

روشی جدید برای کاهش اثر فریب در گیرنده های GPS تک فرکانسه مبتنی بر تبدیل موجک

سید محمدرضا موسوی میرکلایی^۱، امیررضا بازیار^۲ و مریم معاضدی^۳
دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، نارمک، تهران ۱۳۱۱۴-۱۶۸۴۶، ایران
^۱استاد، نویسنده مسئول، m_mosavi@iust.ac.ir
^۲کارشناسی ارشد، amirrezabaziar@elec.iust.ac.ir
^۳دانشجوی دکتری، moazedi@elec.iust.ac.ir

چکیده - در سال های اخیر فریب دهنده یک تهدید ثابت شده برای گیرنده های GPS محسوب می شود. نتیجه حمله فریب خطاهای بزرگ ناوبری در گیرنده ناآگاه با نتایج وخیم است. از آن جا که سیگنال فریب از سیگنال اصلی تقلید می کند، گیرنده متوجه حضور آن نمی شود. از این رو تشخیص و جبران سازی آن سخت تر از دیگر اختلال های مطرح شده برای GPS است. در این مقاله تکنیک پردازشی ارائه شده است که اثر فریبندگی را کاهش می دهد. اساس کار الگوریتم ارائه شده مبتنی بر نویز زدایی با تبدیل موجک است. با توجه به این که مشخصه شبه فاصله در اثر فریب تغییرات غیر معمول تجربه می کند، تبدیل موجک در مرحله ناوبری از فرآیند پردازش گیرنده GPS اعمال می شود. به منظور ارزیابی عملکرد الگوریتم پیشنهادی، آزمایش های متعدد بر روی چندین مجموعه داده انجام شده است. نتایج آزمون ها نشان دادند که روش ارائه شده با متوسط ۶۲/۵٪ و تلورانس ۳۵٪ اثربخشی فریب را محدود می کند.
کلید واژه ها - سیستم موقعیت یاب جهانی، سیگنال فریب، ضد فریب، تبدیل موجک.

۱. مقدمه

متنوعی برای مقابله با فریب ارائه و نمونه های عملی آن ساخته شده است [۳]. قدم نخست در این مسیر شناسایی فریب و به عبارتی تشخیص وجود سیگنال فریب است [۴]. پس از آن که حمله فریب آشکار شد، مرحله بعد که قدم اصلی نیز می باشد، جبران سازی یا کاهش آن است.

در این مقاله روش جدیدی برای کاهش فریب در گیرنده های تک فرکانسه با استفاده از تبدیل موجک ارائه شده است. در ادامه ابتدا مرور مختصری به روش های مطرح شده برای کاهش فریب خواهیم داشت. پس از آن ابزار تبدیل موجک را معرفی می نماییم. در بخش ۴ به توضیح ایده ی روش پیشنهادی و طرز عملکرد آن خواهیم پرداخت. سپس آزمون های انجام شده برای ارزیابی عملکرد الگوریتم ارائه شده شرح داده می شوند. در نهایت بخش ۶ شامل نتیجه گیری و مقایسه کیفی با کارهای قبلی و پیشنهاد برای کارهای آتی می باشد.

۲. مروری بر روش های کاهش فریب

مقالات زیادی در رابطه با فریب این سیستم، آشکارسازی و

مکان یابی، ناوبری و سیستم های وابسته به GPS نقش بسزایی در زندگی روزمره ی ما دارند. از این رو امنیت و صحت عملکرد این سیستم ها، دارای اهمیت ویژه ای می باشند. در دو دهه اخیر امنیت سیستم های مبتنی بر GPS مورد تردید قرار گرفته است [۱]. هر نوع حمله فریب متناسب با روش مورد استفاده و دقت عملکرد آن، محدوده مشخصی به عنوان ناحیه هدف دارد. مشخصات سیگنال های فریب تولید شده در این ناحیه در حد قابل قبولی با نمونه معتبر تطابق دارد و در نتیجه گیرنده از حضور آن بی خبر می ماند.

اغلب گیرنده های GPS قادرند فریب هایی را که در خارج از ناحیه هدف قرار دارند، شناسایی کنند. اما در فضای محدود به ناحیه هدف، گیرنده قادر به تفکیک سیگنال های معتبر و جعلی نیست و با توجه به توان بزرگ تر سیگنال فریب، گیرنده آن را به جای سیگنال اصلی ردیابی و پردازش می کند [۲]. برای حل این مشکل مطالعات گسترده ای در حال انجام است و روش های

کاهش فریب ارائه شده است [۴-۶]. بخشی از روش های موجود مقابله با فریب که در ابتدای تحقیقات در این زمینه بیش تر مورد توجه واقع شد، بر مبنای مقایسه و بررسی مداوم اطلاعات داخلی و خارجی و تخمین سیگنال معتبر در صورت تشخیص وجود حمله، عمل می کنند [۷-۹].

در مرجع [۹] برای گیرنده در دو حالت عمل کردی در نظر گرفته شده است. به این ترتیب که در شرایط عادی داده های دریافتی خود را معتبر می داند و در حالت هوشیار^۱ اطلاعاتی را که از تخمین گر پیش بینی کننده خود دریافت می کند، برای مکان یابی مورد استفاده قرار می دهد. وقتی که علائم مشکوک از بین رفت، گیرنده به حالت عادی برمی گردد. پیش بینی در این سیستم توسط فیلتر کالمن و حسگرهای داخلی انجام می شود. فیلتر کالمن تخمین دقیق تری را نتیجه می دهد و با گذشت زمان و با طولانی شدن حالت هوشیار، خطای کمتری ایجاد می کند.

مشخصه هایی که این روش تخمین می زند، به طور نمونه عبارتند از مکان، آفست کلاک و انتقال داپلر. در بین آن ها معمولاً مشخصه داپلر نتیجه بهتری دارد، زیرا تغییرات آن آرام تر است و امکان پیش بینی آن با خطای ثابت و کوچک در دوره طولانی از زمان وجود دارد، در حالی که خطای مکان به صورت نمایی افزایش می یابد. به این ترتیب گیرنده هدف در صورت تشخیص حمله فریب، با پیش بینی مقدار انتقال یا تغییر داپلر، فرکانس سیگنال خود را متناسب با آن تنظیم می کند.

علاوه بر آن چون فریب دهنده روی زمین قرار دارد و با سرعت کمتر از ماهواره حرکت می کند، نمی تواند انتقال داپلر یکسانی با سیگنال اصلی ایجاد کند. مگر این که فرکانس انتقال خود را برای تطبیق با یکی از گیرنده ها تغییر دهد که در این صورت با حمله پیچیده روبه رو هستیم.

