IUST
Iran University of
Science and Technology

Iranian Journal of Electrical and Electronic Engineering

Journal Homepage: ijeee.iust.ac.ir

GPS Spoofing Detection using CAF Images and Neural Networks Based on the Proposed Peak Mapping Dimensionality Reduction Algorithm and TCNN Model

M. J. Jahantab*, S. Tohidi*, M. R. Mosavi*(C.A.), A. Ayatollahi*

Abstract: Global Positioning System (GPS)-based positioning has become an indispensable part of our daily lives. A GPS receiver calculates its distance from a satellite by measuring the signal reception delay. Then, after determining its position relative to at least four satellites, the receiver obtains its precise location in three dimensions. There is a fundamental flaw in this positioning system, namely that satellite signals at ground level are very weak and susceptible to interference in the bandwidth; therefore, even a slight interference can disrupt the GPS receiver. In this paper, spoofing detection based on the Cross Ambiguity Function (CAF) is used. Furthermore, a dimension reduction algorithm is proposed to improve the speed and performance of the detection process. The reduced-dimensional images are trained by a Convolutional Neural Network (CNN). Additionally, a modified CNN model as Transformed-CNN (TCNN) is presented to enhance accuracy in this paper. The simulation results show a 98.67% improvement in network training speed compared to images with original dimensions, a 1.16% improvement in detection accuracy compared to the baseline model with reduced dimensions, and a 9.83% improvement compared to the original dimensions in detecting spoofing, demonstrating the effectiveness of the proposed algorithm and model.

Keywords: GPS, Spoofing Detection, CAF, TCNN, Dimension Reduction Algorithm.

1 Introduction

FOR modern applications like intelligent transportation systems and location-based services to function and be implemented successfully, a continuous and accurate source of navigation, positioning, and timing information is crucial. Global Navigation Satellite Systems (GNSS) provide the primary source of this information, forming the backbone of Positioning, Navigation, and Timing (PNT) data [1-3], whenever available [4-6].

The Global Positioning System (GPS) has revolutionized navigation, replacing older location-based systems with its remarkable precision. Utilizing satellites, GPS seamlessly covers the entire Earth, enabling the accurate measurement of time, altitude, longitude, and latitude for any desired location. A GPS receiver requires simultaneous information from at least three satellites to calculate two-dimensional coordinates and determine latitude and longitude [7]. Additionally, it needs data from a minimum of four satellites to ascertain three-dimensional coordinates. All GPS signals originate from a fundamental frequency, f_0, approximately equal to 10.3 MHz [7]. These signals are transmitted on two radio frequencies within the Ultra-High Frequency (UHF) band, encompassing frequencies between 500 MHz and 3 GHz. These frequencies are designated as L1 and L2, derived from f_0 [8].

Due to the vast distance between satellites and Earth's surface, the low signal power level, the slow update rate,

Iranian Journal of Electrical & Electronic Engineering, 2024.
Paper first received 04 July 2024 and accepted 03 November 2024.

* The authors are with the School of Electrical Engineering, Iran University of Science and Technology (IUST), Narmak, Tehran 16846-13114, Iran.
E-mail: m_mosavi@iust.ac.ir.
Corresponding Author: M. R. Mosavi

and the radio navigation system, receivers are susceptible to interference from various radio frequency transmitters, either intentionally or unintentionally. The GPS signal structure is open to public ownership. Consequently, the signals can be entirely reconstructed and replicated, making them vulnerable to spoofing attacks, posing a threat to the system's security [9].

