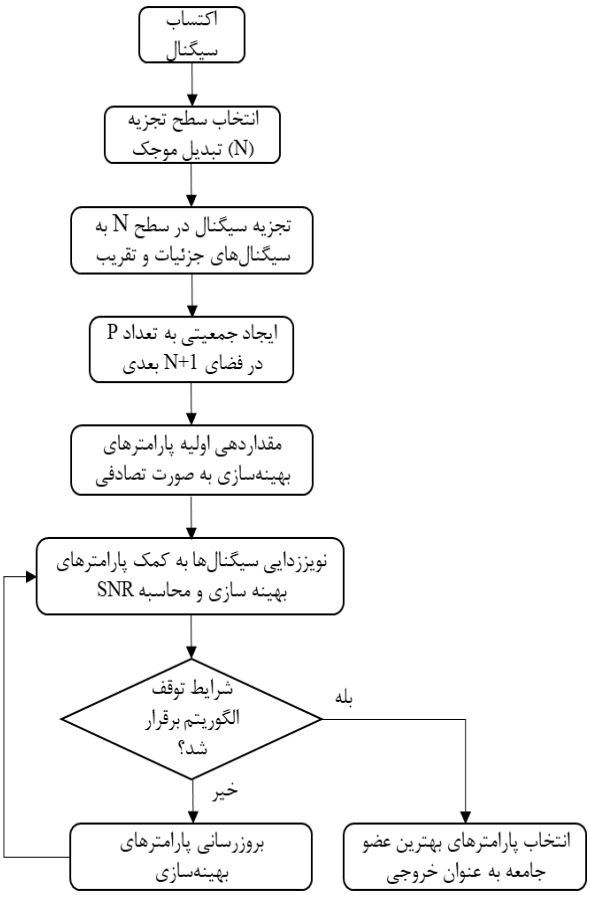
به‌منظور ارزیابی روش پیشنهادی، ابتدا عملکرد الگوریتم در کاهش نویز در چهار سیگنال معیار بلوک‌ها[1]، برجستگی[2]، سینوسی سنگین[3] و داپلر[4] سنجیده شده و سپس با روش‌های نویززدایی Rigrsure، Heursure، Sqtwolog و Minimaxi مقایسه می‌شود که در این قسمت، SNR به‌عنوان تابع هزینه در نظر گرفته شد. نتایج حاصل‌شده از این مقایسه، در بخش ۶-۱ شرح داده شده است.

ازآنجاکه هدف نهایی این مقاله، دفع حمله فریب است، الگوریتم پیشنهادی بر روی سیگنال‌های واقعی GPS نیز اعمال شد. در این بخش تابع هزینه به‌گونه‌ای طراحی شده تا میزان عملکرد سامانه در بخش اکتساب بهبود یابد. به همین دلیل، تعداد ماهواره‌های معتبر شناسایی‌شده در فرایند اکتساب به‌عنوان تابع هزینه در نظر گرفته شد. به‌گونه‌ای که به ازای هر ماهواره‌ای که به‌صورت صحیح تشخیص داده شود، الگوریتم امتیازی مثبت دریافت و درصورتی‌که در تشخیص ماهواره دچار خطا شود، امتیاز منفی دریافت نماید.

فضای مسئله مطرح‌شده در این مقاله شامل پنج پارامتر بهینه‌سازی می‌باشد که چهار مورد از آن‌ها مربوط به انتخاب حد آستانه و یک مورد در ارتباط با فرایند آستانه‌گذاری است. در این مقاله، برای نویززدایی سیگنال در شاخه همبستگی Q، از موجک هار با تجزیه چهار سطحی استفاده می‌شود و لذا برای هر یک از سطوح، به یک سطح آستانه نیاز است. همچنین، در این روش پارامتر دیگری نیز به جهت افزایش درجه آزادی مسئله به فرایند بهینه‌سازی افزوده شده است. این پارامتر در واقع ضریبی است که سعی در بهینه‌سازی فرایند آستانه‌گذاری دارد. این ضریب به‌عنوان پارامتر b در رابطه (۶) وارد شده و شیب آستانه‌گذاری وفقی را کنترل می‌کند. در نتیجه رابطه دقیق آستانه‌گذاری در اینجا مطابق رابطه (۱۵) است:

$$w'_{j.k} = \begin{cases} sgn(w_{j.k})(|w_{j.k}| - \frac{t_j}{(|w_{j.k}|^2 - t_j^2)^{j\times b} + 1}) & |w_{j.k}| \geq t_j \\ 0 & |w_{j.k}| < t_j \end{cases} \quad (۱۵)$$

به‌طور خلاصه می‌توان روش نویززدایی تلفیقی را در فلوچارت شکل (۳) مشاهده کرد.



شکل (۳). فلوچارت روش پیشنهادی

به‌طورکلی می‌توان فرایند مقابله با فریب را در سه مرحله زیر خلاصه نمود:

قدم اول: تجزیه و نویززدایی سیگنال در شاخه همبستگی Q با استفاده از سطوح آستانه به‌دست‌آمده توسط الگوریتم PSO.