به دلیل محدودیت های عملی، معمولاً فرستنده های فریب، به جز فریبنده های ماهر، چندین سیگنال جعلی را از یک آنتن می فرستند در حالی که سیگنال های معتبر GPS از ماهواره های مختلف در مسیرهای گوناگون فرستاده می شوند. از این رو می توان روش پردازش فضایی را برای تخمین اثر سه بعدی سیگنال های دریافت شده و تفکیک این سیگنال ها که رابطه فضایی مشخصی دارند، به کار گرفت [۱۰-۱۳]. به این روش تکنیک زاویه ورود نیز می گویند و بر مبنای این واقعیت، یکی از روش های معتبر و معمول برای شناسایی و کاهش فریب محسوب می شود. برای اجرای آن به داشتن آرایه ای از آنتن نیاز است. یک آرایه آنتن

می تواند توزیع فضایی سیگنال دریافتی را تخمین بزند و سیگنال دریافتی از فرستنده معتبر را از نمونه متناظر جعلی تفکیک کند. سه روش متفاوت برای پیاده سازی آرایه مورد نیاز پیشنهاد شده است.

گیرنده چندآنتنه می تواند روش های پردازش آرایه ای را به دلیل شکل دهی پرتو به کار گیرد و بعد از آشکارسازی مسیر سیگنال فریب دهنده، این گیرنده می تواند صفری^۲ را به سمت منبع فریب هدایت کند و اثر مخرب آن را متوقف کند. با به کارگیری این بردار بهره برای سیگنال نمونه برداری شده، سیگنال فریب دهنده بعد از ترکیب صحیح سیگنال ها برای شاخه های مختلف آنتن حذف می شود [۱۱]. شمای کلی سیستم مقابله با فریب در شکل ۱ نشان داده شده اند.

آرایه دو آنتنه در مرجع [۱۲]، سیگنال های دریافتی از آنتن های مختلف را با همبستگی متقابل، شناسایی و اثر سه بعدی سیگنال های فریب را بر مبنای نفوذ توان فضایی شان استخراج می کند. این روش به کالیبراسیون آرایه آنتن یا هر اطلاعات قبلی راجع به آرایه جهت یابی آنتن نیاز ندارد و می تواند به عنوان یک آنتن سری مستقل ترکیب شده با بلوکی که سیگنال های فریب را قبل از ورود به گیرنده های متعارف GPS کاهش می دهد، استفاده شود. این روش ضد فریب اثر سیگنال فریب را تا زمانی که توان آن به طور قابل ملاحظه ای از توان میانگین سیگنال معتبر بیشتر باشد، با موفقیت کاهش می دهد.

با تغییر مکان آنتن گیرنده منفرد در طول یک بازه زمانی کوتاه، می توان آرایه آنتن مصنوعی تولید کرد. گیرنده دستی قابل حمل در مرجع [۱۳] به طور تصادفی جابجا شده و در هر لحظه سیگنال های GPS را دریافت و ذخیره می نماید. مجموعه داده ای که به این روش جمع آوری می شود با برخی ملاحظات اضافی می تواند به عنوان داده حاصل از آرایه آنتن چندمسیری تلقی شده و برای تفکیک سیگنال معتبر و جعلی مورد استفاده قرار گیرد. البته روش پردازش فضایی در حالت کلی ممکن است در مقابل فریب پیچیده چندآنتنه کارایی نداشته باشد. در کنار کارایی مناسب، این روش پیچیدگی سخت افزاری و پردازشی گیرنده را به طور قابل ملاحظه ای افزایش می دهد.

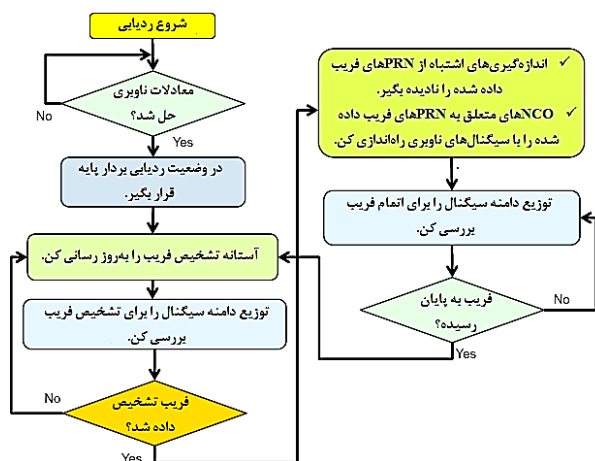
یک روش دیگر به نام نظارت یک پارچه مستقل گیرنده^۳ (RAIM) برای آشکارسازی و کاهش فریب در سطح ناوبری و مسائل مکان یابی ارائه شده است [۱۴]. روش RAIM، دفاعی

^۲ Null

^۳ Receiver Autonomous Integrity Monitoring

^۱ Alert

بگیرد و از اندازه‌گیری‌های سطح ناوبری برای راه‌اندازی NCOها، استفاده کند. این حالت باقی می‌ماند تا پیک همبستگی فریب دور شود و همبسته‌ساز به فرآیند عادی ردیابی سیگنال اصلی بازگردد. شکل ۲ مراحل مختلف این الگوریتم را نشان می‌دهد [۱۵].



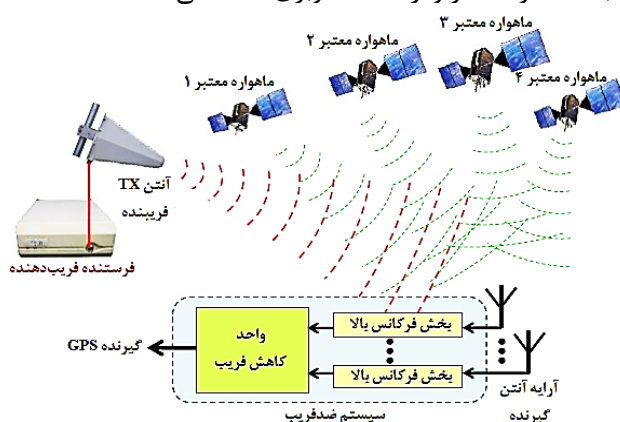
شکل ۲: عمل کرد ضد فریب پیشنهادی گیرنده VB [۱۵].

