

کاهش ابعاد تابع ابهام متقابل با استفاده از روش برش تصاویر برای شناسایی حمله فریب در سامانه GPS

کوروش زرین‌نگار^۱، سمیرا توحیدی^۲، سید محمدرضا موسوی میرکلایی^{۳*}، علی صدر^۴.

۱- دانشجوی کارشناسی ارشد، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران

۲- دانشجوی دکتری، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران

۳- استاد، نوسنده مسئول، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران

۴- دانشیار، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران

چکیده

سامانه‌های موقعیت‌یابی در مقابل انواع اختلال‌های عمدی و غیرعمدی آسیب‌پذیر می‌باشند. از این‌رو شناسایی و مقابله با انواع اختلالات در این سامانه حائز اهمیت می‌باشد. این مقاله یک روش کاهش ابعاد تصاویر تابع ابهام متقابل[†] (CAF) را در بهبود شناسایی اختلال فریب در سامانه موقعیت‌یابی جهانی[‡] (GPS) با استفاده از شبکه‌ی عصبی کانولوشنی بررسی می‌کند. نتایج حاصل از شبیه‌سازی روش پیشنهادی نشان می‌دهد که به ازای تصاویر CAF با ابعاد مختلف، شبکه عصبی کانولوشنی با بکارگیری الگوریتم کاهش ابعاد تصاویر، از نظر دقت و سرعت آموزش، عملکرد بهتری دارد. به طور میانگین، زمان همگرایی آموزش شبکه عصبی ۴۸٫۸٪ و میانگین دقت آموزش شبکه پس از همگرایی ۰٫۷۹٪ بهبود داشته است.

کلمات کلیدی: GPS، اختلال فریب، تابع ابهام متقابل، برش تصویر، شبکه عصبی.

۱. مقدمه

سامانه موقعیت‌یابی جهانی (GPS) یک سامانه ماهواره‌ای است که امروزه به‌طور گسترده‌ای به‌منظور موقعیت‌یابی و زمان‌سنجی مورد استفاده قرار می‌گیرد. GPS که در زمینه‌های مختلفی کاربرد دارد. این سامانه جزئی حیاتی از زیرساخت‌های ملی به حساب می‌آید و امنیت آن یک مسئله مهم است. سیگنال‌های GPS مسافتی طولانی را از ماهواره‌ها تا گیرنده‌ها طی می‌کنند، از این‌رو در سطح زمین توان بسیار پایینی دارند و در برابر انواع اختلالات ضعیف هستند. از این میان، حمله فریب به عنوان خطرناک‌ترین اختلال در سامانه GPS شناخته شده است. چراکه در این حمله، فریبنده سیگنالی که از نظر ساختاری کاملاً مشابه سیگنال اصلی GPS است را به سمت گیرنده منتشر می‌نماید و گیرنده را مجبور به موقعیت‌یابی

* Corresponding Author (Email: m_mosavi@iust.ac.ir)

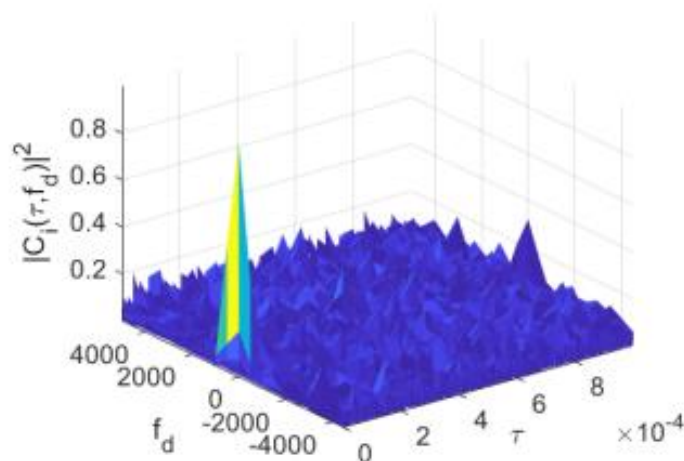
† Cross Ambiguity Function (CAF)

‡ Global Positioning System (GPS)

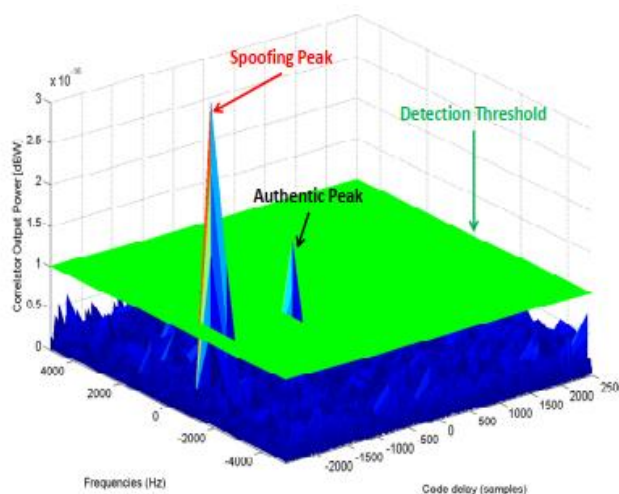
اشتباه می‌کند. به دلیل همین مشابهت در ساختار سیگنال اصلی و سیگنال فریب، آشکارسازی این اختلال بسیار حائز اهمیت است. در واقع، آشکارسازی تداخل فریب برای محافظت از سامانه‌های ناوبری اقدامی اساسی است [۲ و ۱]. در این مقاله، ابتدا ویژگی‌های مربوط به توابع ابهام متقابل در شناسایی فریب GPS توصیف شده است. سپس چگونگی استفاده از شبکه عصبی کانولوشنی برای دسته‌بندی کردن تصاویر CAF توضیح داده شده است. در ادامه روش برش تصویر هوشمند ارائه شده است که با اعمال این روش روی تصاویر CAF، نتایج عملکرد این روش با روش معمول مقایسه شده است. در پایان نیز نتیجه‌گیری و مراجع تحقیق بیان شده است.