قدم دوم: استفاده از نتایج همبستگی Q نویززدایی شده در فرایند اکتساب و شناسایی ماهواره‌ها.

قدم سوم: بررسی میزان شایستگی توسط تابع هزینه تعریف شده و به‌روزرسانی پارامترهای الگوریتم PSO و اجرای دوباره آن.

۶- صحت‌سنجی نتایج شبیه‌سازی

به‌منظور صحت‌سنجی روش پیشنهادی، ابتدا این روش در نویززدایی چهار سیگنال معیار به کار گرفته شده و میزان کارایی آن با روش نویززدایی بر مبنی تبدیل موجک معمولی مقایسه

[1] Blocks
[2] Bumps
[3] Heavy Sine
[4] Doppler

می‌شود. سپس روش پیشنهادی در مسئله مقابله با حمله فریب با اعمال بر روی داده‌های واقعی GPS که فریب به آن‌ها اضافه شده تحلیل و بررسی می‌گردد و کارایی آن با روش مرجع [۳۰] مقایسه می‌شود. در تمامی این مراحل، شبیه‌سازی در نرم‌افزار MATLAB اجرا شده‌اند.

جدول (۲). نتایج به‌کارگیری الگوریتم پیشنهادی بر بهبود SNR در توابع معیار

تابع معیار	SNR	Rigrsure	Sqtwolog	Heursure	Minimaxi	روش تلفیقی	میانگین بهبود (%) SNR
بلوک‌ها	۲	۱۸۶۵/۱۰	۵۳۴۷/۱۱	۱۸۶۵/۱۰	۵۴۹۹/۱۱	۱۵۸۲۲۱	۲۰/۴۶
	۵	۵۱۳۵/۱۲	۷۹۳۳/۱۱	۵۱۳۵/۱۲	۰۲۷۱/۱۲	۴۶۶۱/۱۸	۳۱/۵۱
	۱۰	۰۴۱۳/۱۴	۰۳۷۳/۹	۰۴۱۳/۱۴	۷۹۷۵/۱۱	۰۳۷۰/۱۶	۴۵/۳۵
برجستگی	۲	۸۲۲۱/۷	۱۹۵۹/۸	۸۲۲۱/۷	۱۱۹۵/۸	۴۳۰۵/۱۱	۱۲/۴۳
	۵	۰۴۹۰/۱۲	۸۹۲۸/۸	۰۴۹/۱۲	۹۱۴۲/۹	۷۴۹/۱۴	۸۶/۳۹
	۱۰	۱۳۹۴/۱۴	۸۷۶۴/۸	۱۳۹۴/۱۴	۹۳۸۲/۱۱	۶۳۰۲/۱۶	۴۷/۴۰
سینوسی سنگین	۲	۳۹۳۵/۷	۵۵۸۴/۱۴	۳۹۳۵/۷	۹۱۲۸/۱۳	۳۲۱۳/۱۴	۱۴/۴۷
	۵	۹۳۸۳/۹	۸۱۲/۱۷	۹۳۸۳/۹	۸۱۲/۱۷	۷۵۴۷/۱۷	۱۶/۳۹
	۱۰	۵۸۰۳/۱۲	۸۶۳۲/۱۹	۵۸۰۳/۱۲	۸۳۶۱/۱۹	۸۳۰۲/۱۹	۷۶/۲۸
داپلر	۲	۵۰۰۹/۶	۲۹۳۸/۹	۵۰۰۹/۶	۰۳۶۸/۹	۱۶۶۶/۱۱	۸۱/۴۶
	۵	۲۳۶۹/۹	۹۵۰۷/۹	۲۳۶۹/۹	۹۵۱۳/۹	۸۴۶۸/۱۲	۰۹/۳۴
	۱۰	۸۸۱/۱۲	۷۰۰۴/۱۰	۸۸۱/۱۲	۶۹۲۶/۱۰	۰۳۱۶/۱۶	۱۶/۳۷

۶-۱- نتیجه الگوریتم نویززدایی بر روی سیگنال‌های معیار

در این بخش نتایج الگوریتم نویززدایی تلفیقی که در بخش پیشین معرفی شد، بر روی چهار سیگنال معیار[1] اعمال شده و نتایج آن‌ها ارائه می‌شود.

سیگنال‌های معیار انتخاب شده عبارت‌اند از: ۱- بلوک‌ها، ۲- برجستگی، ۳- سینوسی سنگین و ۴- داپلر. این سیگنال‌ها، در سه سطح مختلف با نویز سفید گوسی ترکیب شده و سیگنال‌هایی با SNR دارای مقادیر ۲، ۵ و ۱۰ ایجاد کرده و سپس به‌عنوان داده آزمایشی به الگوریتم نویززدایی اعمال می‌شوند. این چهار سیگنال به‌طور خاص در مراجع مختلف، جهت بررسی میزان عملکرد روش‌های نویززدایی مورداستفاده قرار گرفته‌اند [۴۸ و ۴۹]. سیگنال‌ها توسط نرم‌افزار MATLAB جهت مقایسه نتایج نویززدایی تبدیل موجک تولید می‌شوند. به همین جهت، در تمامی موارد، طول سیگنال (N) به‌صورت توانی از ۲ در نظر گرفته می‌شود تا فرایند تجزیه در تبدیل موجک به‌سادگی صورت گیرد. در این شبیه‌سازی، طول سیگنال‌ها به‌صورت یکسان و برابر با ۱۰۲۴ نمونه انتخاب شده‌اند.