The vulnerability of GPS receivers to intentional interference makes them highly susceptible and at risk. This susceptibility provides opportunities for malicious actors aiming to compromise GPS-based systems or infrastructure, potentially leading to serious consequences. The lack of built-in security features in GPS systems exposes numerous applications to potential risks, as documented in various papers [10, 11]. Deliberate attacks on GPS receivers can be categorized into two types: physical attacks on the receiver (non-signal attacks) and attacks on the GPS signal-in-space level (signal attacks). Physical attacks involve tampering or manipulating the receiver, while signal attacks target the GPS signals transmitted by the satellites, causing disruption or degradation in the receiver's ability to accurately determine position, velocity, and timing [12]. The focus of this paper is on intentional attacks aimed at GPS signals, which can manifest in three distinct forms:

1. **Blocking**: This technique involves preventing satellite signals from reaching the receiver, which can be achieved simply by creating a gap between the antenna and the receiver.
2. **Jamming**: Jamming, interference generated by a jammer, degrades the receiver's accuracy or completely disrupts its ability to track the desired location. This type of attack is sometimes referred to as "denial of service."
3. **Spoofing**: In this attack, the adversary replaces authentic satellite signals with counterfeit ones. Spoofing is a more sophisticated attack compared to blocking and jamming due to its covert nature [8,9,13,14].

This work focuses on spoofing, a technique where counterfeit GPS-like signals are transmitted to manipulate the position output of the target receiver without disrupting GPS operations, effectively giving the attacker control over the receiver. It's important to distinguish this from jamming attacks, which aim to block GPS positioning services, while spoofing interference seeks to deceive the receiver into providing incorrect position information. These objectives are fundamentally different. The goal of this paper is to use the so-called Cross Ambiguity Function (CAF), computed by GPS receivers, to detect spoofing attacks. GPS receivers [15-19] utilize a statistical hypothesis test to determine the presence or absence of a signal from a specific satellite in the received signal, while also providing a basic estimate of the delay and Doppler frequency when the signal is detected. To perform this test, it is common practice to maximize the CAF between the received signal and a local code replica [20].

The remainder of the paper is organized as follows. Sections 2 and 3 presents a brief theoretical overview of GPS spoofing detection methods. In Section 4, a CNN-based GPS spoofing detection model is introduced. The proposed dimensionality reduction algorithm is presented in Section 5. The simulation results and performance of the proposed algorithm and model in detecting spoofing signals are presented in Section 6. Finally, the conclusions are drawn in Section 7.

2 Spoofing Detection Methods

Amongst various attack types, spoofing is considered the most perilous form of deliberate GPS interference. It deceives the GPS receiver by causing it to track counterfeit signals. Spoofing poses a greater threat than jamming, as the receiver is unable to detect the spoofing attack. In essence, spoofing is a stealthy attack where the spoofer misleads the receiver's location and time measurements by generating fake signals that mimic the original signals. Studies investigating the response of various GPS receiver types to spoofing signal threats have demonstrated the detrimental impact of such attacks on receiver measurements [14,21].

Fig. 1 illustrates the general occurrence of a spoofing attack. Each spoofing system, depending on its type, has a specific coverage area within which it can potentially divert GPS receivers. A GPS receiver under spoofing attack receives both genuine and spoofed signal sets simultaneously. The counterfeit signal is designed to overpower the authentic GPS signal, taking control of the unsuspecting receiver. Spoofing attacks and their countermeasures can be implemented at various receiver levels, including the data bit, acquisition, tracking, pseudo-range extraction, and navigation equation stages [9,22].

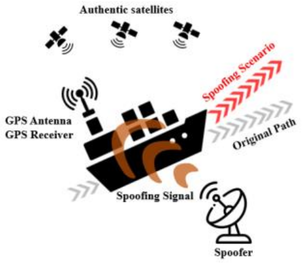


Fig. 1 General schematic of a spoofing attack.

In order to facilitate analysis, deception attacks are categorized into simple, moderate, and complex. In a simple deception, a fake signal simulator is used. In a moderate deception, a GPS receiver is embedded in the deceiver to receive signals from the environment. Then, a manipulated signal is transmitted by modifying the characteristics of the received signal and reproducing a signal based on the new characteristics. In a complex deception, multiple sophisticated deception systems are used in coordination with each other simultaneously [23,24].