۲. تابع ابهام متقابل

یکی از روش‌های آشکارسازی حمله فریب، آشکارسازی با استفاده از تابع ابهام متقابل است. این توابع در گیرنده‌های نرم‌افزاری پس از جستجوی دوبعدی در فرکانس داپلر و فاز کد به دست می‌آیند که اطلاعات مهمی از حضور سیگنال فریب در اختیار دارند. هنگامی که یک سیگنال فریب GPS وجود دارد، بیش از یک نقطه اوج در تصاویر CAF مشاهده می‌شود و اگر فقط سیگنال اصلی حضور داشته باشد، یک نقطه اوج در تصاویر CAF مشاهده می‌شود (مطابق شکل‌های ۱ و ۲). در واقع، این تابع دارای نقاط اوج بسیار زیادی است، اما تعداد نقاط اوج با دامنه‌های بالا و نزدیک به بیشینه تابع، حائز اهمیت می‌باشند و نشان‌دهنده حضور سیگنال اصلی و یا سیگنالی مشابه با سیگنال اصلی GPS هستند.



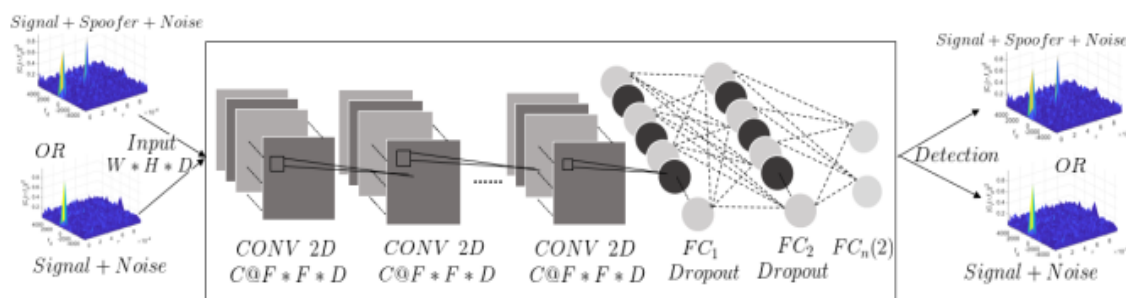
شکل ۱- تابع CAF در شرایط عدم حضور سیگنال فریب [۳].



شکل ۲- تابع CAF در شرایط حضور سیگنال فریب [۳].

۳. تشخیص فریب به کمک شبکه‌های عصبی

پژوهشگران در مقاله [۳] با استفاده از شبکه‌های عصبی چندلایه* (MLP) و شبکه‌های عصبی کانولوشنی† (CNN) و با بهره‌گیری از ویژگی نقاط اوج مربوط به تصاویر CAF، به شناسایی فریب پرداخته‌اند که نتایج حاصله، کارایی بهتر شبکه عصبی CNN را نشان می‌دهد. در واقع، از یک ساختار CNN پیچیده با ۱۳ لایه کانولوشن با دقت آموزش بالا برای دسته‌بندی سیگنال‌ها به دو دسته‌ی سیگنال فریب و سیگنال اصلی استفاده شده است. شکل ۳ طرح کلی آشکارسازی ارائه شده در روش مذکور را نشان می‌دهد [۴ و ۵].



شکل ۳- طرح تشخیص فریب با استفاده از ساختار CNN روش یادگیری عمیق [۳].

تصاویر CAF حجم و ابعاد بالایی دارند به گونه‌ای که تشخیص فریب با بهره‌گیری از CAF با استفاده از روش‌های هوش مصنوعی، نیاز به زمان آموزش زیاد و پردازش‌های عمیق می‌باشد. از طرفی، علاوه بر دقت تشخیص صحیح فریب، برای ما اهمیت دارد که زمان تشخیص صحیح فریب توسط شبکه‌های عصبی تا حد امکان کم باشد. بنابراین، به دنبال روش‌هایی هستیم تا زمان آموزش و دقت شبکه‌های عصبی عمیق را بهبود بدهیم.

* Multi-Layer Perceptron (MLP)

† Convolutional Neural Network (CNN)

۴. الگوریتم برش تصویر*

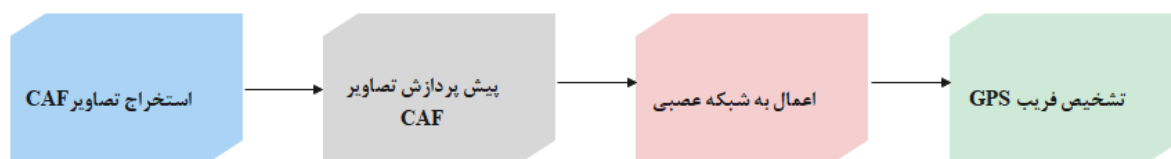
با پیشرفت سریع فناوری‌های تصویربرداری و ذخیره‌سازی، وضوح[†] پیکسلی تصاویر دیجیتال گرفته شده توسط دستگاه‌های تصویربرداری مدرن مانند وب‌کم، دوربین دیجیتال و تلفن همراه به طرز چشم‌گیری افزایش یافته است. روش برش تصاویر زمانی اهمیت یافت که کاربران دستگاه‌های تصویربرداری مدرن، تمایل داشتند هنگام گرفتن عکس، مقدار غیرضروری از پس‌زمینه یا مناظر غیر مرتبط را از تصویر مورد نظر حذف کنند. علاوه بر این، حذف پیکسل‌های کم‌اهمیت، مشکل انتقال تصاویر با حجم بالا را تا حدودی جبران کرد. برای حل این مشکلات، محققان تعدادی روش برش/تغییر اندازه تصویر به صورت هوشمند ارائه کرده‌اند. در شکل ۴ نمونه‌ای از این روش را مشاهده می‌کنید [۶-۹].



شکل ۴- نمونه‌ای از برش تصویر خودکار [۷].

۵. روش کار

در این مقاله، ابتدا تصاویر CAF از واحد اکتساب گیرنده GPS استخراج می‌شوند. سپس، روش برش تصویر به عنوان روش پیش پردازش پیشنهادی بر روی تابع CAF اعمال می‌شود. پس از آن، این تصاویر در شبکه عصبی CNN بررسی شده تا در مورد حضور و یا عدم حضور سیگنال تصمیم‌گیری شود. شکل ۵ بلوک دیاگرام کلی روش پیشنهادی آشکارسازی فریب را نمایش می‌دهد.

