IUST
Iran University of Science and Technology

Iranian Journal of Electrical and Electronic Engineering

Journal Homepage: ijeee.iust.ac.ir

Research Paper

Improving Cross Ambiguity Function Using Image Processing Approach to Detect GPS Spoofing Attacks

K. Zarrinnegar*, S. Tohidi*, M. R. Mosavi*(C.A.), A. Sadr*, and D. M. de Andrés**

Abstract: The Global Positioning System (GPS) is vulnerable to various deliberate and unintentional interferences. Therefore, identifying and coping with various interferences in this system is essential. This paper analyzes a method of reducing the dimensions of Cross Ambiguity Function (CAF) images in improving the identification of spoofing interference at the GPS using Multi-Layer Perceptron Neural Network (MLP NN) and Convolutional Neural Network (CNN). Using the proposed method reduces data complexity, which can reduce the number of learning data requirements. The simulation results indicate that, by applying the proposed image processing algorithm for different dimensions of CAF images, the CNN performs better than MLP NN in terms of training accuracy; the MLP NN is superior to CNN in terms of convergence speed of training. In addition, the results demonstrate that the operation of the proposed method is appropriate in the case of small-delay spoofed signals. Therefore, for the intervals above 0.25 code chip, the proposed method detects spoofing attacks with a correct detection probability close to one.

Keywords: CAF, GPS, GPS Spoofing Attack, Latent Semantic Analysis, Neural Networks.

1 Introduction

THE Global Positioning System (GPS) is a satellite system widely used today for positioning and timing. GPS, being used in various fields, is a vital part of the national infrastructure, and its security is an important issue. GPS signals travel long distances from satellites to receivers, so they have meager power on the ground and are weak against various disturbances. Spoofing attack is known as the most dangerous interference in GPS. In this type of attack, the spoofer sends a signal structurally similar to the authentic GPS signal to receiver and forces the receiver to position incorrectly. Because of this similarity in the structure of the authentic signal and the spoofing signal, interference detection is crucial. Detection of spoofing interference is mandatory in protecting navigation systems [1, 2].

Monitoring signal power in the GPS band is one of the commonest methods of spoofing interference detection. Monitoring the correlation function distortion in the tracking stage is another criterion used to detect interference in the GPS [3]. Signal Quality Monitoring (SQM) is a criterion for measuring correlation function distortion which has been widely investigated. Several countermeasures for measuring interference have been introduced [4]. In [5], the authors examined the ratio test criterion under the presence of the spoofing signal. Pirsiavash *et al.* [6] suggested a countermeasure for monitoring distortion in the frequency domain as a two-dimensional SQM method. In [7], the authors mitigate spoofing attacks in GPS receiver using least mean squares-based adaptive filter. Moazedi *et al.* [8] investigated real-time interference detection in tracking loop of GPS receiver. Borhani-Darian *et al.* [9] presented Multi-Layer Perceptron Neural Network (MLP NN) and complex Convolutional Neural Network (CNN) structure to detect GNSS spoofing attacks. Nowadays, deep neural network structures and machine learning have been very successful in various applications. For example, in [10],

Iranian Journal of Electrical and Electronic Engineering, 2023.
Paper first received 03 July 2022, revised 01 September 2022, and accepted 12 September 2022.
* The authors are with the School of Electrical Engineering, Iran University of Science and Technology (IUST), Narmak, Tehran 16846-13114, Iran.
E-mails: k_zarrinnegar@elec.iust.ac.ir, s_tohidi@elec.iust.ac.ir, m_mosavi@iust.ac.ir, and sadr@iust.ac.ir.
** The author is with the ETSI de Telecomunicación, Universidad Politécnica de Madrid, Av. Complutense 30, 28040 Madrid, Spain.
E-mail: diego.martin.de.andres@upm.es.
Corresponding Author: M. R. Mosavi.
https://doi.org/10.22068/IJEEE.19.1.2584

the authors utilized deep CNN and extreme learning machines stabilized by the chimp optimization algorithm to diagnose COVID-19 from X-Ray images. In [11] Naderan *et al*. used combined machine learning algorithms and fuzzy logic for classification of trust factor in social networks. The high performance of CNN made us base our work on reference [9], which employed CNN in the field of GPS spoofing detection.

In this work, the aim is to detect spoofing attacks using Cross-Ambiguity Function (CAF), which will be discussed in the following. These functions are fed and trained as data to MLP NN and CNN, and finally, after learning, the neural networks will be able to detect spoofing attacks from CAFs. On the other hand, these functions have many volumes and dimensions, and it will require a strong processor to learn MLP NN and CNN. In particular, this paper proposes an effective and known preprocess method to reduce CAF dimensions. This work aims to explore this method's capabilities and modify it to use on CAF data appropriately. Then, to prove the claim, tests are performed, and to validate the results, a comparison is made with other similar reported works.

In the following, the proposed method is presented along with the flowchart. By applying this method to CAF images and then feeding these images to MLP NN and CNN, the performance of the proposed method is evaluated in the results section. Finally, conclusions are drawn, and references are listed.

2 Cross Ambiguity Function

One of the methods of detecting the spoofing attack is the CAF. These functions are obtained in acquisition stage of the receivers after a two-dimensional search in Doppler frequency and the code phase containing essential information on the presence of spoofing signals. When there is a GPS spoofing signal, there is more than one peak in CAF images, and if only the original signal is present, a single peak is observed in CAF images (according to Figs. 1 and 2). Two different hypotheses are intended and tested [9]:

1. The null hypothesis (H_0), stating that the legitimate signal ($S(.)$) and noise ($\eta(.)$) are present, but there is no spoofing signal (i.e., H_0: $Y(t) = S(t) + \eta(t)$).
2. The alternative hypothesis (H_1), stating that both the legitimate signal, spoofed signal ($S_s(.)$), and noise are present in the dataset (i.e., H_1: $Y(t) = S(t) + S_s(t) + \eta(t)$).

In the absence of a spoofing signal, the legitimate signal can be stated by (1):

$$S(t)=\sum_{i=1}^{M} a_i c_i\left(t-\tau_i(t)\right) d_i\left(t-\tau_i(t)\right) \times \exp\left(j\left(\omega_{IF} t-\omega_c \tau_i(t)-\varphi_i(t)\right)\right) \quad (1)$$

where M is the number of spreading codes, a_i is the carrier amplitude of the i-th signal, $c_i(t)$ is the spreading code of i-th satellite, $d_i(t)$ is the i-th signal data bit stream, $\tau_i(t)$ is the i-th signal code phase, ω_c is the carrier frequency, ω_{IF} is the intermediate frequency and $\varphi_i(t)$ is the i-th carrier phase. Also, in the presence of the spoofing attack, the spoofing signal structure is similar to the structure of the legitimate signal in the form of (2):

$$S_S(t)=\sum_{i=1}^{M_s} a_{s,i} c_i\left(t-\tau_i(t)\right) d_i\left(t-\tau_{s,i}(t)\right) \times \exp\left(j\left(\omega_{IF} t-\omega_c \tau_{s,i}(t)-\varphi_{s,i}(t)\right)\right) \quad (2)$$

where M_s denotes the number of spoofed signals. In this case, the only spreading code $c_i(t)$ is the same as the legitimate signal spreading code and amplitude of the spoofed signal $a_{s,i}$, code phase $\tau_{s,i}(t)$, and carrier phase $\varphi_{s,i}(t)$ is different from the legitimate signal [12].