۳. تبدیل موجک

امروزه تبدیل موجک در کاربردهای وسیعی از ریاضیات و علوم مهندسی به کار می‌رود. ظهور این ابزار ریاضی قدرتمند در حوزه پردازش سیگنال به عنوان مهم‌ترین اتفاق در این حوزه پس از تبدیل فوریه محسوب می‌شود. در واقع تبدیل موجک اجازه دسترسی و مطالعه هم‌زمان فرکانس و زمان را در یک سیگنال به ما می‌دهد. این تبدیل، ویژگی‌های محلی و موضعی یک سیگنال را با اتساع و جابجایی یک پنجره‌ی تطبیقی آشکار می‌سازد که این پنجره‌ی تطبیقی یک شبه‌موج^۴ است. تبدیل موجک، ایده‌ی پردازش تکه‌ای در تبدیل فوریه زمان کوتاه^۵ (STFT) را پرورش می‌دهد و بر نقاط ضعفی مانند عدم تغییر اندازه‌ی پنجره STFT با فرکانس و عدم وجود پایه‌ی متعامد گسسته برای STFT، غلبه می‌کند [۱۶].

تبدیل موجک دو فرآیند را بر روی شبه‌موجی که به عنوان شبه‌موج مادر در نظر گرفته می‌شود، اعمال می‌کند. فرآیند نخست انتقال و جابجایی شبه‌موج منتخب در طول سیگنالی است که می‌خواهیم از آن تبدیل موجک بگیریم و فرآیند دوم فشردگی و گسترده سازی و تکمیل فرآیند تبدیل موجک است. به عبارت دیگر، در روند اجرای تبدیل موجک، شبه‌موج مادر در مقیاس‌های مختلف در طول سیگنال جایجا

عملی در مقابل خطای اندازه‌گیری‌های شبه‌فاصله در گیرنده GPS مستقل است که از طریق فرضیه آماری، خطای اندازه‌گیری شبه‌فاصله را آشکار و از مسئله ناوبری حذف می‌کند.



شکل ۱: سیستم ضد فریب با آرایه آنتنی [۱۱].

روش‌های نظارت دامنه نیز برای آشکارسازی حملات فریب بر روی یک گیرنده دنبال‌کننده^۱ کلی، مورد استفاده قرار می‌گیرند. برای جبران‌سازی فریب در طول تداخل سیگنال اصلی و فریب، گیرنده باید توانایی بازبایی سیگنال ازدست‌رفته را داشته باشد. برای رسیدن به این هدف ساختار ردیابی بردار-پایه (VB) استفاده می‌شود. ایده اصلی در این روش، ترکیب پاسخ ناوبری و تحمیل سیگنال ردیابی برای افزایش قدرت گیرنده‌های GPS و حفظ آن‌ها در برابر تداخل است.

یک گیرنده VB زنجیره‌ای می‌تواند نتایج سطح ناوبری و اندازه‌گیری حلقه‌های ردیابی برای راه‌اندازی نوسان‌ساز کنترل‌شونده عددی^۲ (NCO) هر نویز شبه تصادفی^۳ (PRN) را ذخیره کند. به عبارتی دیگر، این گیرنده‌ها می‌توانند به‌طور کلی اندازه‌گیری‌ها را از حسگرهای متفاوت جمع‌آوری نمایند. بنابراین در صورتی که تعدادی از اندازه‌گیری‌های اصلی در اثر حمله فریب دچار خطا شوند، گیرنده VB هنوز می‌تواند بر اساس یک جواب ناوبری معتبر، NCOهای متشابه را راه‌اندازی و فاصله تداخل سیگنال اصلی و فریب را متصل نماید و سرانجام پیک همبستگی اصلی را بعد از این که پیک فریب دور شد، جبران نماید.

ساختار آشکارسازی فریب بر روی خروجی‌های همبسته‌ساز و پرچم‌ها در حضور یک سیگنال فریب به محض مشاهده توزیع غیرعادی هر خروجی همبسته‌ساز، عمل می‌کند. سیستم ضد فریب باید اندازه‌گیری‌های محل، فیلترهای حلقه را نادیده

¹ Tracking Receiver² Numerically Controlled Oscillator³ Pseudo-Range-Noise[‡] Wavelet^Δ Short Time Fourier Transform

$$\psi_{m,n} = 2^{-m/2} \psi(2^{-m}t - n) \quad (4)$$

$$x(t) = \sum_{m=-\infty}^{\infty} \sum_{n=-\infty}^{\infty} T_{m,n} \psi_{m,n}(t) \quad (5)$$

نکته قابل توجه این که شبه موج های گسسته شبکه ی دودویی، متعامد با یکدیگر و نرمالیزه شده به انرژی واحد انتخاب می شوند. این تعامد، ضرب داخلی هر شبه موج را با بقیه ی شبه موج ها صفر می کند. در این حالت، اطلاعات نهفته در هر ضریب موجک منحصربه فرد خواهد بود و در هیچ ضریب دیگر تکرار نخواهد شد. تحت این شرایط است که بازسازی سیگنال اولیه بدون هیچ گونه افزونگی^۳ میسر خواهد بود [۱۷].

۴. روش پیشنهادی

همان طور که در بخش قبلی اشاره شد، تبدیل موجک ابزاری کارا برای تحلیل سیگنال های GPS شناخته شده است [۱۸-۲۱]. در این مقاله روشی جدید برای پردازش داده ی GPS براساس تبدیل موجک ایستا^۴ (SWT) پیشنهاد شده است. در واقع ما نویززدایی را در فرآیند کاهش فریب بر اساس SWT اجرا می کنیم. استفاده از این تبدیل موجک به جای نمونه استاندارد باعث می شود سیگنال مورد نظر که SWT روی آن اعمال شده است، دارای ضرایبی در حوزه ی ضرایب تبدیل موجک باشد که تعداد آن ها بیش از تعداد مورد نیاز برای بازسازی سیگنال اصلی است. به این ترتیب در انتخاب ضرایبی که برای بازسازی سیگنال به کار می روند، گزینه های بیشتری برای انتخاب فراهم می شود تا بتوان با انتخاب مناسب ضرایب، کارایی روش را بهبود داد.

۱.۴. اساس نویززدایی با استفاده از تبدیل موجک

تغییرات اعمالی بر مقادیر ضرایب موجک برای کاهش نویز، نویززدایی^۵ نام دارد. یکی از خواص برجسته ی تبدیل موجک، توانایی متمرکز کردن آن است. سیگنال های مورد استفاده در اغلب کاربردها، دارای تنها چند ضریب متناظر در حوزه ی ضرایب موجک هستند که بخش اعظم انرژی سیگنال را شامل می شوند. از طرف دیگر، نویز اضافه شونده معمولاً سفید در نظر گرفته می شود. سفید بودن نویز باعث می شود که ضرایب مربوط به نویز در تمام فرکانس ها پراکنده باشند. در نتیجه نویز سفید و شبه موج انتخاب شده خوب انطباق نمی یابند و ضرایب موجک

میزان انطباق آن در هر لحظه و مقیاس خاص با سیگنال مورد نظر محاسبه می گردد. میزان انطباق به دست آمده همان مقدار تبدیل موجک در آن لحظه و مقیاس خاص است. به این ترتیب، محاسبات در مقیاس ها و جابجایی های مختلف، تبدیل موجک یک سیگنال را نتیجه می دهد. این تبدیل به دو صورت پیوسته و گسسته قابل پیاده سازی است که در ادامه هر یک به طور مختصر معرفی می شود.