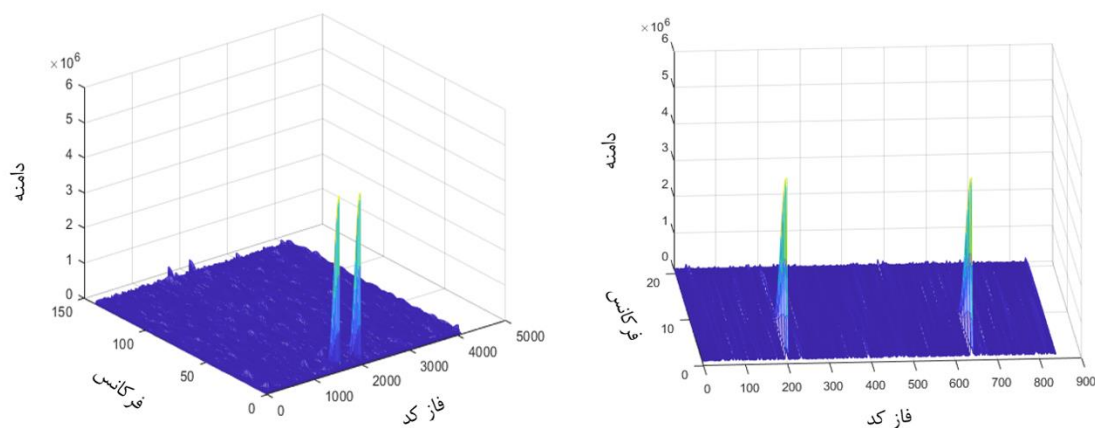


شکل ۵- مراحل کلی تشخیص فریب GPS

با اعمال روش برش تصویر بر روی تصاویر CAF، می‌توان ابعاد ماتریس CAF را تا حد زیادی کاهش داد. شکل ۶ روش برش تصویر را روی تصویر CAF در حضور سیگنال فریب نشان می‌دهد.

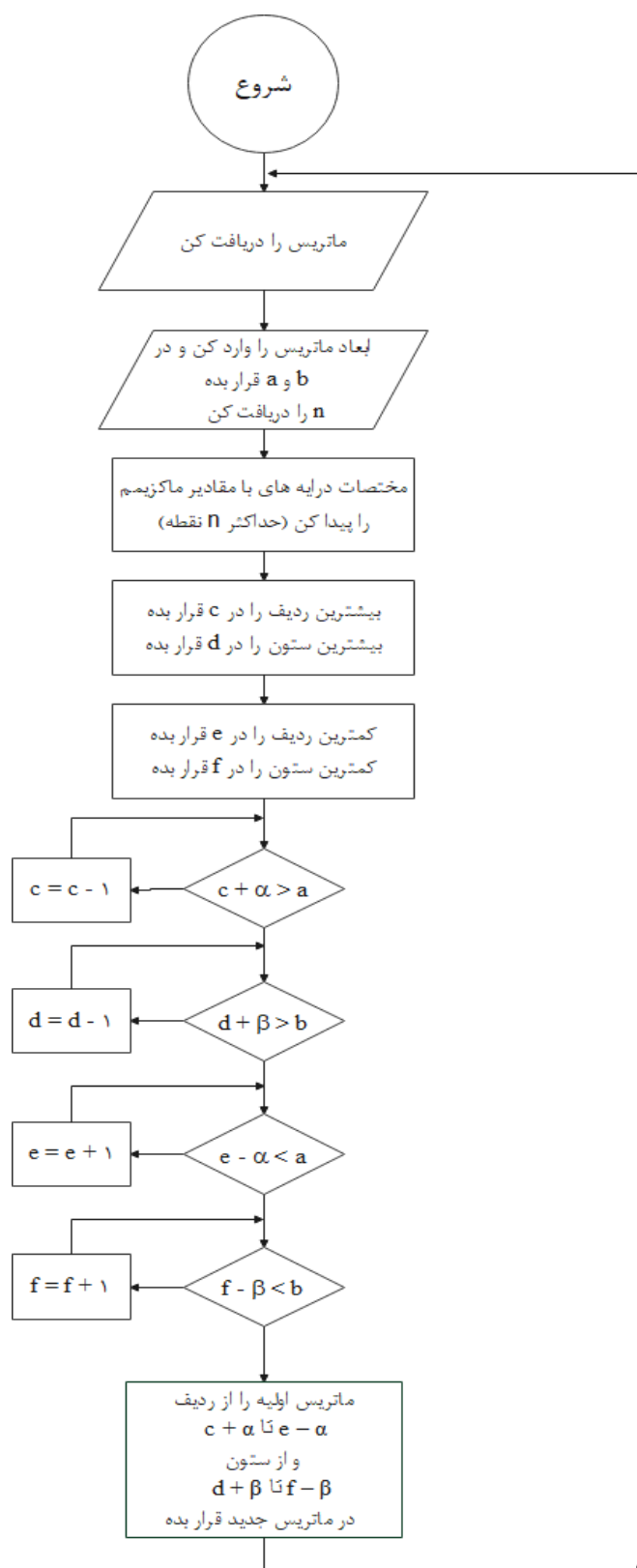
* Image Cropping

† Resolution



شکل ۶- تصویر CAF بدون استفاده از روش برش تصویر (سمت چپ) و تصویر CAF با اعمال روش برش تصویر (سمت راست).

همان‌طور که در شکل ۶ مشاهده می‌شود، تصویر CAF با ابعاد 141×4091 به تصویر CAF با ابعاد تقریباً 20×840 برش خورده است، درحالی‌که اطلاعات مهم خود را حفظ کرده است. انتظار داریم هر چه ابعاد تصاویر ورودی شبکه عصبی کمتر باشد، سرعت همگرایی شبکه به دقت مورد نظر بیشتر و زمان آموزش کمتر می‌شود. در بخش نتایج شبیه‌سازی، نشان خواهیم داد که دقت آموزش شبکه عصبی نیز افزایش می‌یابد. شکل ۷، بلوک دیاگرام روش برش تصاویر را نشان می‌دهد. این بلوک دیاگرام در نرم‌افزار متلب پیاده‌سازی شده است.



شکل ۷- بلوک دیاگرام روش برش تصاویر.

با توجه به الگوریتم برش تصاویر، با انتخاب مناسب α و β ، می‌توان حاشیه امن مناسب برای برش تصاویر ایجاد کرد، به‌گونه‌ای که اطلاعات مهم تصاویر که همان نقاط اوج هستند، از بین نرود.