همان‌طور که پیش‌تر اشاره شد، جهت مقایسه، میزان کاهش نویز در سیگنال‌های معیار، توسط روش‌های متداول انتخاب سطوح آستانه موردبررسی قرار گرفت. در این مقاله به‌طور خاص، روش‌های متداول با نام‌های ۱- Rigrsure، ۲- Heursure، ۳-Sqtwolog و ۴- Minimaxi مورداستفاده قرار گرفته‌اند [۵۰، ۳۴ و ۵۱].

یکی از عوامل مهم در اثربخشی روش پیشنهادی، پارامترهای انتخاب شده برای الگوریتم بهینه‌سازی PSO است که در این بخش از شبیه‌سازی‌ها، مطابق جدول (۱) انتخاب شدند.

جدول (۱). مقادیر پارامترهای الگوریتم PSO در الگوریتم پیشنهادی

پارامتر	مقدار
تعداد جمعیت	۴۰
تعداد دفعات تکرار	۸۰
C_1	۲
C_2	۲
u^{-1}	۹۸/۰

در مقایسه با روش‌های متداول بیان‌شده، مشاهده شد که الگوریتم تلفیقی پیشنهادی می‌تواند میزان SNR را به‌طور میانگین ۴۷/۳ درصد بهبود دهد. جزئیات مقایسه عملکرد الگوریتم تلفیقی با دیگر روش‌ها در جدول (۲) بیان شده است.

هر سطر از جدول (۲) شامل مقادیر SNR سیگنال‌های معیار است که نام هر یک در ستون سمت راست بیان شده است. با توجه به جدول (۲) می‌توان مشاهده کرد که الگوریتم پیشنهادی به‌طورکلی عملکرد بهتری نسبت به روش‌های دیگر داشته و حتی در مواردی همچون تابع نویزی سینوسی سنگین با میزان سیگنال به نویز ۲ را توانسته تا میزان SNR تقریباً دو برابر ارتقا دهد. جدول (۲) نشان می‌دهد که روش پیشنهادی قادر است به‌خوبی میزان SNR را بهبود دهد.

۶-۲- تولید داده فریب

شکل (۴) نحوه‌ی جمع‌آوری داده‌های موردنیاز را نشان‌می‌دهد.

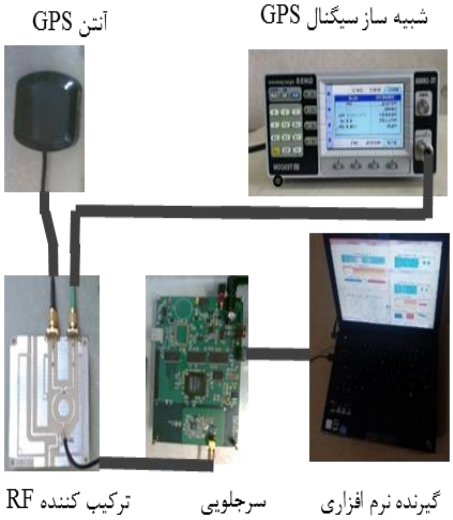
[1] Benchmark

همان‌طور که ملاحظه می‌شود، سیگنال GPS توسط آنتن GPS دریافت می‌شود. مدل ریاضی سیگنال دریافتی توسط گیرنده GPS در فرکانس L_1 را می‌توان مطابق رابطه (۱۶) نوشت [۱۵]:

$$S_{L1_{CA}}(t) = A_c C_i(t) D_i(t) sin(\omega_{L1}(t) + \varphi_{L1}) \quad (۱۶)$$

در این رابطه، A_C دامنه کد C/A و C_i کد C/A برای i امین ماهواره می‌باشند. D_i پیام ناوبری i امین ماهواره، ω_{L1} فرکانس زاویه‌ای سیگنال L1 و φ_{L1} فاز اولیه سیگنال L1 است.

سپس سیگنال اصلی با سیگنال فریب در یک ترکیب‌کننده ترکیب می‌شود. سیگنال فریب از نظر ساختاری کاملاً مشابه با سیگنال اصلی GPS می‌باشد و در شبیه‌ساز سیگنال GPS تولید شده است. پس از ترکیب سیگنال اصلی و فریب، سیگنال ترکیبی در قسمت سر جلویی[1] موجود پردازش شده و به مبدل آنالوگ به دیجیتال[2] (ADC) منتقل می‌شود.