۱.۳. تبدیل موجک پیوسته

در صورتی که انتقال و جابجایی شبه موج حامل به ازای تمام حالت های ممکن انجام شود، تبدیل انجام شده تبدیل موجک پیوسته^۱ (CWT) نامیده می شود. در حالت کلی CWT به صورت زیر محاسبه می شود:

$$T(a,b) = \frac{1}{\sqrt{a}} \int_{-\infty}^{\infty} x(t) \psi\left(\frac{t-b}{a}\right) dt \quad (1)$$

که در آن $x(t)$ سیگنال مورد نظر برای اعمال تبدیل موجک، $\psi(t)$ شبه موج مادر، a عامل اتساع و انقباض و b عامل جابجایی است. a و b مقادیر عددی اختیاری هستند ($a \neq b$). برای بیان CWT به صورت فشرده می توان از ضرب داخلی بهره برد:

$$T(a,b) = \langle x, \psi_{a,b} \rangle \quad (2)$$

۲.۳. تبدیل موجک گسسته

در تبدیل موجک گسسته^۲ (DWT) تنها از برخی ضرایب مقیاس بندی بهره می گیرند. می توان نشان داد که اگر از ضرایب توان^۲ استفاده شود، نتیجه مطلوبی بدست می آید. از آن جا که محاسبه ضرایب به ازای همه حالت های ممکن مقیاس بندی و انتقال در CWT زمان بر است، بازسازی سیگنال اصلی در DWT راحت تر و سریع تر از تبدیل موج پیوسته انجام می شود. از این رو جهت بازسازی بی نقص سیگنال اصلی بیشتر از DWT استفاده می شود. گسسته سازی پارامترهای جابجایی و اتساع از طریق مقیاس بندی به صورت لگاریتمی در پایه ی دو، یک شبکه دودویی به وجود می آورد. با در نظر گرفتن این شبکه ی دودویی، DWT به صورت زیر نشان داده می شود:

$$T_{m,n} = \int_{-\infty}^{\infty} x(t) \psi_{m,n}(t) dt \quad (3)$$

که در آن داریم:

^۳ Redundancy

^۴ Stationary Wavelet Transform

^۵ De-noising

^۱ Continuous Wavelet Transform

^۲ Discrete Wavelet Transform

لازم به ذکر است که تخمین مقادیر واقعی سیگنال در هر دو سطح سیگنال و ضرایب امکان پذیر است. روش های مختلفی برای اعمال به ضرایب سیگنال مانند روش minimax طرح شده اند که تقریب قابل قبولی از سیگنال اصلی ارائه می دهند [۲۱-۲۲].

۲.۴. تبدیل موجک ایستا

ایده ی اساسی SWT، یافتن راهی برای پرکردن فضای ایجاد شده در گام کم نمونه برداری^۲ در تبدیل موجک است که یک تجزیه ی دارای ضرایب اضافی را نتیجه می دهد. افزودن ضرایبی در تبدیل موجک استاندارد به این دلیل است که در آن خروجی فیلتر در هر سطح کم نمونه برداری می شود. برخلاف آن در SWT، فیلترها در هر سطح بیش نمونه برداری^۳ می شوند.

در تبدیل موجک استاندارد با افزایش سطوح، سیگنال تولیدی در هر سطح طول کوتاه تری خواهد داشت. در حالی که حذف فرآیند کم نمونه برداری در SWT به تولید سیگنال هایی با طول یکسان با سیگنال ورودی در هر سطح می انجامد.

با در نظر گرفتن سیگنال ورودی $x[n]$ با طول M که $M=2^J$ (J عدد صحیح است)، برای اعمال SWT، فیلترهای پایین گذر $h[n]$ و بالاگذر $g[n]$ به کار می روند. در گام نخست تبدیل، سیگنال ورودی در حالی به فیلترها اعمال می شوند که بعد از فیلتر کردن هیچ فرآیند کم نمونه برداری دنبال نمی شود. در نتیجه، ضرایب تقریب $a_1[n]$ و ضرایب جزئیات $d_1[n]$ از روابط زیر به دست می آیند:

$$a_1[m] = \sum_l h_1[m-1]x[l] \quad (9)$$

$$d_1[m] = \sum_l g_1[m-1]x[l] \quad (10)$$

در گام دوم، ضرایب تقریب به دست آمده به فیلترهایی اعمال می شوند که از بیش نمونه برداری فیلترهای گام نخست حاصل شده اند. به این ترتیب با تکرار پی در پی این روند، ضرایب SWT محاسبه می شوند:

$$a_{j+1}[m] = \sum_l h_{j+1}[m-1]a_{j+1}[l] \quad (11)$$

$$d_{j+1}[m] = \sum_l g_{j+1}[m-1]a_{j+1}[l] \quad (12)$$

که در آن $j = 1, 2, \dots, j_0-1$ و h_{j+1} و g_{j+1} به ترتیب بیش نمونه برداری شده h_j و g_j هستند. شکل ۳ نتیجه SWT

مربوط به نویز دارای دامنه های کوچک خواهند بود. بنابراین، اجزای نویز یک سیگنال در تمام جزئیات^۱ پخش می شوند. این ویژگی منحصربه فرد امکان تفکیک سیگنال اصلی از نویز را به کمک تبدیل موجک فراهم می آورد. نویززدایی با استفاده از تبدیل موجک شامل سه گام اصلی می شود [۲۲]:

گام ۱: تجزیه ی سیگنال ورودی با طول M در سطح N با استفاده از موجک منتخب.

گام ۲: آستانه گذاری و تغییر ضرایب با استفاده از یک روش اختیاری [۲۳-۲۴].