۶. نتایج شبیه‌سازی

جهت شبیه‌سازی روش پیشنهادی از گیرنده نرم‌افزاری رادیو شناخت‌گر* (SDR) [۱۰] در محیط متلب استفاده شده است و رایانه‌ای با مشخصات پردازنده Core i7 10750 2.6 GHz 2.59 GHz، حافظه رم ۱۶ GB و کارت گرافیک RTX 1660 Ti بکار گرفته شده است. برای شناسایی فریب از شبکه عصبی کانولوشنی مشابه ساختار متداول VGG16 استفاده کردیم. این ساختار شامل ۱۳ لایه کانولوشن و ۳ لایه تمام متصل است. هر لایه کانولوشن توسط یک لایه نرمال‌ساز دسته‌ای[†]، تابع فعال‌ساز[‡] ReLu و لایه کاهش ابعاد ماکس پولینگ[§] دنبال می‌شود [۱۱]. همچنین هر لایه تمام متصل با تابع فعال‌ساز ReLu و لایه حذف تصادفی^{**} با احتمال ۰٫۵ دنبال می‌شود [۱۲ و ۱۳]. تصاویر CAF بدون حضور فریب دارای ابعاد 5714×141 و تصاویر CAF با حضور فریب دارای ابعاد 4092×141 هستند. همچنین برای کاهش بار محاسباتی، این تصاویر سه‌بعدی را به تصاویر دوبعدی سیاه و سفید تبدیل کردیم. در این صورت هر تصویر CAF به شکل ماتریس با ابعاد بیان شده و با مقادیر ۸ بیتی تبدیل می‌شوند. در این آزمایش از ۸۰۰ تصویر CAF جهت آموزش شبکه عصبی مذکور استفاده شده است که تعداد ۴۰۰ تا مربوط به سناریوهای با حضور سیگنال فریب و ۴۰۰ تای دیگر بدون حضور سیگنال فریب هستند. به دلیل تعداد زیاد داده‌ها، پیچیدگی ساختار شبکه عصبی کانولوشنی و ابعاد بالای تصاویر ورودی، تصاویر ورودی شبکه عصبی را دوباره کاهش ابعاد دادیم. لازم به ذکر است که شرایط شبیه‌سازی برای روش برش تصویر و بدون اعمال روش برش تصویر، کاملاً یکسان است. همچنین از بهینه‌ساز آدام^{††} برای بدست آوردن وزن‌ها و حد‌آستانه‌های شبکه عصبی استفاده شده است [۱۴ و ۱۵]. در شکل‌های زیر دقت و تلفات آموزش شبکه عصبی برای تصاویر ورودی CAF با ابعاد متفاوت نمایش داده شده است.

* Software-Defined Receiver (SDR)