شکل (۴). نحوه تولید سیگنال فریب و جمع‌آوری داده‌ها

از نظر ریاضی، سیگنال فریب با تأخیر یافته سیگنال اصلی که دارای دامنه متفاوت است، مدل می‌شود. پس از افزودن سیگنال تأخیر یافته به سیگنال اصلی و ساخت فریب، مدل ریاضی سیگنال دریافتی توسط ADC را می‌توان مطابق رابطه (۱۷) نوشت [۱۵]:

$$C_{L1_{CA}}(t) = A_C^A C_i^A(t) D_i^A(t)\, sin(\omega_{L1}(t) + \varphi_{L1}^A) + A_C^D C_i^D(t) D_i^D(t)\, sin(\omega_{L1}(t - \Delta t_D) + \varphi_{L1}^D) \quad (۱۷)$$

بالانویس و زیرنویس A و D به ترتیب بیان‌گر سیگنال معتبر و تأخیریافته می‌باشند. Δt_D و φ_{L1}^D نیز به ترتیب میزان تأخیر کد و اختلاف فاز سیگنال تأخیریافته نسبت به سیگنال معتبر را بیان می‌کنند.

در رابطه (۱۷)، زیروندهای A وD به ترتیب نشان‌دهنده بخش‌های اصلی و تأخیر یافته سیگنال می‌باشند. در نهایت، خروجی ADC (سیگنال IF) ذخیره می‌شود و توسط گیرنده نرم‌افزاری GPS مبتنی بر MATLAB پردازش شده و اطلاعات ناوبری استخراج می‌شود.

۶-۳- نتایج الگوریتم ضدفریب

الگوریتم پیشنهادی بر روی تعداد زیادی از سیگنال‌های واقعی GPS اعمال شد که در این بخش، به‌منظور تشریح عملکرد الگوریتم پیشنهادی، نتایج حاصل از یک مورد از آن‌ها گزارش می‌شود. مطابق روالی که در بخش پیشین معرفی شد، الگوریتم پیشنهادی بر روی شاخه همبستگی Q در بخش اکتساب به کار گرفته شد که تأثیر به‌کارگیری این الگوریتم بر نتایج اکتساب و نیز تأثیر آن بر مقادیر خطای موقعیت‌یابی در بخش ناوبری، ارائه می‌شود.

به‌منظور صحت‌سنجی دقیق‌تر، نتایج بخش اکتساب در چهار حالت متفاوت موردبررسی قرار گرفت:

۱- گیرنده تحت هیچ‌گونه حمله‌ای نبوده و داده معتبر دریافت می‌کند.

۲- گیرنده تحت حمله فریب قرار می‌گیرد.

۳- گیرنده تحت حمله فریب قرار دارد و مقابله با فریب بر مبنی تبدیل موجک معمول صورت می‌پذیرد که در آن حدود آستانه با استفاده از روش‌های متداول انتخاب شده‌اند.

۴- گیرنده تحت حمله فریب قرار دارد و مقابله با فریب بر مبنی تبدیل موجک ارتقایافته صورت می‌پذیرد که در آن حدود آستانه با استفاده از الگوریتم PSO انتخاب شده‌اند.

مشابه بخش قبلی، در این مرحله از شبیه‌سازی نیز پارامترهای الگوریتم PSO به‌صورت مقادیر مشخصی تنظیم شدند که در جدول (۳) بیان شده‌اند.

جدول (۳). مقادیر پارامترهای الگوریتم PSO در الگوریتم ضدفریب

پارامتر	مقدار
تعداد جمعیت	۴۰
تعداد دفعات تکرار	۴۰
C_1	۲

[1] Front-End
[2] Analog to Digital Converter

C_2	۲
u^{-1}	۹۸/۰

شکل (۵) نتایج بخش اکتساب گیرنده را در حالت عادی و بدون حمله فریب نشان می‌دهد. در این شکل، ستون‌های سبزرنگ نشان‌گر ماهواره‌هایی هستند که در طی فرایند اکتساب به‌عنوان ماهواره در دید شناسایی شدند. در این حالت، شش ماهواره قابل‌رؤیت هستند. به‌طور مشابه، شکل‌های (۶)، (۷) و (۸) نیز نتیجه بخش اکتساب را برای حالات بیان شده نشان می‌دهند.

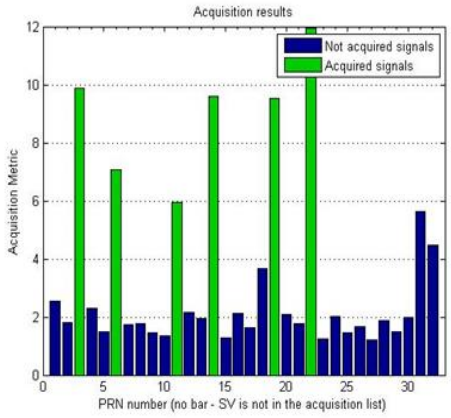
جدول (۴). نتایج به‌کارگیری الگوریتم ضدفریب پیشنهادی در کاهش خطای مکان‌یابی ناشی از حمله فریب