The total signal at the victim receiver antenna during a spoofing attack is as (3):

$$Y(t)=S(t)+S_s(t)+\eta(t) \quad (3)$$

where $\eta(t)$ is the received noise typically modeled as zero-mean, additive, white, and Gaussian [9].

Detection of spoofing attacks using CAF is not always straightforward. In the following cases, it is challenging to detect spoofing attacks using CAF:

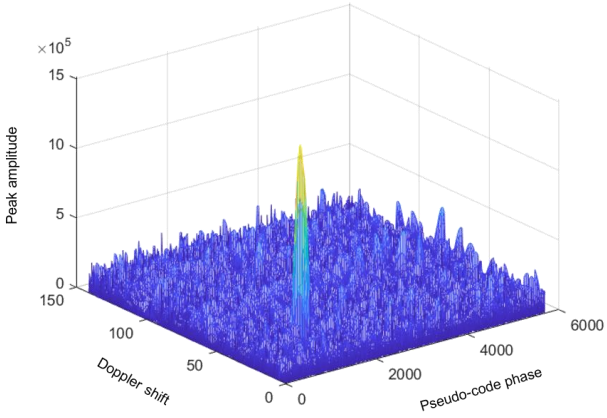

Fig. 1 CAF in the absence of spoofing signal.

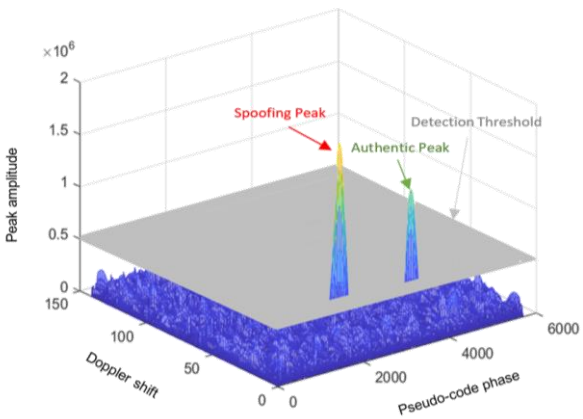

Fig. 2 CAF in the presence of spoofing signal.

- Environments with significant multi-path: In the presence of multi-path, multiple observable peaks occur frequently. The peak points of the multi-path are typically close to the legitimate signal peak in Doppler (i.e., within 10's of Hz) and in time (i.e., within 10's of microseconds). In [13], the way to detect this type of spoofing attack is presented.
- Spoofing signals very close to the legitimate signal in the Doppler frequency and code phase: In the situation where the spoofed and desired signals are close in Doppler (i.e., within 10's of Hz), and time (i.e., within the spreading code symbol duration, e.g., ~1 microsecond for the GPS C/A-code), only one peak may be observable in the CAF. Monitoring the CAF for multiple peaks renders a less effective technique to detect spoofing. In such cases, a variety of methods have been examined to detect spoofing, which are similar to SQM techniques used by civil aviation augmentations to detect malformations in legitimate Global Navigation Satellite System (GNSS) signals [14].
- Spoofing signals are much higher in amplitude than the legitimate GNSS signals accompanied by noise: In this situation, it can be difficult to detect multiple peaks in the CAF, because the true signal peaks are much lower in amplitude than the spoofed signal peaks. Furthermore, the noise floor may be elevated. In [13], it is suggested that CAF monitoring be accompanied by coarse Automatic Gain Control (AGC) monitoring to detect the situation where the noise floor has been significantly altered.

3 Proposed Method

In [9], a spoofing attack has been identified according to the characteristics of the peak points related to the CAF images, using the MLP NN and CNN. Furthermore, a complex CNN structure with 13 layers of convolution with high training accuracy has been used to classify the signals into two classes: spoofing and legitimate signals. Fig. 3 depicts the acquisition-based spoofing detection scheme of the GNSS system presented in [9] using the CNN [15, 16].

CAF images have a large size; therefore, detecting the spoofed signal from CAF using artificial intelligence requires a lot of training time and deep processing. On the other hand, in addition to the accuracy of correct detection of the spoofing attack, NNs' time for correct detection of the spoofing attack must be as short as possible. Therefore, we are looking for approaches to improve the timing and accuracy of deep NNs. For this reason, in this paper, the algorithm of the volume and dimensions reduction of the Latent Semantic Analysis (LSA)-transform is recommended [17-22].

LSA is a technique in natural language processing, particularly distributional semantics, for analyzing relationships between a set of documents and the terms they contain by producing a set of concepts related to the documents and terms. It uses singular value decomposition, a mathematical technique to scan the unstructured data to pinpoint hidden relationships between terms and concepts. One of the effective ways to reduce the dimensions of image data is the LSA-transform. According to LSA-transform, this method eliminates the trivial information of the image matrix and reduces its size and dimensions. Assume that I is an image matrix and M is the matrix of the brightness of the image pixels, in which case, the LSA-transform only selects even columns and rows of the matrix M and forms M1. For better understanding, you can see the grey image in Fig. 4 that has 2129×3840 dimensions. This method was applied four times to the image, and the image in Fig. 5 was obtained. As can be seen, the general concept of the image is recognizable [19].

4 Procedure

In the present study, CAF images were extracted from the acquisition stage of the GPS receiver. The LSA-transform method as the proposed pre-processing method was applied to the CAF function. These images were then fed to MLP NN and CNN to decide on the presence or absence of the signal. Fig. 6 shows the general diagram of the proposed method of spoofing detection.

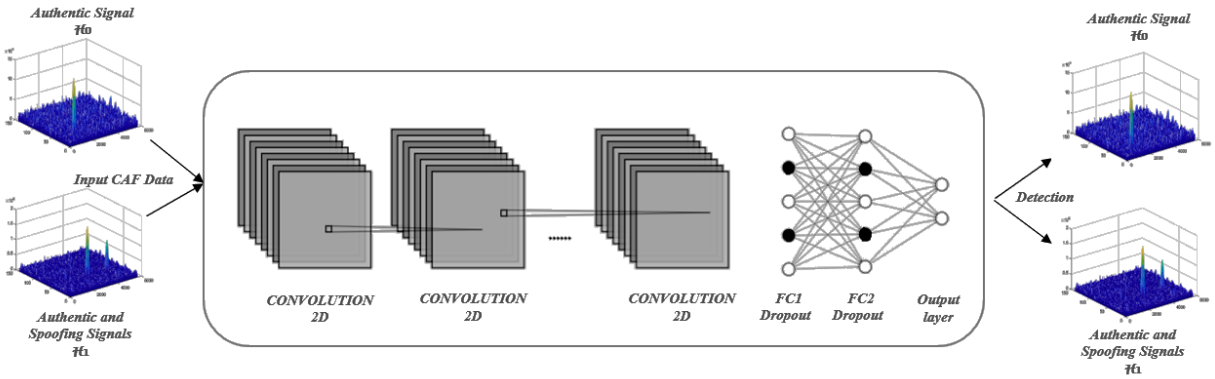

Fig. 3 Spoofing detection scheme in the acquisition stage of GNSS receiver using the CNN structure.

Fig. 4 An image (Naghsh-e-Jahan square of Isfahan) with dimensions of 2129×3840.

Fig. 5 Naghsh-e-Jahan square of Isfahan with dimensions of 133×240 (LSA-transform applied four times).