For enhanced effectiveness of anti-spoofing techniques, a comprehensive understanding of spoofing methods and spoofer types is essential. Various approaches exist for spoofing detection and mitigation. These methods are designed to address the diverse scenarios involved in generating spoofed GPS signals. For instance, in a coordinated spoofing attack, the peak correlation of the spoofed signal is matched to the peak of the genuine signal. Subsequently, the power of the genuine signal is gradually increased. Finally, the gain of the spoofed signal tracks the delay lock loop gain to encompass the peak correlation and bring it under its control [25-27]. Consequently, anti-spoofing methods are tailored and implemented based on the specific type of spoofing attack.

In a spoofing attack, some or all of the received signal characteristics are compromised. The extent of GPS signal degradation presents an opportunity for spoofing detection. Therefore, by examining various characteristics of the GPS signal received by the target receiver, the presence of a spoofed signal can be inferred.

Fig. 2 illustrates the general process of creating a spoofing attack by a spoofing device in the presence of valid satellite signals and the countermeasure system. The spoofing detection stage focuses on distinguishing features between valid and spoofed signals.

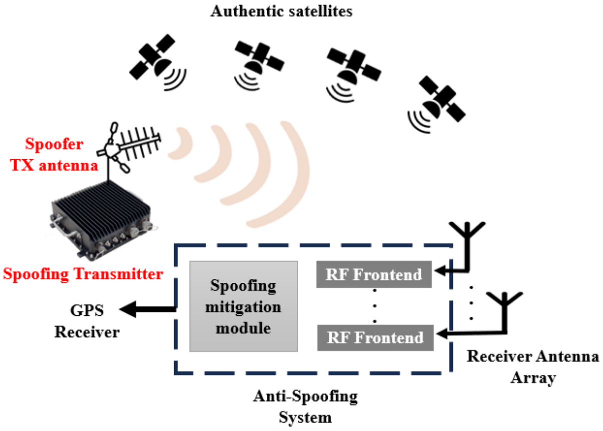


Fig. 2 General overview of a spoofing attack and anti-spoofing system.

Various methods have been developed for spoofing detection over the years. Some fall into the category of traditional methods, while others belong to intelligent spoofing detection methods. In 2012, authors in reference [28] conducted a comprehensive study on spoofing threats and introduced anti-spoofing methods into two main categories: spoofing detection and spoofing mitigation. According to related literature, actions taken toward spoofing detection and mitigation can be divided into four groups: anomaly detection in signal power [29,30], anomaly detection in time of arrival [31,32], spatial processing [33], and anomaly detection in correlation [34,35].

In recent years, researchers in the field of spoofing detection have introduced the application of artificial intelligence algorithms in various receiver components for spoofing detection and mitigation. These include references [22,36] that employed a multi-layer Neural Network (NN) for spoofing detection, and reference [37] that proposed machine vision techniques in this domain. References [38,39] treated CAF as an image and employed a Convolutional Neural Network (CNN) to detect spoofing interference. Building on this approach, reference [40] investigates the detection of spoofing attacks with delays less than two chips by examining the cross-ambiguity function in the receiver's acquisition unit. This method utilizes a CNN to analyze the merged peaks of the spoofed and genuine signals, enabling spoofing attack detection. Reference [41] estimates the clock bias using a multi-layer NN and compares the estimated value with the measured value to detect spoofing attacks.

In this paper, we propose a dimensionality reduction algorithm to utilize simpler networks and consequently improve detection speed, employing CAF images as matrix-based data for spoofing detection. We compare the results with the conventional method.

3 Cross Ambiguity Function

In the signal processing chain, the first step performed by a GPS receiver is signal acquisition. The outcome of this process determines whether a specific satellite signal exists in the received signal or not. It also provides an approximate estimate of the associated code delay and Doppler frequency if present. All GPS receivers execute such an acquisition process by evaluating what is known as CAF and maximizing it [20]. Therefore, one of the methods for spoofing detection is CAF-based detection [38,40].