شرایط گیرنده	مکان‌یابی در حالت بدون فریب (m)	اعمال الگوریتم ضدفریب با استفاده از نویززدایی معمول موجک [۳۰]	اعمال الگوریتم ضدفریب با استفاده از نویززدایی پیشنهادی با به‌کارگیری الگوریتم PSO	درصد بهبود روش پیشنهادی
مؤلفه x موقعیت	۹۴/۳۲۳۴۹۱۹	۸۹/۳۲۳۴۹۴۳	۹۶/۳۲۳۴۹۱۴	۲۰/۷۹
مؤلفه y موقعیت	۹۴/۴۰۵۳۰۲۴	۷۴/۴۰۵۳۰۵۷	۷۳/۴۰۵۳۰۲۵	۵۹/۹۷
مؤلفه z موقعیت	۸۸/۳۷۰۳۴۶۵	۹۸/۳۷۰۳۴۷۹	۴۳/۳۷۰۳۴۶۱	۴۳/۶۸
خطای کل مکان‌یابی	-	۶۳/۳۹	۶۷/۲۴	۷۴/۳۷

جدول (۵). مقایسه کیفی روش پیشنهادی با سایر روش‌ها

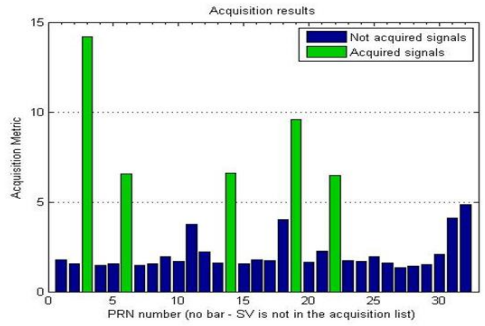
روش کار	محدودیت	مزیت	تجهیزات موردنیاز	محل اعمال الگوریتم	آشکارسازی	مقابله
تلفیق با ناوبری مبتنی بر IMU [۲۵]	کارایی ضعیف در حملات فریب طولانی‌مدت (با نرخ کند تغییرات)	تشخیص آسان	ارتقای نرم‌افزاری و سخت‌افزاری	واحد ناوبری	بلی	بلی
نظارت بر توان [۱۸]	محدوده بزرگ عدم کارایی	تشخیص آسان و پیچیدگی کم	ارتقای نرم‌افزاری و سخت‌افزاری	بخش سرجلویی گیرنده	بلی	خیر
نظارت بر همبستگی [۲۰-۲۴]	کارایی ضعیف در حضور چندمسیری	تشخیص آسان	ارتقای نرم‌افزاری	شاخه‌های همبسته‌ساز	بلی	خیر
پردازش فضایی [۲۸]	عدم کارایی در حملات پیچیده	قابلیت اطمینان بالا	ارتقای نرم‌افزاری و سخت‌افزاری	بخش سرجلویی گیرنده	بلی	بلی
نظارت بر زمان ورود [۱۹]	تشخیص پس از تسلط فریبنده و قابلیت پیش‌بینی بیت‌ها توسط فریبنده	تشخیص آسان	ارتقای نرم‌افزاری	واحد ناوبری	بلی	خیر
روش پیشنهادی	عدم کارایی در حملات اعمال شده در واحد ردیابی	پیاده‌سازی آسان	ارتقای نرم‌افزاری	واحد اکتساب	خیر	بلی

کانال‌های جعلی شناسایی می‌شوند. مطابق شکل (۶)، ماهواره شماره ۱۱ به‌طورکلی حذف شده است. پس از اعمال الگوریتم ضدفریب که بخش نویززدایی آن با روش‌های متداول انجام شده است، اکتساب بهبود چندانی نداشته و مشاهده می‌شود که ماهواره ۱۴ حذف شده و کانال غیرمعتبر شماره ۱۸ نیز اشتباهاً شناسایی شده است (مطابق شکل ۷).

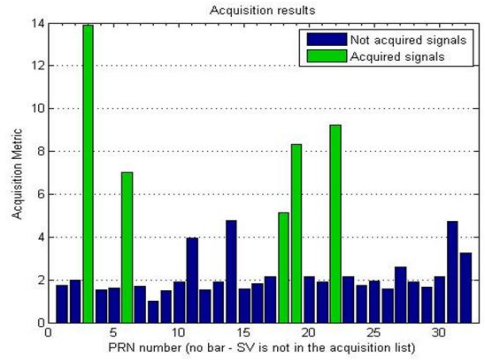


شکل (۵). نتیجه بخش اکتساب برای گیرنده در حالت بدون فریب

درصورتی‌که گیرنده تحت حمله فریب قرار گیرد، فرایند اکتساب دچار اختلال شده و تعدادی از کانال‌های ماهواره حذف شده و یا