گام ۳: بازسازی ضرایب تغییر یافته برای بازیابی یک سیگنال نویززدایی شده که تقریبی از سیگنال اصلی بدون نویز ناشناخته است. برای سیگنالی که نویز سفید به آن اضافه شده است، داریم:

$$x(i) = s(i) + \sigma n(i); i = 1, 2, \dots, N \quad (6)$$

که در آن $s(i)$ سیگنال اصلی بدون نویز است که مجهول می باشد. N نشان دهنده ی طول سیگنال، $x(i)$ سیگنال نویزی، $n(i)$ نویز سیگنال و δ انحراف معیار نویز است. با فرض این که نویز سفید دارای توزیع گوسی با متوسط صفر است، انحراف معیار نویز باید تقریب زده شود. هدف از نویززدایی بازیابی سیگنال اصلی $s(i)$ از سیگنال نویزی $x(i)$ است. در نویززدایی قبل از هر چیز باید یک تابع هزینه تعریف شود که واریانس خطای تقریبی باشد. این تابع هزینه تفاوت بین مقدار محاسبه شده و مقدار واقعی مجهول خواهد بود. واریانس ضرایب از طریق کمینه کردن تابع هزینه تخمین زده می شود. بنابراین، می توان نوشت:

$$R(X, \hat{X}) = E\|(X - \hat{X})\|^2 \quad (7)$$

که در آن X مقدار واقعی سیگنال و $\hat{X}$ مقدار تقریبی است. برای تابع هزینه می توان نوشت:

$$R(X, \hat{X}) = E\|(X - \hat{X})\|^2 = E\|W^{-1}(C - \hat{C})\|^2 = E\|(C - \hat{C})\|^2 \quad (8)$$

البته رابطه بالا در صورت به دست آوردن ضرایب موجک سیگنال تحت شرایط تعامد، صادق است. اگر C و $\hat{C}$ به ترتیب مقادیر واقعی و تخمین زده شده ی ضرایب باشند، می توان نوشت:

$$C = WX \text{ or } X = W^{-1}C$$

^۲ Under-Sampling

^۳ Over-Sampling

^۱ Details

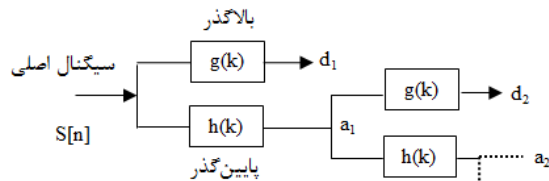
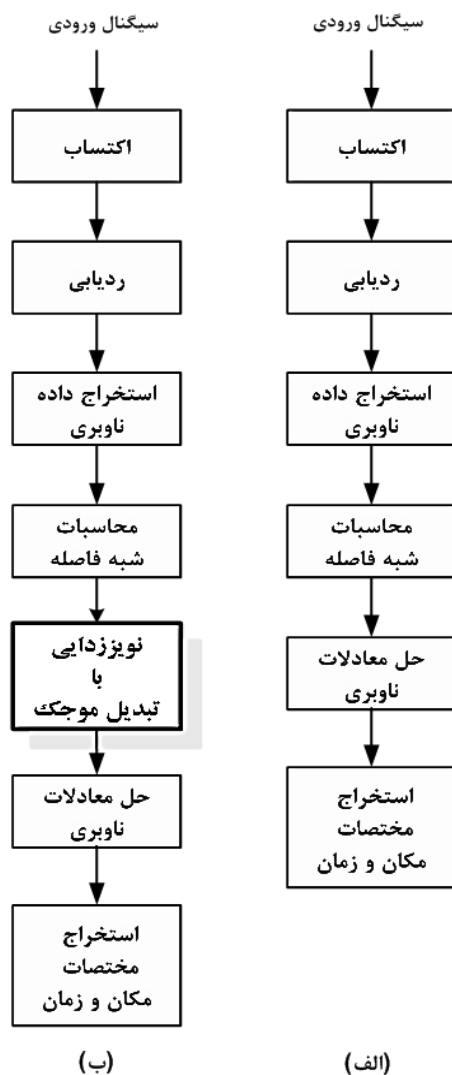
در این مرحله که تا حدود زیادی فارغ از تأثیرات فریب می باشند، مجدداً به فرآیند حداقل مربعات اعمال می شوند.

۵. شرح آزمون

در حالت کلی می توان مراحل فرآیند موقعیت یابی در گیرنده ی GPS تک فرکانسه را در شکل ۴-الف خلاصه کرد [۲۵]. در صورت ادغام الگوریتم تشریح شده در بخش قبل با گیرنده اصلی، فرآیند موقعیت یابی بر اساس ضدفریب در گیرنده ی GPS تک فرکانسه حاصل می شود که در شکل ۴-ب ترسیم شده است. با استفاده از گیرنده GPS نرم افزاری [۲۵] و چهار مجموعه داده که نحوه ی شکل گیری آن ها در بخش آتی آمده است، اثربخشی الگوریتم پیشنهادی آزموده می شود.

۱.۵. تولید داده فریب

ذخیره سازی و تأخیر در سیگنال حقیقی GPS به منظور تولید فریب در گذشته بررسی شده است [۹].



شکل ۳: SWT پیاده سازی شده به صورت بانک فیلتر [۱۶-۱۷].

۳.۴. روش پیشنهادی برای گیرنده ی ساکن

با تحلیل و بررسی اثر فریب در گیرنده نرم افزاری، می توان پی برد که عمده اثرگذاری حمله فریب در مقدار شبه فاصله و مکان ماهواره ها مشاهده می شود. با توجه به این که معادلات ناوبری و استخراج مختصات مکان و زمان بر مبنای این مشخصات انجام می شوند، این مسئله منجر به ایجاد تفاوت در مکان نهایی بدست آمده برای گیرنده نسبت به مقدار واقعی آن می گردد که به عنوان فریب شناخته می شود [۹]. با توجه به تأثیر بیشتر تغییرات شبه فاصله نسبت به تغییرات مکان ماهواره ها، فرآیند کاهش فریب با اعمال پردازش بر روی مشخصه شبه فاصله ماهواره ها آغاز می گردد که عبارت است از نویز زدایی شبه فاصله با اعمال SWT. استخراج و کاهش فریب با استفاده از SWT از چهار گام اساسی تشکیل می شود:

گام ۱: اعمال باقی مانده های شبه فاصله به SWT.

گام ۲: تغییر در ضرایب بدست آمده از مرحله ی قبل با استفاده از روش آستانه گذاری.

گام ۳: بازسازی ضرایب حاصل از گام دوم.