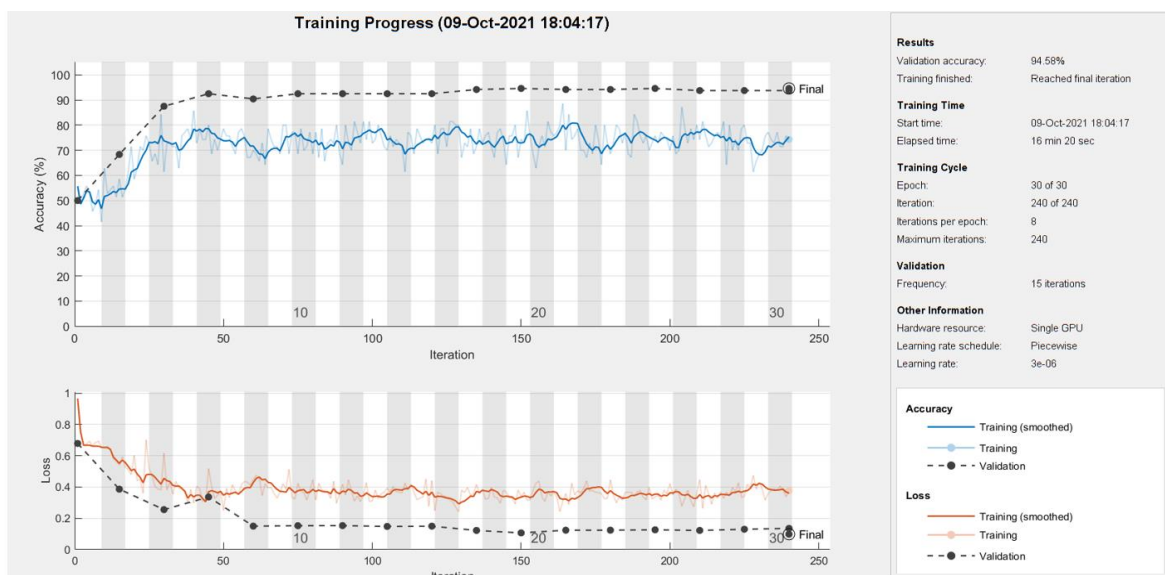
† Batch Normalization

‡ Rectified Linear Unit

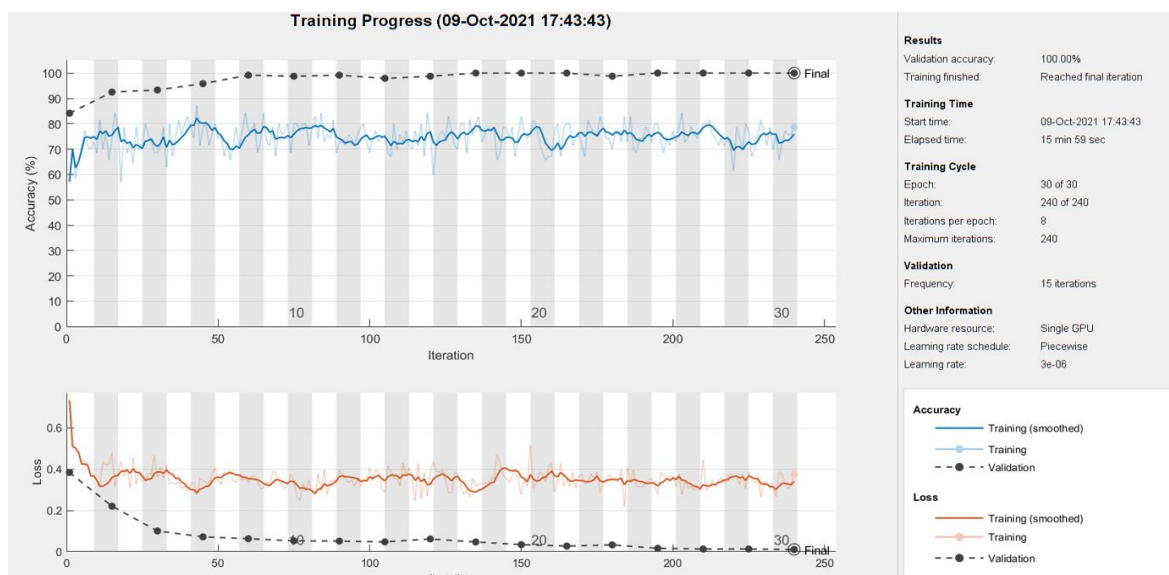
§ Max Pooling

** Dropout

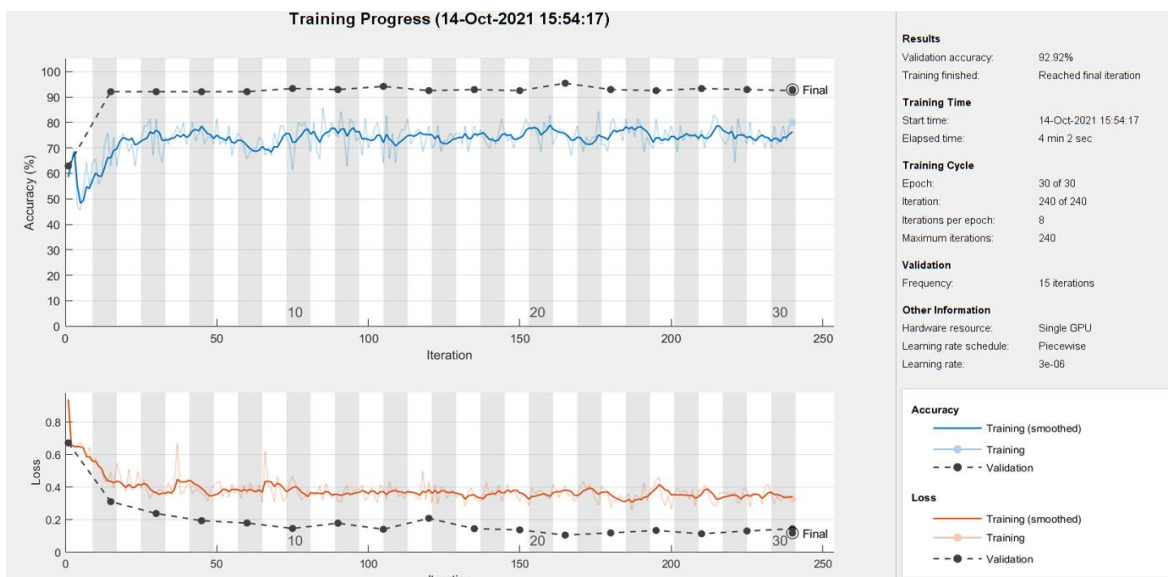
†† ADAM



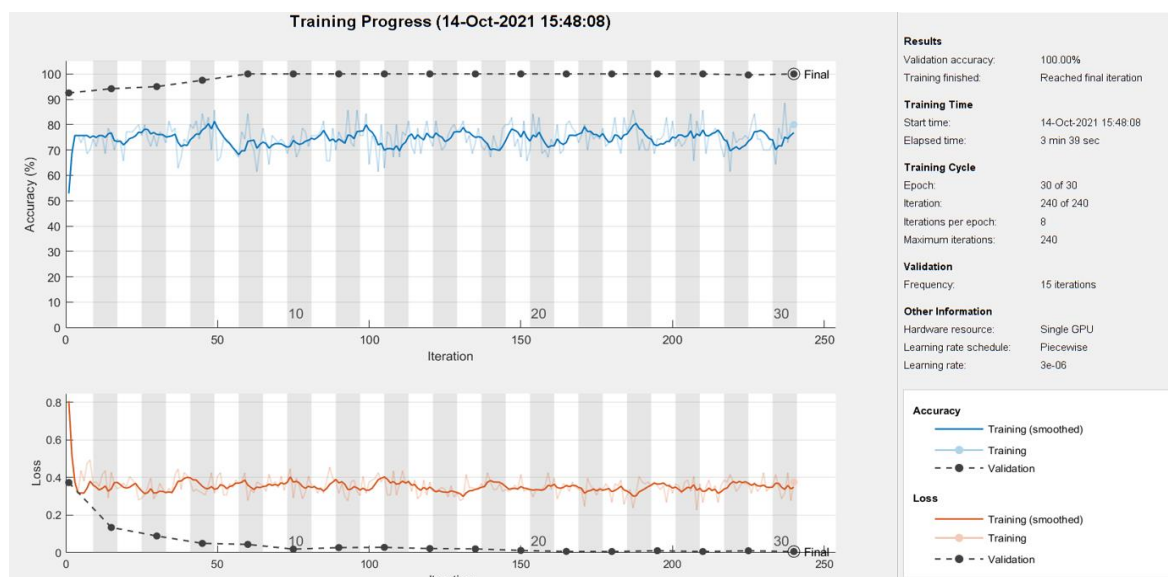
شکل ۸- دقت آموزش CNN بدون اعمال روش برش تصویر برای ابعاد ورودی 50×50 .