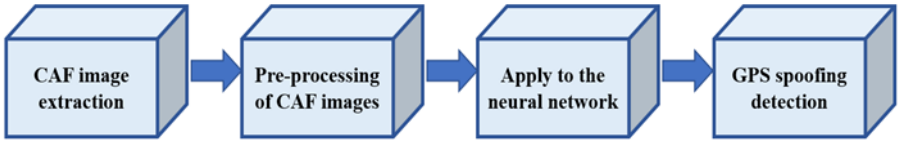

Fig. 6 General steps to detect GPS spoofing.

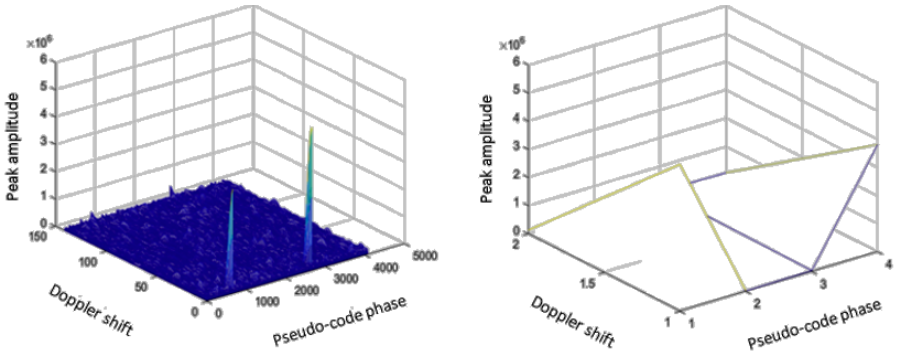

Fig. 7 The original CAF acquired image (left), and the modified version using the LSA-transform method (right).

4.1 Applying the LSA-transform Method on CAF Images

Given that the most important image information in CAF images is the peak points, the LSA-transform is modified to have the highest reduction of dimensions and prevents the peak points from disappearing. Part of this method is decided based on the column and row related to the peak points to remove the odd or even rows or columns. For example, Fig. 7 shows the CAF image of a spoofing signal (including two peak points) with dimensions of 141×4192 which has been reduced to 2×4 by the modified LSA-transform method. This method reduces the complexity of NN learning and, in a shorter period, can train the NN with more learning data. On the other hand, training losses are reduced, and the accuracy of learning increases. NN training time also decreases.

Fig. 8 shows the flowchart of the modified LSA-transform in the presence of the original signal. This method has been implemented in MATLAB software. Fig. 9 shows how the LSA-transform algorithm performs in the presence of the spoofing signal.

The modified LSA-transform method is implemented simply when only the authentic signal is present. It is illustrated in Fig. 8. In the presence of the spoofing signal, the row and column related to the peak points were obtained first, and then every other matrix rows are deleted; so that only the peak points remain. Then, similarly to every other matrix columns are deleted based on the being even or odd columns of the peak points. Fig. 9 shows the modified LSA-transform method applied on a 6×6 CAF matrix. NN training time also decreases. Fig. 8 shows the flowchart of the modified LSA-transform in the presence of the original signal.

In the presence of the spoofing signal, it is challenging to detect the spoofing attack when Doppler frequency and code phase delay related to the authentic signal and the spoofed signal are close to each other. In other words, peak points are very close to each other.

Under these conditions, the criterion of performance of the modified LSA-transform algorithm will be measured, and the results will be presented in the results section. Figs. 10 and 11 show the two-dimensional view of the CAF image. In Fig. 10, only the authentic signal is present, and in Fig. 11, both authentic and the spoofing signals are present with the distance of a chip. In this case, in Fig. 12, an area around the maximum peak point is considered to detect the presence of the spoofing attack, and then the sum of the CAF values of this area is compared to the threshold λ. A spoofed signal has occurred close to the maximum peak point if the total amount of CAF of the considered area is more significant than λ. Otherwise, only the authentic signal is present.

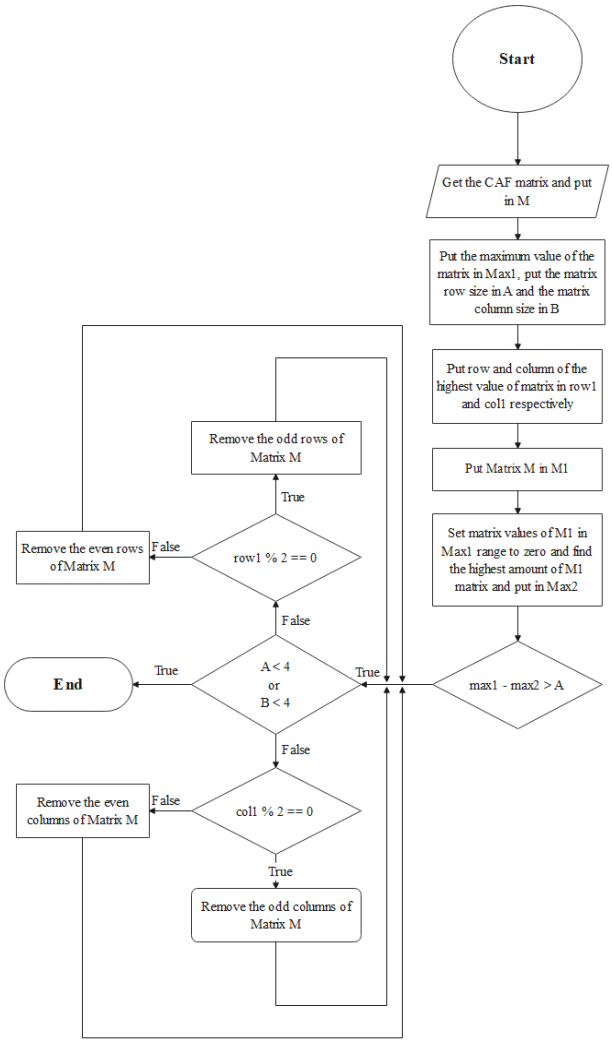

Fig. 8 The flowchart of the LSA-transform method in the presence of the authentic signal.

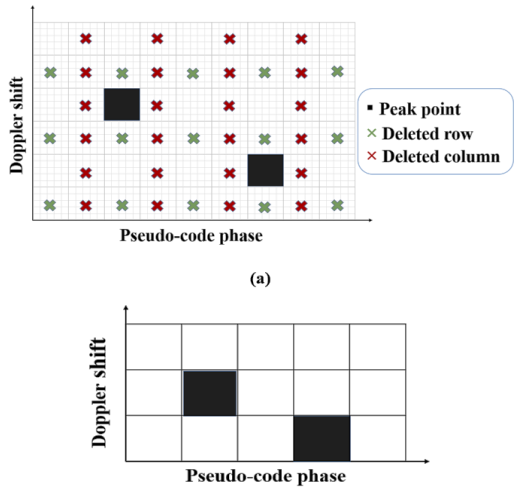

Fig. 9 An example of the modified LSA-transform method in the presence of the spoofing attack: (a) 6×9 CAF matrix, and (b) CAF matrix with reduced dimensions 5×3 after applying modified LSA-transform method.