CAF is a two-dimensional function that relates to the correlation between the received signal and the local replica for each possible delay/Doppler pair, which is then maximized for signal detection. In this process, two hypotheses are available: (1) the null hypothesis H0, which states that there is no signal present or it is not properly aligned with the local replica, and (2) the alternative hypothesis H1, which assumes that a signal is present and properly aligned with the local replica. When a GPS spoofing signal is present, more than one peak point is observed in the CAF images, whereas if only the genuine signal is present, a single peak point is observed in the CAF images (as shown in Figs. 1 and 2).

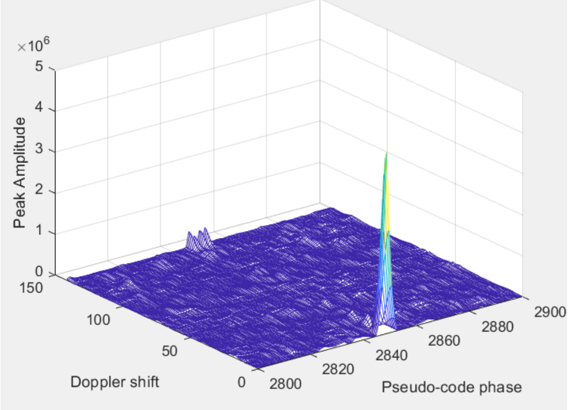


Fig. 3 CAF in the absence of spoofing signal.

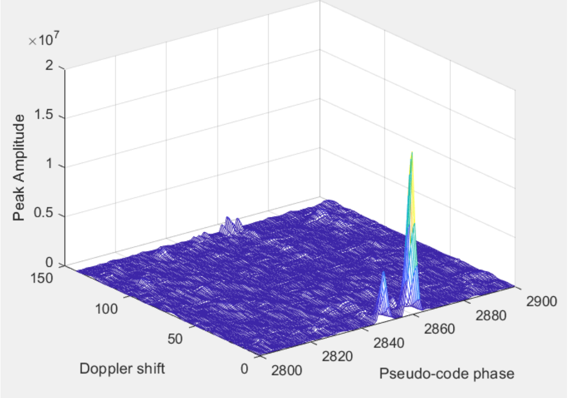


Fig. 4 CAF in the presence of spoofing signal.

4 NN-Based Spoofing Detection and Proposed Model

Detection of spoofing based on NNs has gained significant attention due to their capability to predict outputs of complex systems. Nowadays, with the advancement of intelligent methods, extensive research has been conducted in the field of spoofing detection in GPS systems using NNs. The input to the NN is defined based on feature vectors obtained from satellite systems, such as received signal strength and correlation function distortion, so that the designed NN, after necessary processing, can classify received satellite signals into categories such as jammed signals, spoofed signals, multi-path signals, or interference-free signals.

Researchers in reference [38] also discuss the use of deep learning architectures for spoofing detection. With the aim of utilizing the features of the CAF in the presence and absence of spoofed signals, a set of data-driven models that provide probabilistic classification are trained. Two classes, namely valid and spoofed signals, are defined based on the extracted CAF features, and signals corresponding to each scenario are classified into their respective classes. The model used in this paper is a complex CNN structure with 13 convolution layers.

In this paper, we adopt the general architecture depicted in Fig. 5, similar to references [38] and [39]. A more detailed structure is shown in Fig. 6. Furthermore, to improve accuracy, we propose a modified CNN model (TCNN) with a structure as depicted in Fig. 7.

The components of the transformer section are as follows:

• Multi-Head Attention Layer: The multi-head attention layer is a crucial component in the transformer model. This layer calculates attention scores between input data and itself. In this paper, the number of heads is set to 16, and the key dimensions are set to 64.

• Dropout: Dropout is a regularization technique that helps prevent overfitting. In this case, a dropout rate of 0.1 is applied to the output of the multi-head attention layer. This layer randomly sets some values to zero during training.

• Layer Normalization: Layer normalization is applied to the output of the dropout layer. This layer normalizes values independently for each feature dimension.