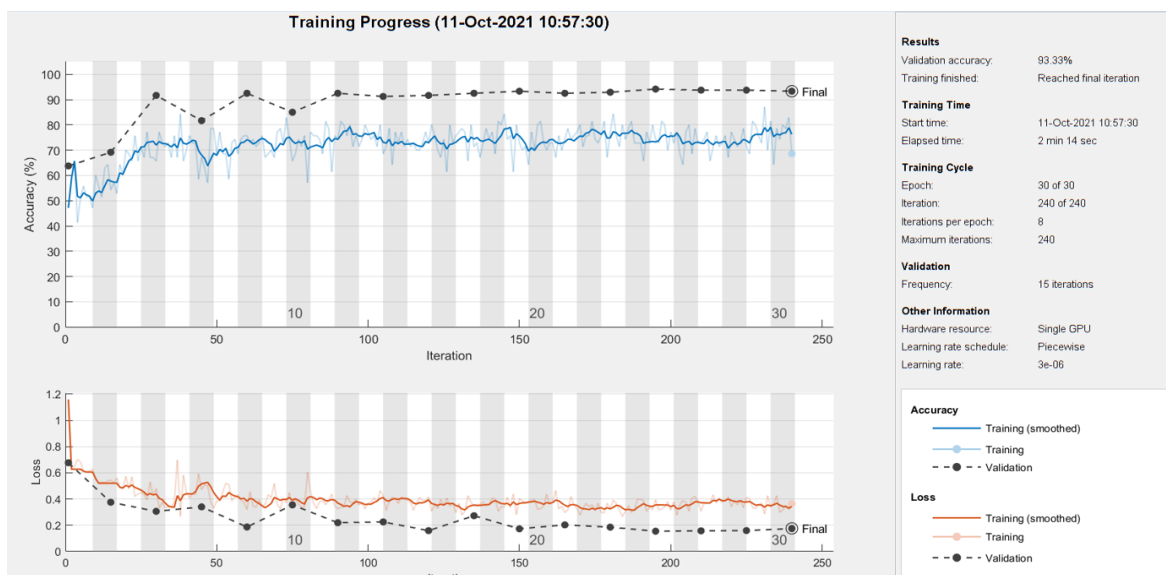
شکل ۹- دقت آموزش CNN با اعمال روش برش تصویر برای ابعاد ورودی 50×50 .



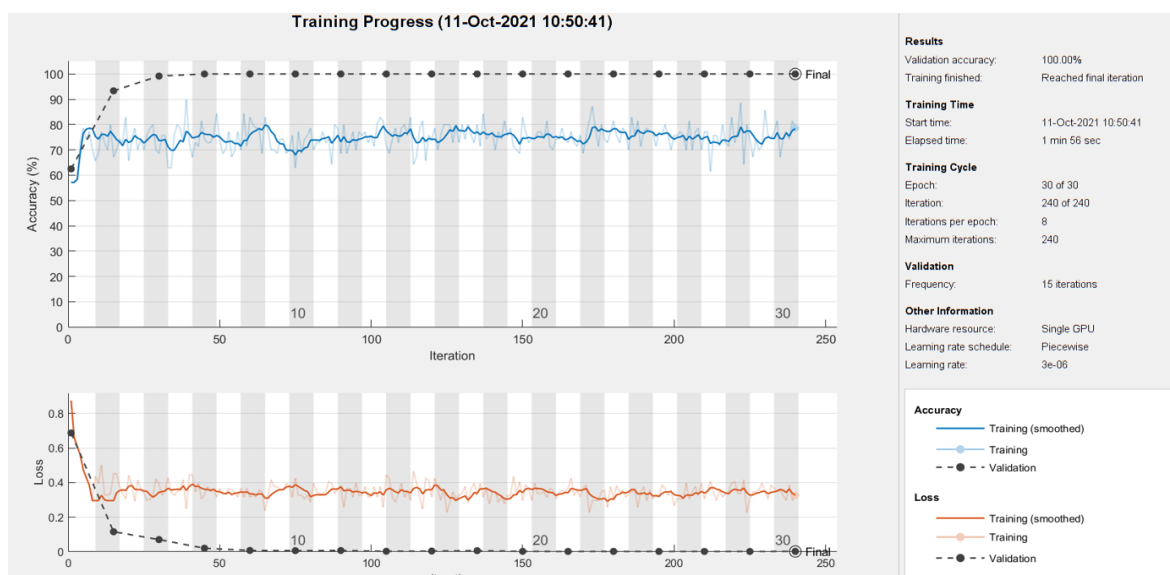
شکل ۱۰- دقت آموزش CNN بدون اعمال روش برش تصویر برای ابعاد ورودی 300×50 .



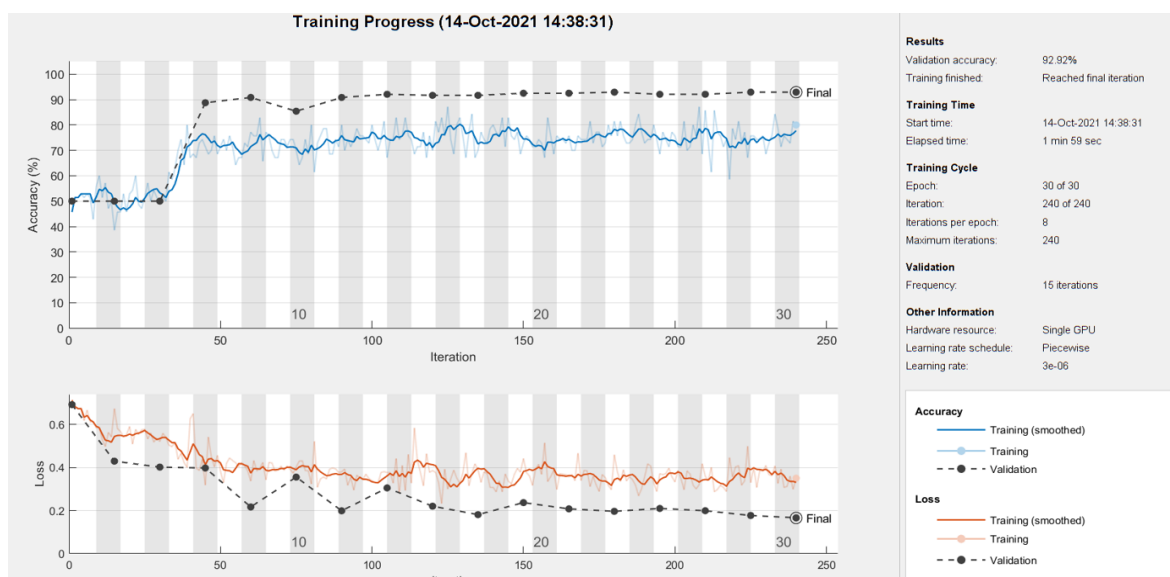
شکل ۱۱- دقت آموزش CNN با اعمال روش برش تصویر برای ابعاد ورودی 300×50 .