گام ۴: اعمال مقدار فریب استخراج شده به شبه فاصله اولیه. در گام دوم برای تغییر در ضرایب، روش آستانه گذاری خاصی بر اساس آنچه که پیش از این ذکر شده است، برگزیده می شود. به عبارت دیگر مبنای انتخاب آستانه گذاری روش اصلاح ضرایب و مدل نویز در نظر گرفته می شود. با توجه به این که در این تحقیق از SWT بهره برده ایم، فرآیند بازسازی در گام سوم متفاوت از فرآیند مشابه در تبدیل موجک استاندارد خواهد بود. زیرا که SWT منجر به تولید فراوانی در ضرایب می شود. هم چنین لازم به ذکر است که به دلیل حذف نویز در این مرحله تنها خطای موجود، خطای فریب خواهد بود. برای حذف فریب، اختلال شبه فاصله مستخرج در گام سوم باید به طور مستقیم به شبه فاصله نخست اعمال شود. شبه فاصله های جدید بدست آمده

شکل ۴: مراحل فرآیند موقعیت‌یابی گیرنده‌ی GPS

تک‌فرکانسه: (الف) در شرایط عادی و (ب) پس از اعمال الگوریتم ضد فریب.

می‌دانیم در صورت داشتن گیرنده واقعی و وجود سیگنال واقعی GPS در محیط، پس از انتشار سیگنال تأخیر یافته در ورودی گیرنده واقعی مجموع دو سیگنال جعلی و معتبر دریافت می‌شود. با توجه به این نکته برای تولید سیگنال جعلی از سیگنال‌های واقعی جمع‌آوری شده، ابتدا از سیگنال معتبر دریافتی به مدت کافی نمونه‌برداری و سپس در فضای حافظه در دسترس ذخیره‌سازی کردیم و پس از ایجاد تأخیر مناسب، آن را برای ترکیب با سیگنال‌های حقیقی GPS منتشر نمودیم.

• مجموعه داده اول

مجموعه داده نخست با ایجاد تأخیر $2623/7$ ms توسط مکانیزم تأخیر و ترکیب ایجاد شده‌است. این مجموعه قادر به فریب ۱۹۲ متری گیرنده‌ی تک‌فرکانسه می‌باشد. با اعمال الگوریتم پیشنهادی توانستیم ۶۰ درصد از فریب این مجموعه را کاهش دهیم.

• مجموعه داده دوم

مجموعه داده دوم با ایجاد تأخیر $699/7$ ms توسط مکانیزم تأخیر و ترکیب ایجاد شده‌است. این مجموعه قادر به فریب ۲۸۰ متری گیرنده‌ی تک فرکانسه می‌باشد. با اعمال الگوریتم پیشنهادی توانستیم ۷۵ درصد از فریب این مجموعه را کاهش دهیم.

• مجموعه داده سوم

مجموعه داده سوم با ایجاد تأخیر $4330/8/5$ ms توسط مکانیزم تأخیر و ترکیب ایجاد شده‌است. این مجموعه قادر به فریب ۹۷۰ متری گیرنده‌ی تک‌فرکانسه می‌باشد. با اعمال الگوریتم پیشنهادی توانستیم ۷۵ درصد از فریب این مجموعه را کاهش دهیم.

• مجموعه داده چهارم

مجموعه داده چهارم با ایجاد تأخیر $12243/9$ ms توسط مکانیزم تأخیر و ترکیب ایجاد شده‌است. این مجموعه قادر به فریب ۱۱۴۰ متری گیرنده‌ی تک‌فرکانسه می‌باشد. با اعمال الگوریتم پیشنهادی توانستیم ۴۰ درصد از فریب این مجموعه را کاهش دهیم.

خلاصه نتایج بدست‌آمده از چهار آزمایش انجام‌شده در

جدول ۱ گزارش شده‌است. با دقت در مقادیر جدول مشخص می‌شود که استفاده از تبدیل موجک Bior 3.7 در سطح ۳، در بدترین حالت توانایی کاهش بیش از ۴۰ درصد از فریب ایجادشده را فراهم کرده است. به عبارت دیگر می‌توان گفت در حالت کلی با اعمال الگوریتم پیشنهادی در مجموعه مورد نظر توسط تبدیل موجک یادشده، قادر به کاهش بیش از ۴۰ درصدی فریب با تلورانس ۳۵ درصدی و میانگین $62/5$ درصدی هستیم.

بر پایه مطالب بیان‌شده، در این بخش تأثیر الگوریتم پیشنهادی را در دو مجموعه داده‌ای که کاهش فریب چشم‌گیری دارند، بررسی می‌کنیم. مجموعه داده‌ی سوم دارای فریب موثر ۹۷۰ متر می‌باشد. شکل ۵ تأثیر فریب ایجادشده بر مشخصه شبه‌فاصله را در این مجموعه داده نشان می‌دهد. در این شکل محور عمودی بیان‌گر اختلاف شبه‌فاصله در حالت حقیقی و فریب می‌باشد که عامل اصلی تغییر موقعیت حاصل در دو سیستم حقیقی و فریب می‌باشد. محور افقی نیز تعداد دفعات موقعیت‌یابی را در این آزمایش نشان می‌دهد.

این اختلاف برای تمامی ماهواره‌ها تقریباً ثابت می‌باشد. استفاده از تبدیل موجک Bior 3.7 در سطح ۳ توانایی کاهش ۷۵ درصد از فریب ایجادشده را فراهم می‌کند. برای نشان دادن میزان اثربخشی روش ارائه‌شده، در شکل ۶ اختلاف شبه‌فاصله را در مجموعه داده‌ی مورد نظر قبل و بعد از اعمال الگوریتم ضد فریب ترسیم کرده‌ایم. همان‌طور که از شکل نیز مشخص است کاهش اختلاف شبه‌فاصله به واسطه‌ی روش پیشنهادی ضد فریب محسوس است. در این شکل محور عمودی بیان‌گر اختلاف شبه‌فاصله بین حالت حقیقی و حالت فریب قبل و بعد از اعمال الگوریتم می‌باشد. محور افقی تعداد دفعات موقعیت‌یابی در این آزمایش را نشان می‌دهد. دو منحنی مربوط به اختلاف شبه‌فاصله بین سیستم حقیقی و سیستم فریب قبل و بعد از اعمال الگوریتم می‌باشند. با توجه به شکل، الگوریتم اعمال‌شده در تمامی لحظات اختلاف شبه‌فاصله دو سیستم حقیقی و فریب را یکسان کاهش نمی‌دهد، ولی در بیشتر موارد کاهش اختلاف شبه‌فاصله و نزدیک شدن آن به مقدار حقیقی (سطح صفر محور عمودی) مشخص است. به طور مشابه موجک مورد نظر توانایی کاهش ۷۵ درصدی فریب را در مجموعه داده‌ی دیگر دارد که دارای فریب موثر ۲۸۰ متر می‌باشد.