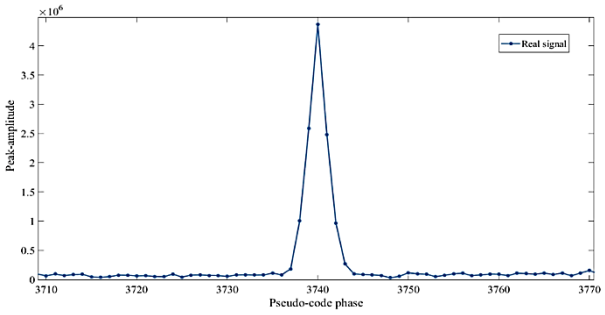

Fig. 10 Two-dimensional view of the CAF image in the presence of an authentic signal.

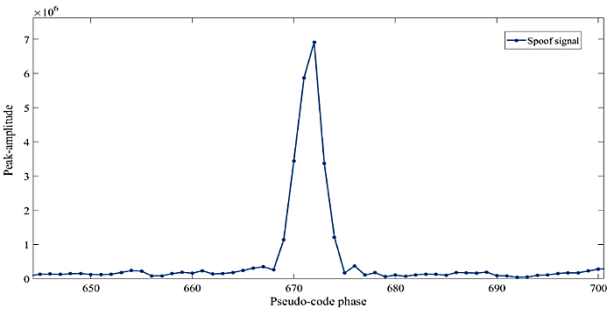

Fig. 11 Two-dimensional view of the CAF image in the presence of both authentic signal and spoofing signal with one chip distance.

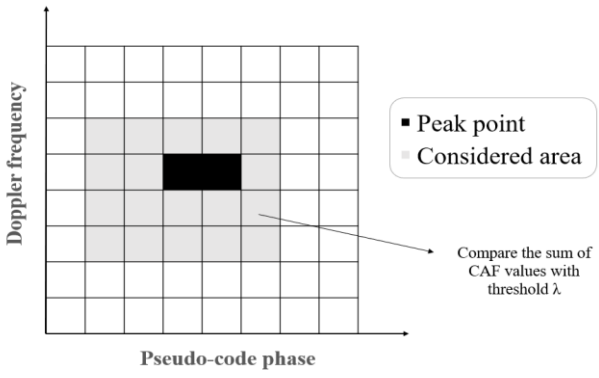

Fig. 12 Performance of the LSA-transform algorithm in the presence of the authentic signal and the spoofing signal with one chip distance.

5 Results

The Software-Defined Receiver (SDR) [23] has been used in the MATLAB environment to simulate the proposed method. The sampling frequency in front-end stage of the GPS receiver was set at 4.092 MHz, and the IF signal frequency was adjusted to 1.023 MHz. Processor system specifications include Intel Core i7-10750 CPU @ 2.6 GHz 2.59 GHz and 16 GB of memory RAM and NVIDIA GeForce GTX-1660 Ti graphics cards. MLP NN and CNN were used to detect spoofing attacks. CNN consists of two convolutional layers and three fully connected layers. Each convolutional layer used a batch normalization and a rectified linear unit activation function [24]. In addition, the ReLu activation function and dropout layer with a probability of 0.5 were used in each fully connected layer [25, 26].

MLP NN consists of three connected layers that follow up the ReLu activation function and a dropout layer with a probability of 0.5. The last fully-connected layer consists of two neurons representing the CAF image classification in one of the two spoof and the authentic classes. CAF images were of 141×4092 dimensions. In extracting CAF images, the Doppler frequency shift search step was set to 500 Hz, and the code phase search step was set to 0.5 chip. In this case, each CAF image is converted into a matrix with 141×4092 dimensions and 8-bit values. The simulation uses 2400 CAF images to train MLP NN and CNN, of which 1200 images are associated with the scenarios with presence of the spoofing signal and another 1200 images associated with presence of the authentic signal.

As shown in Fig. 13, the authentic signal is delayed and utilized as a spoofing signal at the IF level. Out of 2400 data, 30% is used to evaluate the NN. Adam's optimizer is also used to obtain weights and thresholds of the NN [27, 28]. In the first part of the simulation, preprocessing was done on the CAF image to reduce image dimensions to 2×4. Then, these images were fed to MLP NN and CNN for training. In the second part, the unprocessed CAF images with 20×1023 dimensions, similar to [9], are given to MLP NN and CNN as training data. These two simulation parts are performed to determine the importance of the proposed method. In Table 1, the structure of the MLP NN and CNN used in this work is shown. Also, in Figs. 14 to 17, the accuracy and losses of MLP NN and CNN are shown in both simulation parts.

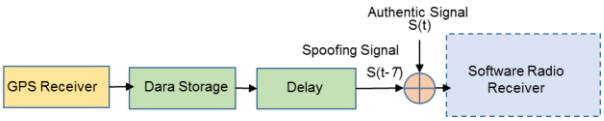

Fig. 13 Block diagram of the spoofing signal generation.

Table 1 The structure of deep learning models used in the first simulation part.

MLP structure	CNN structure
✓ Fully connected layer	✓ 2×2 Convolutional layer
✓ ReLu activation function	✓ Batch normalization layer
✓ Dropout layer	✓ ReLu activation function
✓ Fully connected layer	✓ 2×2 Convolutional layer
✓ ReLu activation function	✓ Batch normalization layer
✓ Dropout layer	✓ ReLu activation function
✓ Fully connected layer	✓ Fully connected layer
-	✓ ReLu activation function
-	✓ Dropout layer
-	✓ Fully connected layer
-	✓ ReLu activation function
-	✓ Dropout layer
-	✓ Fully connected layer

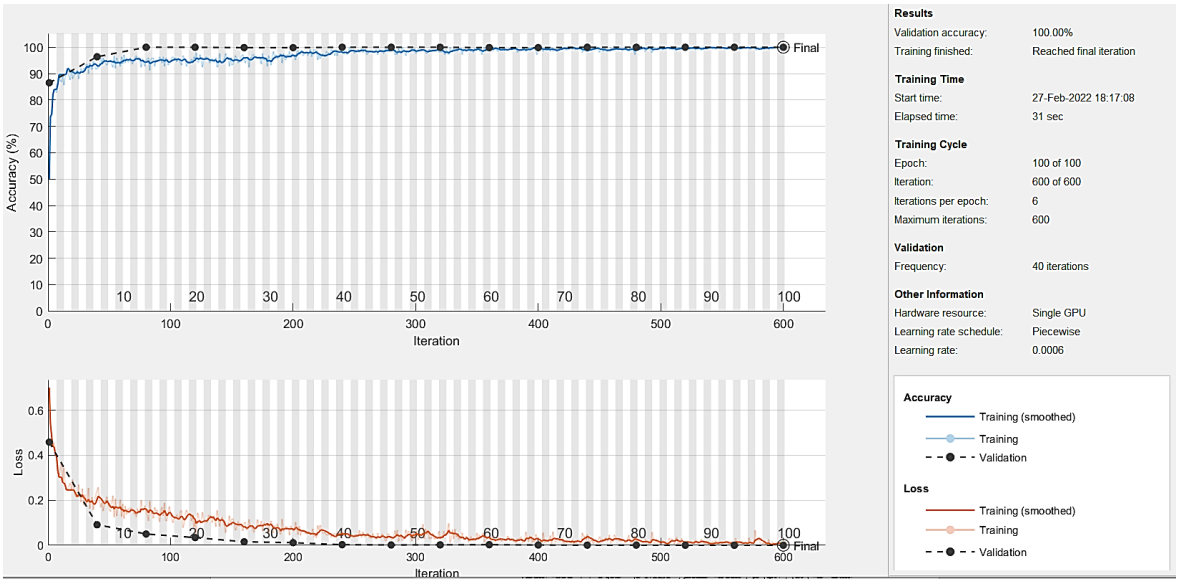

Fig. 14 Accuracy (top panel) and losses (bottom panel) of MLP NN training by applying the modified LSA-transform method.