• Feed-Forward: After multi-head attention, the output is passed through a feed-forward layer. In this case, this layer consists of two fully connected layers, each with 64 units, and Re-Lu activation functions, which are a common choice for non-linear activation functions in deep learning models.

CAF images have high volume and dimensionality, making spoofing detection using CAF with AI methods time-consuming to train. While accurate detection is crucial, minimizing the network's spoofing detection time is equally important. Therefore, Section 6 proposes a dimensionality reduction algorithm for CAF images that preserves key features while reducing processing time and maintaining high detection accuracy.

5 Data Processing

The CAF images used in this paper have dimensions of 141 * 5714. Processing these dimensions is not only time-consuming, but also requires powerful graphics and processing equipment. To address these challenges, we propose a dimensionality reduction algorithm using image mapping. The steps for preparing the dataset with reduced dimensions for the NN input are as follows (as shown in Figs. 8 and 9):

Step 1: Iterate through the input 2D matrix, store the input matrix dimensions in (a, b), and find the P most prominent peaks in the matrix.

Step 2: Store the columns and rows of the P most prominent peaks found.

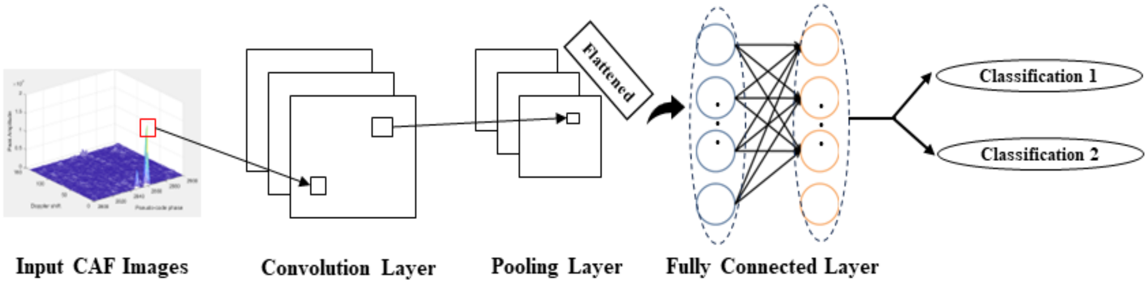


Fig. 5 CNN architecture.

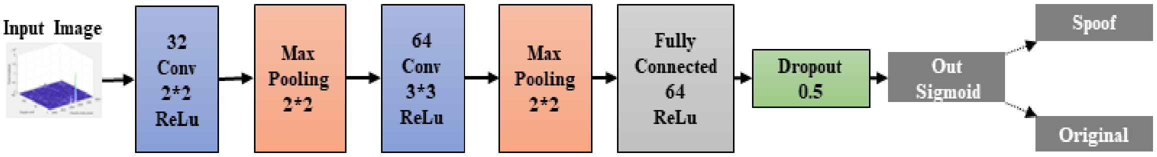


Fig. 6 Base network architecture.