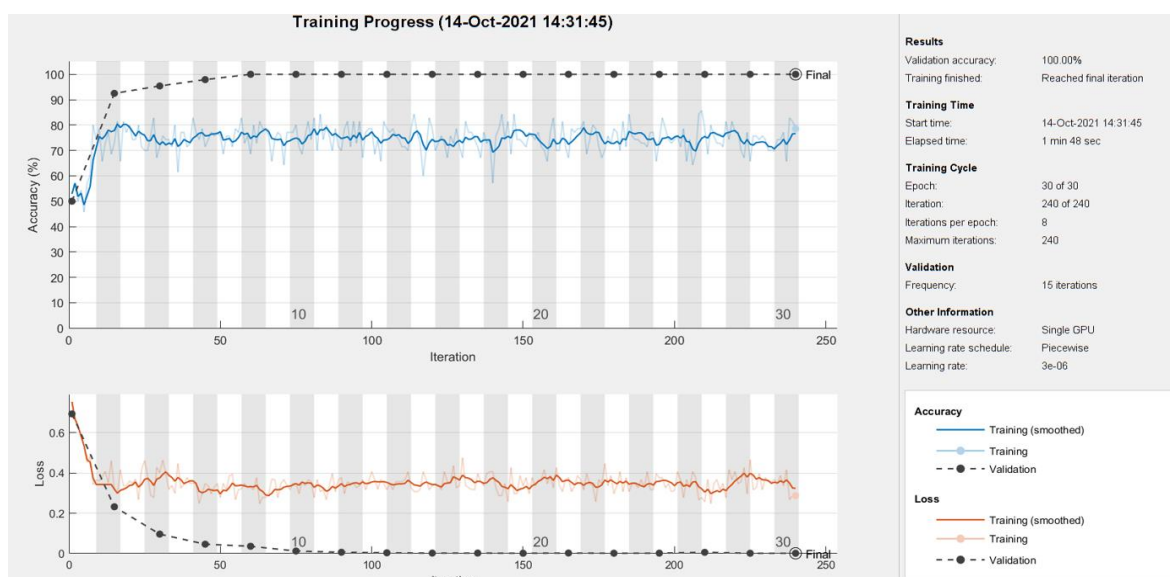
شکل ۱۲- دقت آموزش CNN بدون اعمال روش برش تصویر برای ابعاد ورودی ۲۲۰×۳۵.



شکل ۱۳- دقت آموزش CNN با اعمال روش برش تصویر برای ابعاد ورودی ۲۲۰×۳۵.



شکل ۱۴- دقت آموزش CNN بدون اعمال روش برش تصویر برای ابعاد ورودی ۱۴۰×۳۵ .



شکل ۱۵- دقت آموزش CNN با اعمال روش برش تصویر برای ابعاد ورودی ۱۴۰×۳۵ .

همان‌طور که از تصاویر بالا مشاهده می‌شود، سرعت همگرایی و دقت آموزش شبکه عصبی تحت تاثیر بکارگیری الگوریتم برش تصاویر بهبود می‌یابد. بعنوان مثال، برای تصاویر با ابعاد ۱۴۰×۳۵ ، در حالت بدون اعمال روش برش تصویر، شبکه پس از حدود ۴۶ تکرار* و حدود ۲۵ ثانیه همگرا می‌شود و میانگین دقت آموزش شبکه عصبی پس از همگرایی ۷۳٫۸۸٪ محاسبه شده است. این در حالی است که با اعمال روش برش تصویر برای تصاویر با ابعاد ۱۴۰×۳۵ ، شبکه پس از حدود ۱۵ تکرار و حدود ۱۷ ثانیه به دقت ۸۰٪ می‌رسد و میانگین دقت آموزش شبکه عصبی در این حالت ۷۴٫۸۱٪ محاسبه شده است. در جدول‌های ۱ تا ۵ نتایج مقایسه روش بکار برده شده با روش معمول به روشنی بیان شده است.

* Iteration

جدول ۱- مقایسه روش ارائه شده برش تصویر برای تصاویر CAF با ابعاد 60×40 پیکسل.

تصاویر CAF با اعمال روش برش تصویر	تصاویر CAF بدون اعمال روش برش تصویر	پارامترهای اندازه‌گیری شده
4.6	12.66	زمان همگرایی دقت آموزش شبکه عصبی [ثانیه]
74.57	74.19	میانگین دقت آموزش از تکرار ۳۰ ام به بعد [بر حسب درصد]
0.3494	0.3636	میانگین تلفات آموزش از تکرار ۳۰ ام به بعد
100	93.75	دقت داده‌های اعتبارسنجی در پایان آموزش [بر حسب درصد]
0.0089	0.1560	تلفات داده‌های اعتبارسنجی در پایان آموزش
52	72	زمان کل آموزش [ثانیه]

جدول ۲- مقایسه روش ارائه شده برش تصویر برای تصاویر CAF با ابعاد 140×35 پیکسل.

تصاویر CAF با اعمال روش برش تصویر	تصاویر CAF بدون اعمال روش برش تصویر	پارامترهای اندازه‌گیری شده
13.73	21.2	زمان همگرایی دقت آموزش شبکه عصبی [ثانیه]
74.81	73.88	میانگین دقت آموزش از تکرار ۳۰ ام به بعد [بر حسب درصد]
0.3444	0.3763	میانگین تلفات آموزش از تکرار ۳۰ ام به بعد
100	92.99	دقت داده‌های اعتبارسنجی در پایان آموزش [بر حسب درصد]
0.0012	0.1658	تلفات داده‌های اعتبارسنجی در پایان آموزش
108	119	زمان کل آموزش [ثانیه]

جدول ۳- مقایسه روش ارائه شده برش تصویر برای تصاویر CAF با ابعاد ۲۲۰×۳۵ پیکسل.

تصاویر CAF بدون اعمال روش برش تصویر	تصاویر CAF با اعمال روش برش تصویر	پارامترهای اندازه‌گیری شده
22.26	7.6	زمان همگرایی دقت آموزش شبکه عصبی [ثانیه]
73.76	75.12	میانگین دقت آموزش از تکرار ۳۰ ام به بعد [بر حسب درصد]
0.3745	0.3445	میانگین تلفات آموزش از تکرار ۳۰ ام به بعد
93.33	100	دقت داده‌های اعتبارسنجی در پایان آموزش [بر حسب درصد]
0.1761	0.0022	تلفات داده‌های اعتبارسنجی در پایان آموزش
134	116	زمان کل آموزش [ثانیه]

جدول ۴- مقایسه روش ارائه شده برش تصویر برای تصاویر CAF با ابعاد ۳۰۰×۵۰ پیکسل.