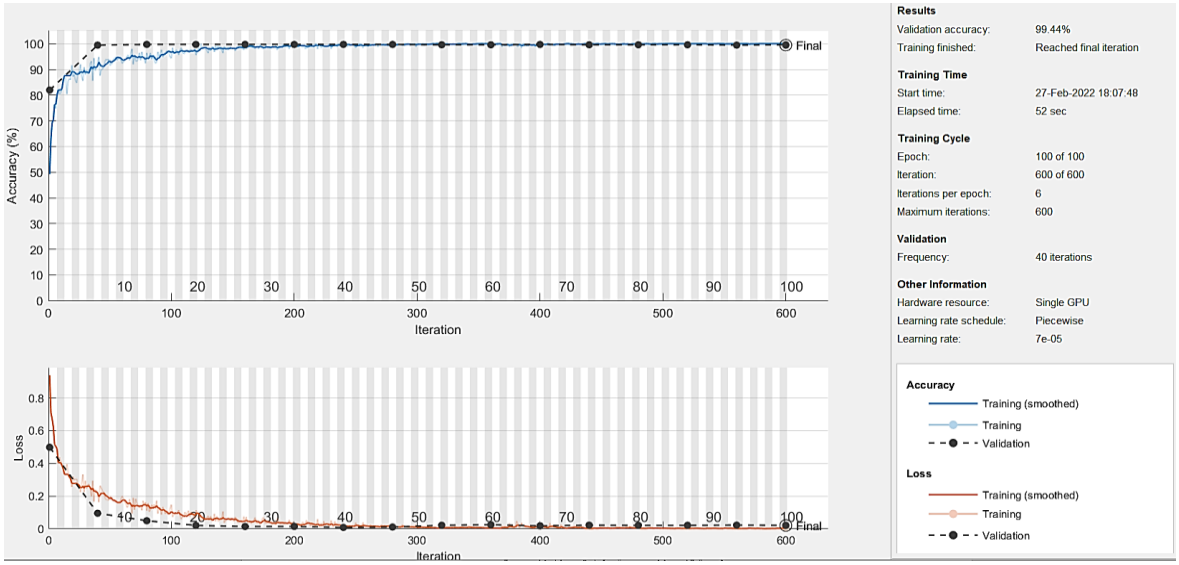

Fig. 15 Accuracy (top panel) and losses (bottom panel) of CNN training by applying the modified LSA-transform method.

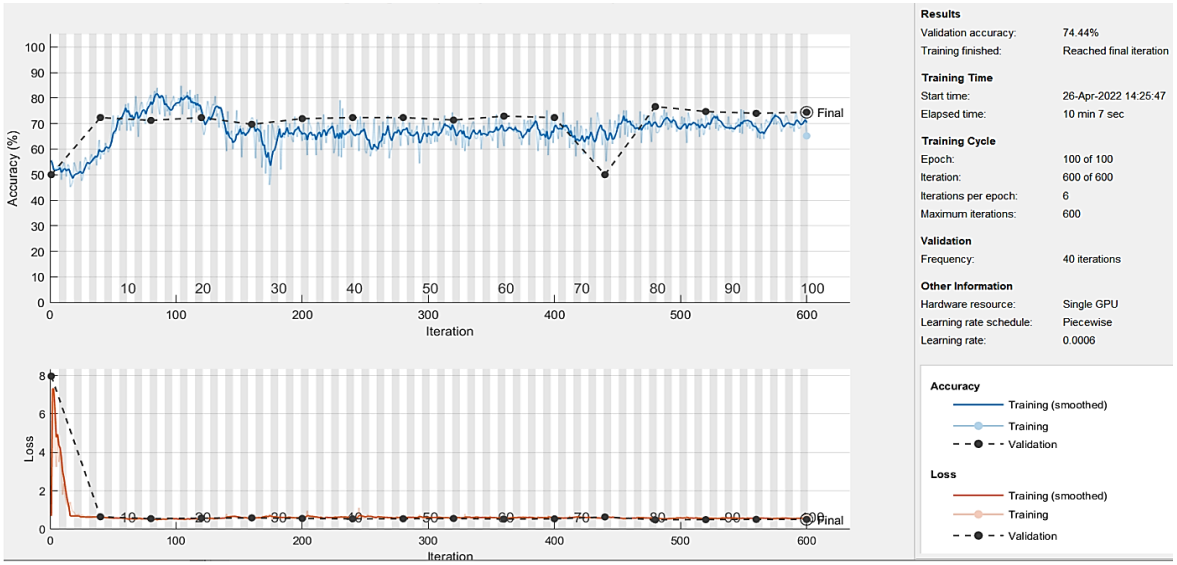

Fig. 16 Accuracy (top panel) and losses (bottom panel) of MLP NN training without applying the preprocessing method.

In Fig. 15, according to the simulation results with the CNN, the average accuracy after the 95th iteration was calculated at about 99.42%. Also, the CNN total training time was about 52 seconds due to time-consuming calculations and a more complex structure than the MLP NN. Convergence time was about 4.9 seconds and 8.23 seconds for MLP NN and CNN, respectively. As expected, MLP NN learning speed is faster than CNN for the same learning data. Another advantage of the CNN is its fewer training losses compared to the MLP NN. In addition, the MLP NN structure uses 1816 activations per image data, while the CNN structure uses 2448 activations per image data. Therefore, CNN structure consumes more memory for learning than MLP NN. As also mentioned in [29], in aggregate, the CNN performs better than the MLP NN in detecting spoofing attacks.

To accurately assess the simulation results of CNN and MLP NN and to validate the LSA-transform preprocessing method, a comparison has been made between these two parts of the simulation results in this work. It should be noted that simulation conditions such as NN structure, hardware processing system, and all parameters of NN training, such as learning rate, for both simulation parts are quite the same. Considering that [9] did not provide information about the structure of the MLP NN, it is not possible to compare the results of the MLP NN in this work with the MLP NN results in [9]. As shown in Fig. 16, the average accuracy after convergence was calculated at about 69.46%. This average accuracy is close to the average obtained in [9]. According to Fig. 17, CNN simulation results have worst accuracy, total training time, and convergence than anticipated. Simulation results are found in Tables 2 and 3 utterly.