در شکل ۷ نیز می‌توان اثربخشی الگوریتم پیشنهادی را مشاهده کرد. همان‌طور که از شکل‌های ۶ و ۷ مشخص است رابطه مشخصی بین دفعات موقعیت‌یابی و اختلاف شبه فاصله

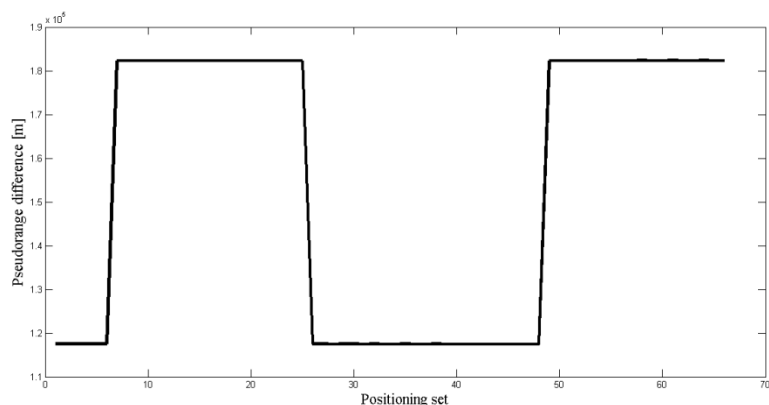
وجود ندارد، در عین حال میزان تغییرات خطای شبه‌فاصله بر اساس تعداد موقعیت شدید نیست.

۶. نتیجه‌گیری، مقایسه و پیشنهاد برای کارهای آتی

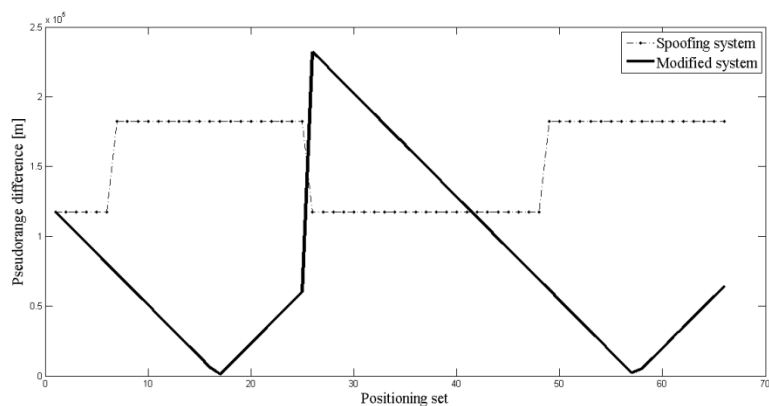
در این مقاله روشی برای مقابله با فریب ارائه شد که می‌تواند با بهره‌گیری از تبدیل موجک به‌طور قابل ملاحظه‌ای اثر فریب‌دهنده را در گیرنده GPS تک‌فرکانسه کاهش دهد. با توجه به این‌که اثر حمله فریب در مقادیر شبه‌فاصله محاسبه‌شده برای ماهواره‌ها به‌طور شهودی قابل درک است، عملیات کاهش بر روی مشخصه شبه‌فاصله پیاده‌سازی شد. سپس الگوریتم

جدول ۱: جزئیات عمل‌کرد الگوریتم کاهش فریب.

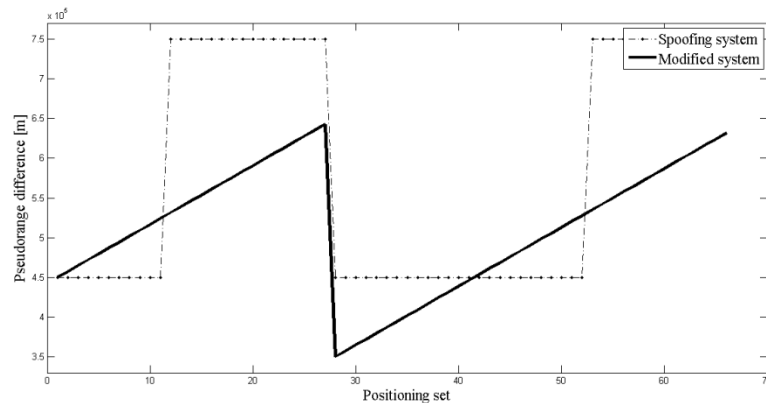
تبدیل موجک	سطح	متراف فریب				میانگین درصد کاهش	تلورانس درصد کاهش
		۱۹۲	۲۸۰	۹۷۰	۱۱۴۰		
		درصد کاهش					
Bior 3.7	۳	۶۰	۷۵	۷۵	۴۰	۶۲/۵	۳۵



شکل ۵: اختلاف شبه‌فاصله بین سیستم حقیقی و فریب برای مجموعه داده سوم.



شکل ۶: اختلاف شبه‌فاصله بین سیستم حقیقی و فریب قبل و بعد از اعمال الگوریتم ضد فریب برای مجموعه داده سوم.



شکل ۷: اختلاف شبه‌فاصله بین سیستم حقیقی و فریب قبل و بعد از اعمال الگوریتم ضدفریب برای مجموعه داده دوم.

سپاس‌گزاری

نویسندگان بر خود لازم می‌دانند تا از آقایان محمدجواد رضایی و محمدرضا آذرباد برای در اختیار قرار دادن تجربه‌هایشان تقدیر و تشکر کنند. همچنین از کارفرمایی که ما را مورد حمایت ارزشمند خود قرار داد، سپاس‌گزاریم.

مراجع

- [1] X. J. Cheng, K. J. Cao, J. N. Xu and B. Li, "Analysis on Forgery Patterns for GPS Civil Spoofing Signals," *The 4th International Conference on Computer Sciences and Convergence Information Technology (ICCIT '09)*. Korea, pp. 1-4, 2009.
- [2] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon and P. M. Kintner, "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," *ION GNSS. USA*, pp. 1-12, 2008.
- [3] T. E. Humphreys, J. Bhatti and B. Ledvina, "The GPS Assimilator: a Method for Upgrading Existing GPS User Equipment to Improve Accuracy, Robustness and Resistance to Spoofing," *The ION GNSS Conference. USA*, pp. 1-11, 2010.
- [4] امیررضا بازاریار، مریم معاضدی، سید محمدرضا موسوی میرکلایی و سید زمان غفاری، "ارائه روشی جدید برای آشکارسازی فریب GPS مبتنی بر اندازه‌گیری شبه‌فاصله به منظور استفاده در سامانه‌های ناوبری دریایی،" *مجله دریا فنون*، دانشگاه علوم دریایی امام خمینی (ره) نوشهر، جلد اول، شماره دوم، ص ۸-۲۱، ۱۳۹۳.
- [5] A. J. Jahromi, A. Broumandan, J. Nielsen and G. Lachapelle, "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques," *International Journal of Navigation and Observation*, Vol. 2012, pp. 1-16, 2012.
- [6] P. Zalewski, "Real-time GNSS Spoofing Detection in Maritime Code Receivers," *Scientific Journals*, Vol. 38, No 110, pp. 118-124, 2014.
- [7] M. H. Jin, Y. H. Han, H. H. Choi, C. Park, M. B. Heo and S. J. Lee, "GPS Spoofing Signal Detection and Compensation Method in DGPS Reference Station," *The 11th International Conference on Control, Automation and Systems (ICCAS)*. Korea, pp. 1616-1619, 2011.
- [8] Z. Lin, C. Haibin and Z. Naitong, "Anti-Spoofing Extended Kalman Filter for Satellite Navigation Receiver," *IEEE International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 996-999, 2007.
- [9] P. Papadimitratos and A. Jovanovic, "GNSS-Based Positioning: Attacks and Countermeasures," *IEEE Military Communications Conference. USA*, pp. 1-7, 2008.