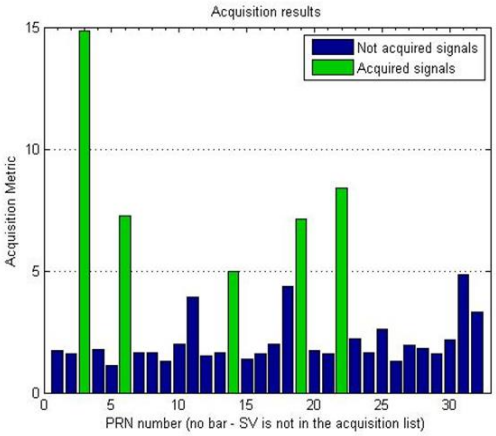


شکل (۶). نتیجه بخش اکتساب برای گیرنده تحت حمله فریب



شکل (۷). نتیجه بخش اکتساب برای گیرنده تحت حمله فریب و اعمال الگوریتم ضدفریب نویززدایی متداول در شاخه همبستگی Q

حال اگر الگوریتم نویززدایی با کمک الگوریتم PSO اعمال شود، نتایج متفاوتی را شاهد خواهیم بود. شکل (۸) نتیجه بخش اکتساب را در این حالت نشان می‌دهد. مطابق شکل (۷) در اینجا برخلاف حالت قبل هیچ کانال غیرمعتبری در فرایند اکتساب وارد نشده است.



شکل (۸). نتیجه بخش اکتساب برای گیرنده تحت حمله فریب و اعمال الگوریتم ضدفریب نویززدایی ارتقایافته توسط بهینه‌سازی PSO در شاخه همبستگی Q

در نهایت برای سنجش و مقایسه میزان عملکرد الگوریتم ضدفریب پیشنهادی، مقادیر خطای ناوبری و موقعیت جغرافیایی محاسبه شد و در جدول (۴) گزارش می‌شود. مطابق این جدول، مشاهده می‌شود که در صورت استفاده از الگوریتم معمول موجک جهت نویززدایی، گیرنده خطای بیشتری را متحمل می‌شود و با به‌کارگیری روش پیشنهادی دقت نهایی مکان‌یابی ۳۷/۷۴ درصد بهبود دارد. به‌منظور صحت‌سنجی بیشتر، روش پیشنهادی با دیگر روش‌های معمول در حوزه‌ی آشکارسازی و مقابله با فریب مورد مقایسه کیفی قرار گرفت که نتایج آن در جدول (۵) ملاحظه می‌شود.

۷- نتیجه‌گیری

در این پژوهش، روش جدیدی برای کاهش اثر مخرب اختلال فریب در سامانه‌ی GPS پیشنهاد شد. در این روش، ابتدا به کمک الگوریتم بهینه‌سازی PSO مقادیر حدود آستانه تبدیل موجک گسسته به‌صورت بهینه تنظیم شد و از این طریق میزان عملکرد این تبدیل در فرایند کاهش نویز، بهبود قابل‌توجهی حاصل شد. میزان SNR سیگنال‌های معیار پس از اعمال روش پیشنهاد شده، در مقایسه با نویززدایی از طریق روش‌های آستانه‌گذاری Rigrsure، Heursure، Sqtwolog و Minimaxi به ترتیب ۴۷/۳، ۳۸/۴، ۴۷/۳ و ۳۰ درصد بهبود یافت. پس‌ازآن که از عملکرد روش پیشنهادی در کاهش نویز اطمینان حاصل شد، این الگوریتم به‌منظور کاهش تأثیر نویزگونه سیگنال فریب روی شاخه همبستگی Q در بخش اکتساب گیرنده GPS به کار گرفته شد. روش پیشنهادی روی داده‌های واقعی سیگنال GPS دارای اختلال فریب، اعمال شد. نتایج حاصله، کاهش ۳۷/۷۴ درصدی خطای موقعیت‌یابی ناشی از فریب را در مقایسه با الگوریتم‌های معمول نشان داد.

۶- مراجع

[1] M. R. Mosavi, "Data processing on single-frequency GPS receivers," Iran University of Science and Technology, 2010. (in persion)

[2] M. Moazedi, M. Mosavi, Z. Nasrpooya, & A. Sadr, "GPS spoofing mitigation using adaptive estimator in tracking loop," *Journal of Electronical & Cyber Defence*, vol. 6, no. 3, 2018. (in Persian)

[3] H. N. Li, D. S. Li, & G. B. Song, "Recent applications of fiber optic sensors to health monitoring in civil engineering," Engineering Structure, vol. 26, no. 11, pp.1647-1657, 2004.

[4] D. Ahn, J. Park, C. Kim, J. Kim, Y. Qian & T. Itoh, "A design of the low-pass filter using the novel microstrip defected ground structure," IEEE Transactions on Microwave Theory and Techniques, vol. 49, no. 1, pp. 86-93, 2001.

[5] B. Baykal & A. G. Constantinides, "A neural approach to the underdetermined-order recursive least-squares adaptive filtering," Neural Networks, vol. 10, no. 8, pp. 1523-1531, 1997.

[6] M. Han, Y. Liu, J. Xi & W. Guo, "Noise smoothing for nonlinear time series using wavelet soft threshold," IEEE Signal Processing Letters, vol. 14, no. 1, pp. 62-65, 2007.