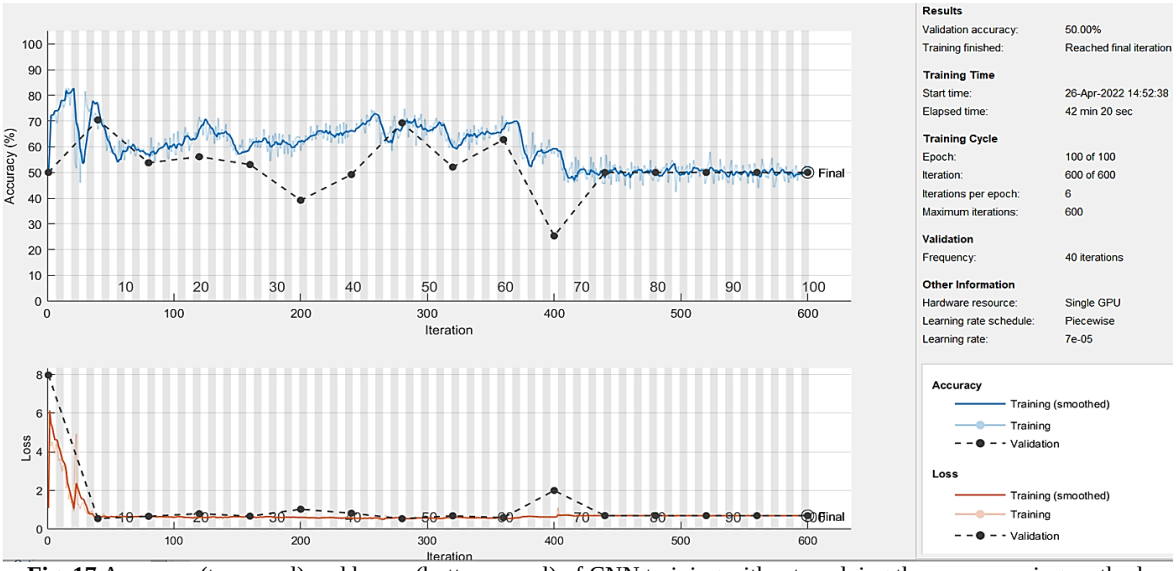

Fig. 17 Accuracy (top panel) and losses (bottom panel) of CNN training without applying the preprocessing method.

Table 2 Comparison of MLP NN simulation results with the structure introduced in this work, applying pre-processing and without pre-processing on CAF images.

Measured parameters	CAF images without pre-processing	CAF images by applying LSA-transform	Improvement [%]
Convergence time of NN training accuracy [sec]	68.8	4.9	92.88
The average accuracy of training after convergence [%]	68.46	98.28	29.82
Average losses of training after convergence	0.597	0.0512	91.43
Validation data accuracy at the end of the training [%]	50	100	50
Validation data losses at the end of the training	0.5121	0.0008492	99.84
Total training time [sec]	607	31	94.9
Adjusted CAF image dimensions [pixels]	**20×1023**	**2×4**	**99.96**

Table 3 Comparison of CNN simulation results with the structure introduced in this work, applying pre-processing and without pre-processing on CAF images.

Measured parameters	CAF images without pre-processing	CAF images by applying LSA-transform	Improvement [%]
Convergence time of NN training accuracy [sec]	63.5	8.23	87.04
The average accuracy of training after convergence [%]	59.29	99.44	40.15
Average losses of training after convergence	0.6755	0.033	95.12
Validation data accuracy at the end of the training [%]	50	99.42	49.42
Validation data losses at the end of the training	0.6986	0.0195	97.21
Total training time [sec]	2540	52	97.96
Adjusted CAF image dimensions [pixels]	**20×1023**	**2×4**	**99.96**

Table 2 shows that the average training accuracy after convergence has improved by 29.82% as a result of applying the LSA-transform method on CAF images. The total MLP NN training time is reduced by 94.9% compared to the case where LSA-transform is not applied to the CAF images. Training data losses after convergence have increased about 0.1 times in this case.

Considering the results from Table 3, the average training accuracy after convergence has improved by 40.15% by applying LSA-transform on CAF images. The total training time of CNN has been reduced by 97.96% compared to the case where LSA-transform is not applied to the CAF images. Training data losses after convergence have increased 97.21% in this case. Comparing the measured parameters for both MLP NN and CNN in this work, it can be claimed that this method is effective.

The detection process determines the presence or absence of spoofing, and the output is the random variable called the decision variable. If the spoofer is present, the probability that the decision variable passes a threshold is called the detection probability. If the spoofer is absent, it is called false alarm probability. Then, the plot of probability detection (Pd) versus the probability of false alarm (Pfa) is called the Receiver Operating Characteristic (ROC) [9]. The ROC curve is a graphical tool for investigating the discriminatory power of a detection method [30]. The performance of the modified LSA-transform method and the method of [31] are shown in Figs. 18 and 19, when the peak points are

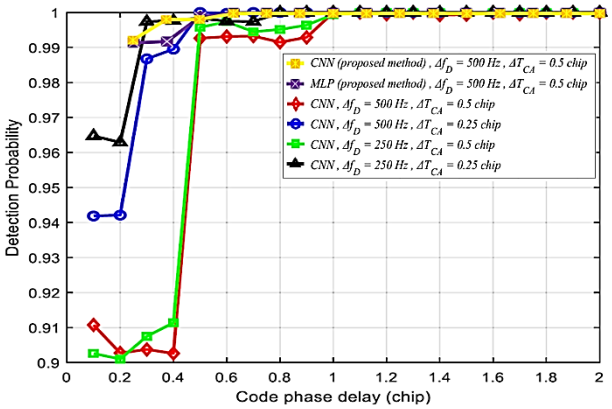

Fig. 18 Comparison of the probability of correct detection of the learning models presented in this work with the work done in [31].

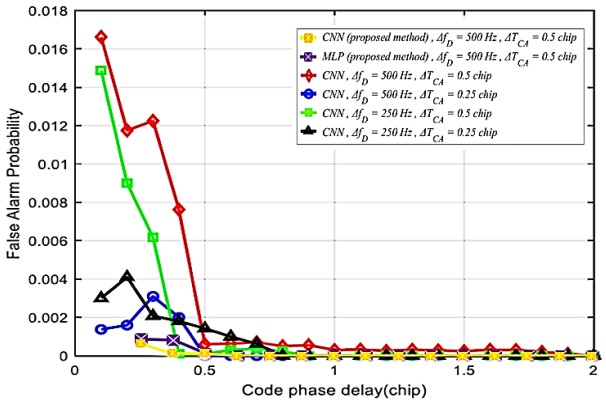

Fig. 19 Comparison of the probability of false alarm of the learning models presented in this work with the work done in [31].

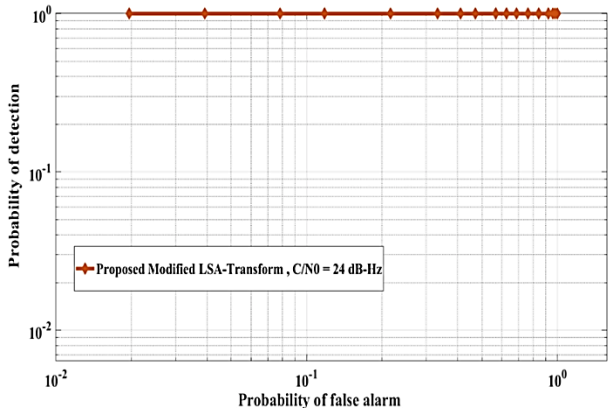

Fig. 20 ROC curve performance of the proposed LSA-transform method.