تصاویر CAF بدون اعمال روش برش تصویر	تصاویر CAF با اعمال روش برش تصویر	پارامترهای اندازه‌گیری شده
29.13	23.4	زمان همگرایی دقت آموزش شبکه عصبی [ثانیه]
74.48	74.63	میانگین دقت آموزش از تکرار ۳۰ ام به بعد [بر حسب درصد]
0.3667	0.3509	میانگین تلفات آموزش از تکرار ۳۰ ام به بعد
92.92	100	دقت داده‌های اعتبارسنجی در پایان آموزش [بر حسب درصد]
0.1195	0.0066	تلفات داده‌های اعتبارسنجی در پایان آموزش
242	219	زمان کل آموزش [ثانیه]

جدول ۵- مقایسه روش ارائه شده برش تصویر برای تصاویر CAF با ابعاد ۵۰۰×۵۰ پیکسل.

تصاویر CAF بدون اعمال روش برش تصویر	تصاویر CAF با اعمال روش برش تصویر	پارامترهای اندازه‌گیری شده
120.93	49.8	زمان همگرایی دقت آموزش شبکه عصبی [ثانیه]
74.11	75.17	میانگین دقت آموزش از تکرار ۳۰ ام به بعد [بر حسب درصد]
0.3640	0.3457	میانگین تلفات آموزش از تکرار ۳۰ ام به بعد
94.58	100	دقت داده‌های اعتبارسنجی در پایان آموزش [بر حسب درصد]
0.0984	0.0115	تلفات داده‌های اعتبارسنجی در پایان آموزش
980	959	زمان کل آموزش [ثانیه]

در جداول ۱ تا ۵ میانگین دقت آموزش شبکه از تکرار ۳۰ ام به بعد که شبکه همگرا شده، گزارش شده است. همان‌طور که در این جداول مشاهده می‌شود، با بکارگیری الگوریتم برش تصاویر، دقت شبکه آموزش یافته و میزان زمان همگرایی در همه موارد بهبود یافته است. به عنوان مثال، زمان همگرایی برای تصاویر با ابعاد ۱۴۰×۳۵ تقریباً ۳۵٪ و میانگین دقت حدود ۱٪ بهبود داشته است. به طور کلی، پس از محاسبه میانگین نتایج گزارش شده در همه جداول می‌توان گفت که زمان همگرایی آموزش شبکه عصبی ۴۸٫۸٪ و میانگین دقت آموزش شبکه پس از همگرایی ۰٫۷۹٪ بهبود داشته است.

۷. نتیجه‌گیری

حجم و ابعاد بالای تصاویر CAF باعث شده است که آموزش شبکه‌های عصبی کانولوشنی توسط این تصاویر برای تشخیص فریب، دارای پیچیدگی محاسباتی بالایی باشد. همچنین برای تعداد داده‌های آموزشی بالا، زمان و تلفات آموزش، زیاد خواهد شد. در این کار، قبل از آموزش شبکه عصبی، پیش‌پردازش تصاویر CAF با بکارگیری روش برش تصویر پیشنهاد شد. به کمک این روش ابعاد تصویر CAF کاهش یافت. نتایج نشان می‌دهند که شبکه عصبی، به ازای داده‌های برش خورده نسبت به داده‌های اصلی، عملکرد بهتری دارد. در واقع، در این حالت زمان همگرایی شبکه عصبی و دقت آموزش هر دو بهبود یافتند.

۸. مراجع

- [۱] سید محمدرضا موسوی میرکلائی، "پردازش داده‌ها در گیرنده‌های تک فرکانسه GPS"، انتشارات دانشگاه علم و صنعت ایران، ۱۳۹۰.
- [۲] سید محمدرضا موسوی میرکلائی، مریم معاضدی، محمدجواد رضایی و امیر طباطبایی، "مقابله با اختلال در گیرنده‌های GPS"، انتشارات دانشگاه علم و صنعت ایران، ۱۳۹۴.

- [3] P. Borhani Darian, H. LI, P. Wu, P. Closas, "Deep Neural Network Approach to Detect GNSS Spoofing Attacks," *In Proceedings of the 2020 International Technical Meeting of The Institute of Navigation*, 2020.
- [4] K. Simonyan and A. Zisserman, "Very Deep Convolutional Networks for Large-scale Image Recognition", arXiv preprint arXiv:1409.1556, 2014.
- [5] S. Liu and W. Deng, "Very Deep Convolutional Neural Network based Image Classification Using Small Training Sample Size," *3rd IAPR Asian Conference on Pattern Recognition (ACPR)*, pp. 730-734, 2015.
- [6] B. K. Mishra, D. Thakker, S. Mazumdar, D. Neagu, M. Gheorghe and S. Simpson, "A Novel Application of Deep Learning with Image Cropping: A Smart City Use Case for Flood Monitoring," *Journal of Reliable Intelligent Environments*, pp. 51-61, 2020.
- [7] J. Chen, G. Bai, S. Liang and Z. Li, "Automatic Image Cropping: A Computational Complexity Study," *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 507-515, 2016.
- [8] R. C. Gonzalez and R. E. Woods, "Digital Image Processing", Beijing: Publishing House of Electronics Industry, 3rd edition, 2006.
- [9] M. A. Joshi, "Digital Image Processing: An Algorithmic Approach", PHI Learning Pvt. Ltd., 2018.
- [10] K. Borre, D. M. Akos, N. Bertelsen, P. Rinder, and S. H. Jensen, "A Software-Defined GPS and Galileo Receiver, A Single-Frequency Approach," Springer Science & Business Media, 2007.
- [11] C. Mouton, J. C. Myburgh, and M. H. Davel, "Stride and Translation Invariance in CNNs," *Southern African for Conference Artificial Intelligence Research (SACAIR)*, Part of Communications in Computer and Information Science Book, vol. 1342, pp. 267-281, 2020.
- [12] J. Schmidhuber, "Deep Learning in Neural Networks: An Overview," *Neural Networks*, vol. 61, pp. 85-117, 2015.
- [13] N. G. Polson and S. L. Scott, "Data Augmentation for Support Vector Machines," *Bayesian Analysis*, vol. 6, no. 1, pp. 1-23, 2011.



- [14] P. Toulis and E. M. Airoidi, "Asymptotic and Finite-sample Properties of Estimators based on Stochastic Gradients," *Annals of Statistics*, vol. 45, no. 4, pp. 1694-1727, 2017.
- [15] N. Qian, "On the Momentum Term in Gradient Descent Learning Algorithms," *The Official Journal of the International Neural Network Society*, vol. 12, no.1, pp. 145-151, 1999.