[7] J. Baili, S. Lahouar, M. Hergli, I. L. Al-Qadi, & K. Besbes, "GPR signal de-noising by discrete wavelet transform," Ndt and E International, vol. 42, no. 8, pp.696-703, 2009.

[8] T. H. Yi, H. N. Li, & X. Y. Zhao, "Noise smoothing for structural vibration test signals using an improved wavelet thresholding technique," Sensors, vol. 12, no. 8, pp. 11205-11220, 2012.

[9] D. L. Donoho & I. M. Johnstone, "Adapting to unknown smoothness via wavelet shrinkage," J. Am. Statist. Assoc. vol. 90, no. 432, pp. 1200-1224, 1995.

[10] D. L. Donoho & I. M. Johnstone, "Ideal spatial adaptation via wavelet shrinkage," Biometrika, vol. 81, no. 3, pp. 425-455, 1994.

[11] A. R. Baziar, M. R. Mosavi, & M. Moazedi, "Spoofing mitigation using double stationary wavelet transform in civil GPS receivers," Wireless Personal Communications, vol. 109 no. 3, pp.1827-1844, 2019.

[12] X. Gu, J. Shi, J. Li, Y. Huang & J. Lin, "Application of wavelets analysis in image denoising," 2008 International Conference on Apperceiving Computing and Intelligence Analysis, pp. 49-52, 2008.

[13] B. J. Yoon & P. P. Vaidyanathan, "Wavelet-based denoising by customized thresholding," IEEE International Conference on Acoustics, Speech, and Signal Processing, 2004.

[14] G. X. Song & R. Z. Zhao, "Three novel models of threshold estimator for wavelet coefficients," International Conference on Wavelet Analysis and Its Applications, pp. 145-150. 2001.

[15] M. R. Mosavi, M. Moazedi, M. J. Rezaei & A. Tabatabaei, "Interference mitigation in GPS receivers," Iran University of Science and Technology, 2015. (in persion)

[16] KD. Wesson, JN. Gross, TE. Humphreys, & BL. Evans, "GNSS signal authentication via power and distortion monitoring," IEEE Transactions on Aerospace and Electronic Systems, vol. 54, no. 2, pp. 739-754, 2018.

[17] X. Shang, F. Sun, L. Zhang, J. Cui, & Y. Zhang, "Detection and mitigation of GNSS spoofing via the pseudo-range difference between epochs in a multicorrelator receiver," GPS Solutions, vol. 26, no. 2, pp. 1-14, 2022.

[18] D. P. Shepard & T. E. Humphreys, "Characterization of receiver response to spoofing attacks, " GPS World, vol. 21, no. 9, pp. 27-33, 2010.

[19] S. C. Lo & P. K. Enge, "Authenticating aviation augmentation system broadcasts," IEEE/ION Position, Location and Navigation Symposium, pp. 708-717, 2010.

[20] C. Sun, J. W. Cheong, A. G. Dempster, H. Zhao, L. Bai, & W. Feng, "Robust spoofing detection for GNSS instrumentation using Q-channel signal quality monitoring metric," IEEE Transactions on Instrumentation and Measurement, vol. 70, pp. 1-15, 2021.

[21] A. M. Khan & A. Attiq, "Global navigation satellite systems spoofing detection through measured autocorrelation function shape distortion," International Journal of Satellite Communications and Networking, vol. 40, no. 2, pp. 148-156, 2022.

[22] W. Zhou, Z. Lv, X. Deng & Y. Ke, "A new induced GNSS spoofing detection method based on weighted second-order central moment," IEEE Sensors Journal, vol. 22, no. 12, pp. 12064-12078, 2022.

[23] J.N. Gross, C. Kilic, & TE. Humphreys, "Maximum-likelihood power-distortion monitoring for GNSS-signal authentication," IEEE Transactions on Aerospace and Electronic Systems, vol. 55, pp. 469-475, 2019.

[24] Y. Guo, L. Miao, & X. Zhang, "Spoofing detection and mitigation in a multi-correlator GPS receiver based on the maximum likelihood principle," Sensors, vol. 19, no. 1, 2019.

[25] Y. Liu, S. Li, Q. Fu, Z. Liu, & Q. Zhou, "Analysis of kalman filter innovation-based GNSS spoofing detection method for INS/GNSS integrated navigation system," IEEE Sensors Journal, vol. 19, no. 13, pp. 5167-5178, 2019.

[26] N. Stenberg, E. Axell, J. Rantakokko, & G. Hendeby, "Results on GNSS spoofing mitigation using multiple receivers," Journal of the Institute of Navigation, vol. 69, no. 1, pp. 1-29, 2022.

[27] B. Pardhasaradhi, G. Srinath, G. S. Vandana, P. Srihari, & P. Aparna, "GNSS spoofing detection and mitigation in multireceiver configuration via tracklets and spoofer localization," IEEE Access, vol. 10, pp. 42014-42028, 2022.

[28] F. Rothmaier, Y. H. Chen, S. Lo, & T. Walter, "GNSS spoofing detection through spatial processing," Journal of Navigation, vol. 68, no. 2, pp. 243-258, 2021.