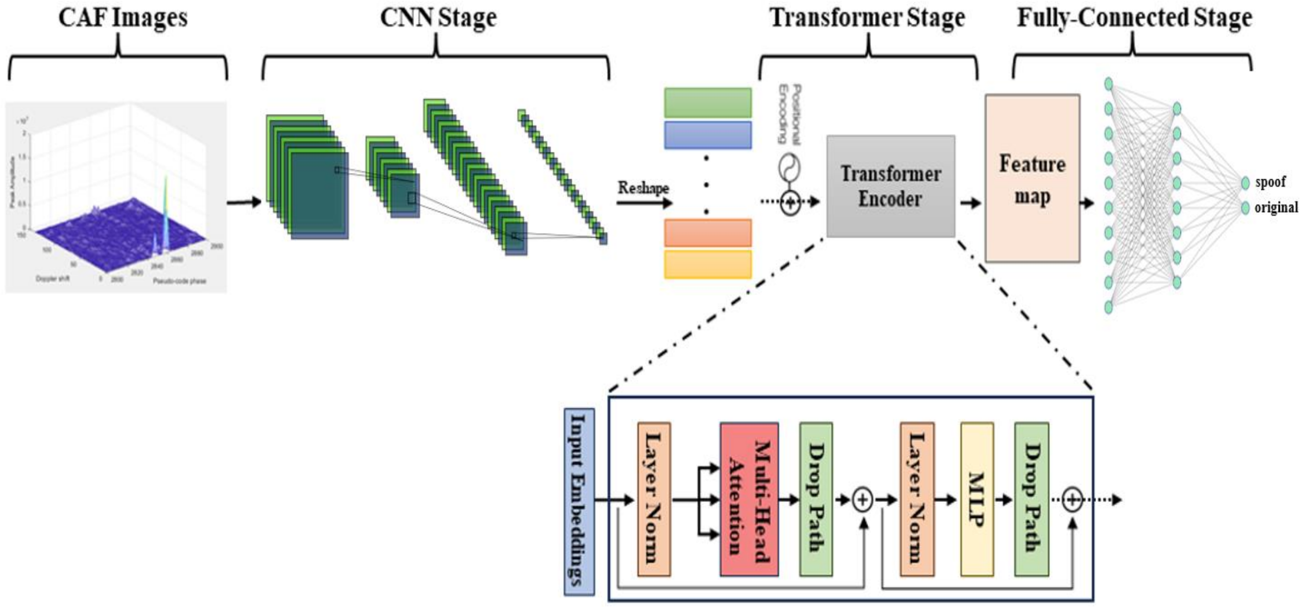


Fig. 7 Overall Structure of the proposed TCNN architecture.

Step 3: Obtain the desired dimensions of the reduced matrix and store them in (L, Q).

Step 4: Using an appropriate method, map these P most prominent peaks to the reduced matrix in a way that the positions of the found peaks indicate the range of the peaks in the original matrix.

Step 5: Feed the reduced matrix as input to the NN.

Figs. 10 and 11 illustrate the results of dimensionality reduction applied to a CAF image and a gray scale image for both real and spoofed signals, respectively.

As observed in Fig. 10, the images have been successfully reduced from dimensions of 141*5714 to 9*9. The key features of the images are preserved after dimensionality reduction, which contributes to faster spoofing detection.

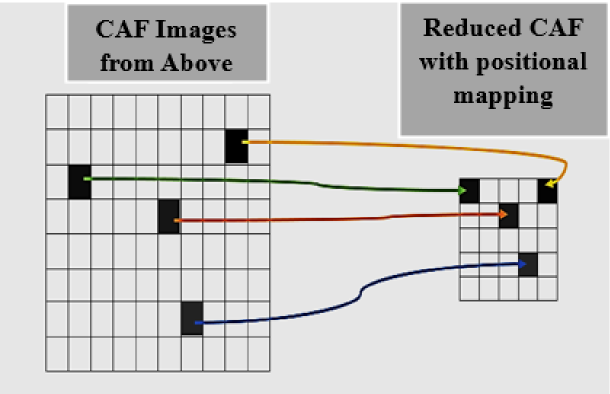


Fig. 8 A visualization of peak mapping.

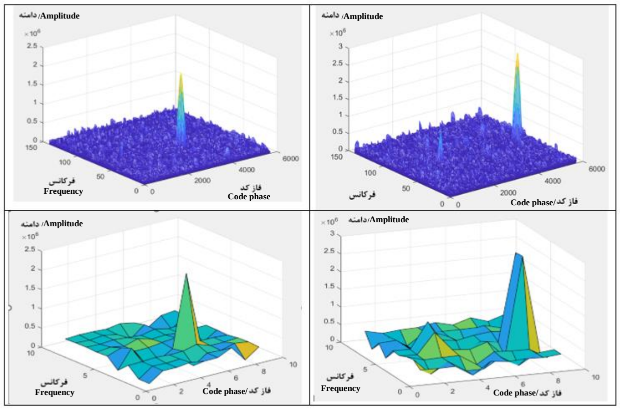


Fig. 10 The CAF image without using the dimensionality reduction algorithm (top) and the CAF image after dimensionality reduction (bottom) for the real signal (left) and spoofing with less than 0.5 chips (right).