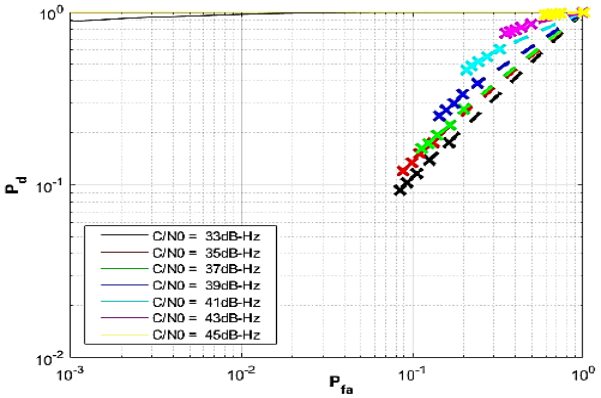

Fig. 21 ROC curve performance of MLP NN [9].

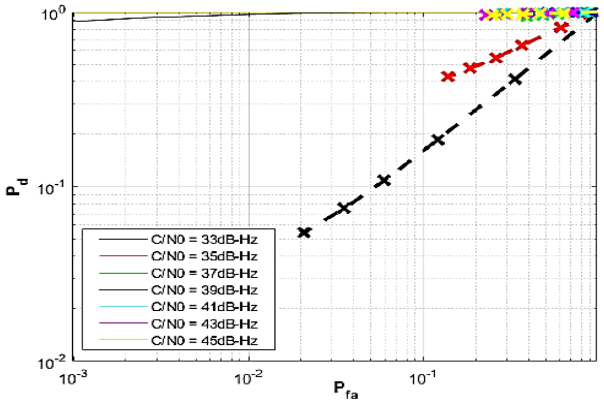

Fig. 22 ROC curve performance of complex CNN [9].

very close to each other (i.e., in small delay spoofing attack). As shown in Fig. 18, for the intervals below 0.25 chip, the proposed method cannot detect spoofing, and the probability of correct detection of spoofing is severely dropped. Whereas for the peak points of more than 0.25 chips, the probability of false alarm is within an order of 10^{-4}, so the method's performance is satisfying (as shown in Fig. 19).

To evaluate the performance of the LSA-transform method proposed to detect spoofing, the ROC curve for this method is plotted in Fig. 20. For an optimal performance of the detector, the ROC curve is close to the upper left corner as far as possible [30]. In the ROC curve of Fig. 20, the excellent performance of the proposed method is clearly observed.

Furthermore, the ratio of carrier power to noise power (C/N_0) related to the signals extracted in the results was estimated, as follows [32-34]:

$$\frac{C}{N_0}(dB-Hz)=10.\log_{10}\left(\frac{\overline{I^2_{ACC}}}{Q^2_{ACC}}\right)+10.\log_{10}\left(\frac{NBW}{f_s\,.\tau}\right) \quad (4)$$

where I_{ACC} denotes the output of I accumulator, Q_{ACC} is the output of Q accumulator in the tracking section of GNSS receiver, NBW is the noise bandwidth at the intermediate frequency, f_s is the A/D sampling frequency, and τ is the accumulation period. In the present study, this value was calculated equal to 23.89 dB-Hz, which was approximated to the value of 24 dB-Hz. ROC curves for GNSS software receiver, MLP NN, and complex CNN structure (VGG16) for different C/N_0 are depicted in Figs. 21 and 22, respectively.

Comparing Figs. 20, 21, and 22, it can be concluded

Table 4 Comparison of the simulation results in this work with the simulation results of other references.

Comparison of reported NNs / Specifications	MLP NN presented in [9]	Complex CNN presented in [9]	CNN presented in [31]	CNN proposed in this work	MLP NN proposed in this work
Number of layers	-	41	13	16	10
The average accuracy of training after convergence	[60-70]	[95-100]	97.64	99.42	98.28
Number of learnable parameters	-	107,004,610	493,822	65,918	93,602
Number of activations per image data	-	27,973,252	16,921	2,448	1,816
Adjusted CAF image dimensions	20×1,023	20×1,023	9×9	2×4	2×4
GNSS data set	10,000	10,000	200,000	2,400	2,400

that the ROC curve is improved in Fig. 20, despite the low ratio of C/N_0.

5.1 Neural Network Performance

In addition to the accuracy of the training and losses of a NN, there are other criteria for examining the performance of a NN. These criteria include learning parameters and the number of activations per image data to investigate the complexity of the NN structure. Learning parameters in a NN are any parameters such as weights and thresholds that can be learned. The amount of memory that a NN consumes for training can be calculated from the number of activations in all layers. Due to the dependence of the memory consumed on other parameters and its approximation, we only rely on the learnable and activation parameter. In Table 4, the comparison is made between the results of the present work and the study done in [31] and [9]. For the sake of fair comparison, the reference NN results [31] were considered only in the Doppler frequency search step of 500 Hz and the code phase search step of 0.5 chip. It should be noted that there is not enough information on MLP NN structure in [9].

6 Conclusion

CAF images in the acquisition section of GNSS software receivers include a lot of information that can be used to detect spoofing attacks. Due to CAF images' high dimensions, MLP NN and CNN training by these images have high computational complexity. Also, training time and losses increased in case of a significant number of learning data. Before training the CNN and MLP NN, CAF image pre-processing was proposed using the modified LSA-transform method. This method reduced the dimensions of the CAF images. The results showed that the training time and losses of both MLP NN and CNN decreased, and training accuracy increased. The ROC curve presented in the results showed that the proposed method has a proper performance in detecting spoofing attacks above 0.25 chip distance. In the case of spoofing less than one chip distance, the accuracy of the proposed CNN was higher than that of the MLP NN. In addition, CNN has higher complexity than the MLP NN. Finally, by applying the proposed LSA-transform method, the number of learnable parameters and activations per image data was reduced. Therefore, the memory consumption was significantly reduced and the learning speed increased. Comparison of the presented results with other reported results showed that the proposed LSA-transform method can be considered as a proper pre-processing method on CAF images. The only limitation was that the proposed method has a low probability of detection and a high probability of false alarm in spoofing attacks less than 0.25 chip distance.

Intellectual Property

The authors confirm that they have given due consideration to the protection of intellectual property associated with this work and that there are no impediments to publication, including the timing of publication, with respect to intellectual property.

Funding

No funding was received for this work.

CRediT Authorship Contribution Statement

K. Zarrinnegar: Conceptualization, Methodology, Software, Data curation, Visualization, Investigation, Original draft preparation. **S. Tohidi:** Data curation, Visualization, Investigation. **M. R. Mosavi:** Supervision, Investigation, Reviewing and editing. **A. Sadr:** Supervision, Investigation, Reviewing and editing. **D. M. de Andrés**: Supervision, Investigation, Reviewing and editing.

Declaration of Competing Interest

The authors hereby confirm that the submitted manuscript is an original work and has not been published so far, is not under consideration for publication by any other journal and will not be submitted to any other journal until the decision will be made by this journal. All authors have approved the manuscript and agree with its submission to "Iranian Journal of Electrical and Electronic Engineering".

References

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

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

[3] M. Mosavi, Z. Nasrpooya, and M. Moazedi, "Advanced anti-spoofing methods in fracking loop," *Journal of Navigation*, Vol. 69, No. 4, pp. 883–904, 2016.

[4] M. Moazedi, M. Mosavi, and A. Sadr, "Real-time interference detection and mitigation in robust tracking loop of GPS receiver," *Analog Integrated Circuits and Signal Processing*, Vol. 95, No. 1, pp. 93–113, 2018.

[5] E. G. Manfredini, F. Dovis, and B. Motella, "Validation of a signal quality monitoring technique over a set of spoofed scenarios," in *7th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, pp. 1–7, 2014.