نتایج حاصل نشان می‌دهند که با به کارگیری تبدیل موجک Bior 3.7 در سطح ۳ مقدار موثر فریب را با تلورانس ۳۵ درصد و میانگین ۶۲/۵ درصدی کاهش دادیم.

با توجه به نبود مراجع کافی برای این موضوع و عدم تشابه این روش به نمونه‌های موجود، امکان مقایسه کمی با کارهای قبلی وجود ندارد. به عنوان نمونه در مرجع [۱۱] سطح اکتساب ماهواره‌ها را نشان داده است که توانسته نمونه‌های جعلی را از فرایند پردازش خارج کند. در مرجع [۱۱] برای ارزیابی الگوریتم خود، توان سیگنال فریب را قبل و پس از اعمال روش ضدفریب گزارش کرده است که توانسته بود به مقدار ۱۱ dB آن را کاهش دهد. کارآیی روش مرجع [۱۵] نیز با گزارش تغییرات خطای مکان‌یابی بر حسب زمان سنجیده شده است. هرچند این روش عمل‌کرد قابل قبولی دارد، اما پیاده‌سازی آن نیاز به تغییر ساختار گیرنده دارد. در مرجع [۲۶] میزان کاهش فریب به درصد بیان شده است، اما نتیجه ارائه شده در آن از تحلیل آماری حاصل شده است و شبیه‌سازی یا آزمایش عملی برای آن انجام نشده است. با توجه به مطالب بیان شده، الگوریتم پیشنهادی با در نظر گرفتن پیچیدگی و هزینه اجرا، کارآیی بهتری در مقایسه با دیگر روش‌های ارائه شده دارد.

وجود اختلاف آشکار در کارآیی عمل‌کرد سیستم اصلاح شده به ازای آزمایش‌های مکرر، بیان‌گر این نکته است که عوامل موثر دیگر نیز وجود دارند که میزان فریب را تعیین می‌کنند. از این رو می‌توان در آینده برای بهبود کارآیی الگوریتم ضدفریب با تحقیق بیشتر، عوامل اثرگذار دیگر را مورد بررسی قرار داد. هم‌چنین در صورت استفاده از آشکارساز بلادرنگ می‌توان از اطلاعات ذخیره شده در گیرنده GPS قبل از شروع حمله فریب برای بهبود دقت الگوریتم استفاده نمود.

- [10] C. E. McDowell, "GPS Spoofer and Repeater Mitigation System Using Digital Spatial Nulling," U.S. Patent 7250903 B1, 31 July 2007.
- [11] S. Daneshmand, A. J. Jahromi, A. Broumandan and G. Lachapelle, "GNSS Spoofing Mitigation in Multipath Environments Using Space-Time Processing," *European Navigation Conference (ENC 2013)*, Austria, pp. 1-12, 2013.
- [12] S. Daneshmand, "GNSS Interference Mitigation using Antenna Array Processing," *Doctoral Dissertation, Department of Geomatics Engineering, University of Calgary, Alberta, Canada*, April 2013.
- [13] J. Nielsen, A. Broumandan and G. Lachapelle, "Spoofing Detection and Mitigation with a Moving Handheld Receiver," *GPS World Magazine*, Vol. 21, No. 9, pp. 1-5, 2010.
- [14] B. M. Ledvina, W. J. Bencze, B. Galusha and I. Miller, "An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers," *The 2010 International Technical Meeting of The Institute of Navigation*, USA, pp. 689-712, 2010.
- [15] A. J. Jahromi, "GNSS Signal Authenticity Verification in the Presence of Structural Interference," *Doctoral Dissertation, Department of Geomatics Engineering, University of Calgary, Alberta, Canada*, Sept. 2013.
- [16] C. S. Burrus, R. A. Gopinath and H. Guo, *Introduction to Wavelet and Wavelet Transforms: a Primer*, Prentice Hall, 1998.
- [17] P. S. Addison, *The Illustrated Wavelet Transform Handbook*, Institute of Physics Publishing, 2002.
- [18] M. R. Azarbad and 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.
- [19] M. R. Mosavi and M. R. Azarbad, "Multipath Error Mitigation Based on Wavelet Transform in L1 GPS Receivers for Kinematic Applications," *International Journal of Electronics and Communications*, Vol. 67, No. 10, pp. 875-884, 2013.
- [20] L. Musumeci and F. Dovis, "Use of the Wavelet Transform for Interference Detection and Mitigation in Global Navigation Satellite Systems," *International Journal of Navigation and Observation*, pp. 1-14, Feb. 2014.
- [21] A. I. Jumah, "Denoising of an Image using Discrete Stationary Wavelet Transform and Various Thresholding Techniques," *Journal of Signal and Information Processing*, Vol. 4, pp. 33-41, Feb. 2013.
- [22] 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.
- [23] D. Donoho, I. Johnstone, G. Kerkycharian and D. Picard, "Wavelet Shrinkage: Asymptopia?," *Journal of the Royal Statistical Society*, Vol. 57, No. 2, pp. 301-369, 1995.
- [24] E. M. Souza and J. F. G. Monico, "Wavelet Shrinkage: High Frequency Multipath Reduction from GPS Relative Positioning," *Journal of GPS Solution*, Vol. 3, NO. 8, pp.152-159, 2004.
- [25] K. Borre, D. M. Akos, N. Bertelsen, P. Rinder and S. H. Jensen, *A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach*, Birkhauser Engineering, 2007.
- [26] J. Nielsen, V. Dehghanian and G. Lachapelle, "Effectiveness of GNSS Spoofing Countermeasure Based on Receiver CNR Measurements," *International Journal of Navigation and Observation*, Vol. 2012, pp. 1-9, 2012.