[29] Z.Lin, C. Haibin, & Z. Naitong, "Anti-spoofing extended Kalman filter for satellite navigation receiver," IEEE Conference on Wireless Communications, Networking and Mobile Computing, pp. 996-999, 2007.

[30] M. R. Mosavi, R. Zebarjad & M. Moazedi, "Novel anti-spoofing methods based on discrete wavelet transform in the acquisition and tracking stages of civil GPS receiver," International Journal of Wireless Information Networks, vol. 25, no. 44, pp. 449-460, 2018.

[31] L. Chun-Lin, "A tutorial of the wavelet transform," NTUEE, Taiwan, 2010.

[32] R. Polikar, "The wavelet tutorial," IOWA State University, USA, 1996.

[33] C. Taswell, "The what, how and why of wavelet shrinkage denoising," Journal of Computing in Science and Engineering, vol. 2, no. 3, pp. 12-19, 2000.

[34] Y. Chen, Y. Cheng, & H. Liu, "Application of improved wavelet adaptive threshold de-noising algorithm in FBG demodulation," Optik, vol. 132, pp.243-248, 2017.

[35] R. Rangarajan, R. Venkataramanan, & S. Shah, "Image denoising using wavelets," Wavelet and Time Frequencies, vol. 14, pp. 1-14, 2002.

[36] D. L. Donoho, & I. M. Johnstone, "Adapt to unknown smoothness via wavelet shrinkage", Journal of the american statistical association, vol. 90, pp.1200-1224, 1995.

[37] A. K. Verma & N. Verma, "Performance analysis of wavelet thresholding methods in denoising of audio signals of some indian musical instruments," Int. J. Eng. Sci. Technol., vol. 4, no. 5, pp. 2047-2052, 2012.

[38] N. K. Al-Qazzaz, S. Ali, S. A. Ahmad, M. S. Islam, & M. I. Ariff, "Selection of mother wavelets thresholding methods in denoising multi-channel EEG signals during working memory task," IEEE Conference on Biomedical Engineering and Sciences (IECBES), pp. 214-219, 2014.

[39] M. stndag, A. Sengr, M. Gkbulut, & F. Ata, "Performance comparison of wavelet thresholding techniques on weak ECG signal denoising," Przegld Elektrotechniczny, vol. 89, no. 5, pp. 63-66, 2013.

[40] D. Valencia, D. Orejuela, J. Salazar & J. Valencia, "Comparison analysis between rigrsure, sqtwolog, heursure and minimaxi techniques using hard and soft thresholding methods," 2016 XXI Symposium on Signal Processing, Images and Artificial Vision (STSIVA), pp. 1-5, 2016.

[41] J. Kennedy & R. Eberhart, "Particle swarm optimization," Proceedings of ICNN'95-International Conference on Neural Networks, vol. 4, pp. 1942-1948, 1995.

[42] Z. A. Bashir & M. E. El-Hawary, "Applying wavelets to short-term load forecasting using PSO-based neural networks," IEEE Transactions on Power Systems, vol. 24, no. 1, pp. 20-27, 2009.

[43] W. Yu & X. Li, "Fuzzy identification using fuzzy neural networks with stable learning algorithms," IEEE Transactions on Fuzzy Systems, vol. 12 no. 3, pp.411-420, 2004.

[44] J. S. Heo, K. Y. Lee, & R. Garduno-Ramirez, "Multiobjective control of power plants using particle swarm optimization techniques," IEEE Transactions on Energy Conversion, vol. 21, no. 2, pp.552-561, 2006.

[45] B. Jiao, Z. Lian, & X. Gu, "A dynamic inertia weight particle swarm optimization algorithm," Chaos, Solitons & Fractals, vol. 37, no. 3 pp.698-705, 2008.

[46] M. Souza, J. F. G. Monico, A. Pagamisse & W. G. C. Polezel, "An effective wavelet method to detect and mitigate low-frequency multipath effects," International Association of Geodesy Symposia, vol. 132, pp. 179-184, 2008.

[47] M. R. Azarbad & M. R. Mosavi, "A new method to mitigate multipath error in single-frequency GPS receiver with wavelet transform," Journal of GPS Solutions, vol. 18, no. 2, pp. 189-198, 2014.

[48] D. L. Donoho, & I. M. Johnstone, "Ideal Spatial Adaptation by Wavelet Shrinkage," Biometrika, vol. 81, pp. 425-455, 1994.

[49] D. L. Donoho, & I. M. Johnstone, "Adapting to unknown smoothness via wavelet shrinkage," Journal of the American Statistical Association, vol. 90, pp. 1200-1224, 1995.

[50] D. L. Donoho, "Progress in wavelet analysis and WVD: a ten minute tour," Progress in Wavelet Analysis and Applications (Y. Meyer, and S. Roques, eds.). Gif-sur-Yvette: Editions Frontières, 1993.

[51] D. L. Donoho, "De-noising by soft-thresholding," IEEE Transactions on Information Theory, vol. 42, no. 3, pp. 613-627, 1995.