[6] A. Pirsiavash, A. Broumandan, and G. Lachapelle, "Two-dimensional signal quality monitoring for spoofing detection," in *Proceedings of the ESA/ESTEC NAVITEC 2016 Conference*, pp. 14–16, 2016.

[7] M. R. Mosavi and Z. Shokhmzan, "Spoofing mitigation of GPS receiver using least mean squares-based adaptive filter," *Iranian Journal of Electrical and Electronic Engineering*, Vol. 11, No. 3, pp. 184–194, 2015.

[8] M. Moazedi, M. R. Mosavi, and A. Sadr, "Real-time interference detection in tracking loop of GPS receiver," *Iranian Journal of Electrical and Electronic Engineering*, Vol. 13, No. 2, pp. 194–204, 2017.

[9] P. Borhani-Darian, H. LI, P. Wu, and P. Closas, "Deep neural network approach to detect GNSS spoofing attacks," in *Proceedings of the 2020 International Technical Meeting of The Institute of Navigation*, 2pp. 3241–3252, 020.

[10] T. Hu, M. Khishe, M. Mohammadi, G. Parvizi, S. H. T. Karim, and T. A. Rashid, "Real time COVID-19 diagnosis from X-ray images using deep CNN and extreme learning machines stabilized by chimp optimization algorithm," *Biomedical Signal Processing and Control*, Vol. 68, p. 102764, 2021.

[11] M. Naderan, E. Namjoo, and S. Mohammadi, "Trust classification in social networks using combined machine learning algorithms and fuzzy logic," *Iranian Journal of Electrical and Electronic Engineering*, Vol. 15, No. 3, pp. 294–309, 2019.

[12] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proceedings of the IEEE*, Vol. 104, No. 6, pp. 1258–1270, 2016.

[13] C. Hegarty, B. O'Hanlon, A. Odeh, K. Shallberg, and J. Flake, "Spoofing detection in GNSS receivers through cross-ambiguity function monitoring," in *Proceedings of the 32nd International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS)*, pp. 920–942, 2019.

[14] K. Wesson, D. Shepard, J. Bhatti, and T. Humphreys, "An evaluation of the vestigial signal defense for civil GPS anti-spoofing," in *Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS)*, pp. 2646–2656, 2011.

[15] S. Liu and W. Deng, "Very deep convolutional neural network-based image classification using small training sample size," in *3rd IAPR Asian Conference on Pattern Recognition (ACPR)*, pp. 730–734, 2015.

[16] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," *arXiv preprint arXiv:1409.1556*, 2014.

[17] 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.

[18] J. Chen, G. Bai, S. Liang, and Z. Li, "Automatic image cropping: a computational complexity study," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 507–515, 2016.

[19] A. S. Nsung, A. M. Bello, and H. Shamsudeen, "Image reduction assorted dimensionality reduction techniques," in *Proceedings of the Twenty-Sixth Modern Artificial Intelligence and Cognitive Science Conference*, pp. 139–146, 2015.

[20] S. Banerjee and A. Roy, *Linear algebra and matrix analysis for statistics*, 1st ed. Boca Raton: CRC Press, 2014.

[21] R. C. Gonzalez and R. E. Woods, *Digital image processing*, 3rd ed. Beijing: Publishing House of Electronics Industry, 2006.

[22] M. A. Joshi, *Digital image processing: An algorithmic approach*. PHI Learning Pvt. Ltd, 2018.

[23] 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.

[24] C. Mouton, J. C. Myburgh, and M. H. Davel, "Stride and translation invariance in CNNs," in *Southern African for Conference Artificial Intelligence Research (SACAIR)*, Vol. 1342, pp. 267–281, 2020.

[25] J. Schmidhuber, "Deep learning in neural networks: An overview," *Neural Networks*, Vol. 61, pp. 85–117, 2015.

[26] N. G. Polson and S. L. Scott, "Data augmentation for support vector machines," *Bayesian Analysis*, Vol. 6, No. 1, pp. 1–23, 2011.

[27] P. Toulis and E. M. Airoldi, "Asymptotic and finite-sample properties of estimators based on stochastic gradients," *Annals of Statistics*, Vol. 45, No. 4, pp. 1694–1727, 2017.

[28] 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.

[29] P. Borhani-Darian and P. Closas, "Deep neural network approach to GNSS signal acquisition," in *IEEE/ION Position, Location and Navigation Symposium (PLANS)*, pp. 1214–1223, 2020.

[30] C. Sun, J. W. Cheong, A. G. Dempster, H. Zhao, L. Bai, and 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.

[31] J. Li, X. Zhu, M. Ouyang, W. Li, Z. Chen, and Z. Dai, "Research on multi-peak detection of small delay spoofing signal," *IEEE Access*, Vol. 8, pp. 151777–151787, Aug. 2020.

[32] E. D. Kaplan and C. Hegarty, "Understanding GPS/GNSS: Principles and applications," Boston & Landan: Artech House, 1996.

[33] B. W. Parkinson and J. Spilker, Eds., *Progress in astronautics and aeronautics: Global positioning system: Theory and applications*. American Institute of Aeronautics and Astronautics, 1996.

[34] R. N. McDonough and A. D. Whalen, *Detection of signals in noise*. Academic Press, 1995.

K. Zarrinnegar received his B.Sc. degree in Electrical Engineering from Ferdowsi University of Mashhad (FUM) in 2020. He is currently pursuing the master's degree in Integrated Circuit and Electronics Engineering at Iran University of Science and Technology (IUST). His research interests include artificial intelligence, global navigation satellite system, signal acquisition, and GNSS anti-spoofing technology.

S. Tohidi received her B.Sc. and M.Sc. degrees in Electronic Engineering from respectively Shahid Beheshti University and Malek Ashtar University of Technology, Tehran, Iran. She is currently a Ph.D. Student in the Department of Electrical Engineering at Iran University of Science and Technology. Her research interests include signal processing, artificial intelligence, and GPS applications.

M. R. Mosavi received his B.Sc., M.Sc., and Ph.D. degrees in Electronic Engineering from Iran University of Science and Technology (IUST), Tehran, Iran in 1997, 1998, and 2004, respectively. He is currently a faculty member (Full Professor) of the Department of Electrical Engineering of IUST. He is the author of more than 450 scientific publications in journals and international conferences in addition to 12 academic books. His research interests include circuits and systems design. He is also editor-in-chief of "Iranian Journal of Marine Technology" and editorial board member of "Iranian Journal of Electrical and Electronic Engineering" and "GPS Solutions".

A. Sadr received the Ph.D. degree in Instrumentation from Department of instrumentation & Analytical Science (DIAS), University of Manchester Institute of Science and Technology (UMIST), Manchester, England in 2002. He is currently an Associate Professor in Electronic Engineering Department of Iran University of Science and Technology (IUST). His research interest includes nondestructive evaluation, medical instrumentation, and microprocessor & microcontroller- based systems design.

D. M. de Andrés received the B.Sc. degree in computer engineering and the M.Sc. degree in computer science from the Department of Informatics, Carlos III University of Madrid, Spain, where he received his Ph.D. degree in 2012. Now, he is a lecturer at the Department of Telematics of the Technical University of Madrid (UPM). His main research subjects, within the GISAI groups at UPM, are internet of things, cyber-physical systems, physically unclonable functions (PUFs), blockchain, knowledge management, information retrieval, and research methods.