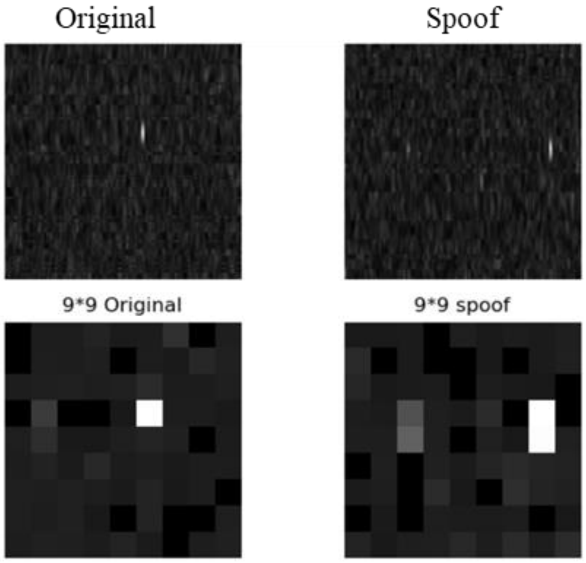


Fig. 11 Grayscale CAF images before (top) and after (bottom) dimensionality reduction for the original and spoofing signals.

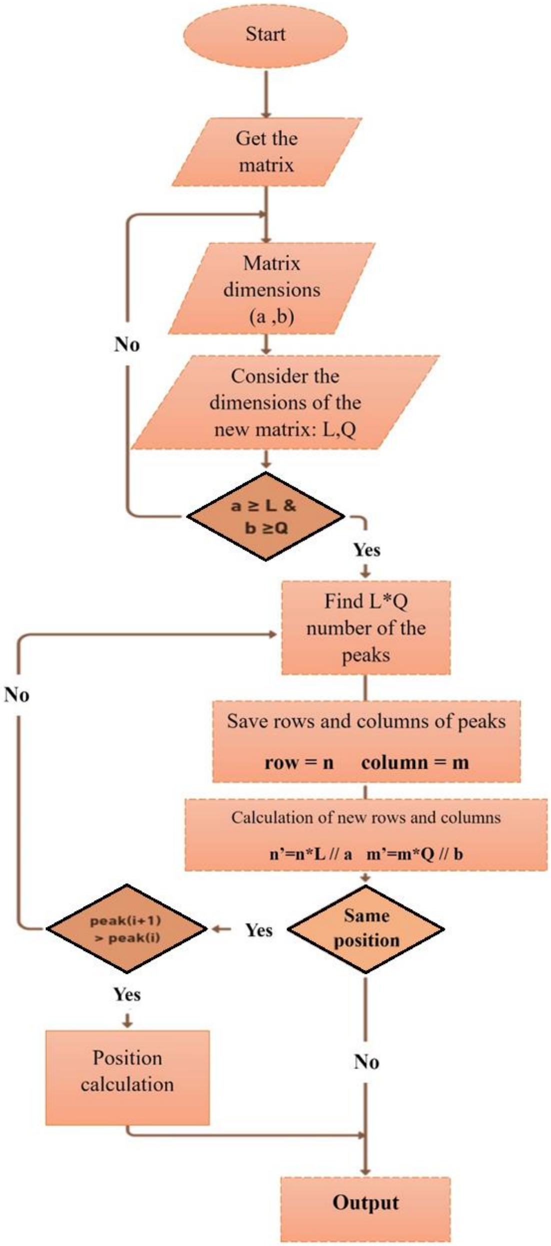


Fig. 9 Diagram of the proposed dimensionality reduction method.

6 Simulation Results

The proposed method was evaluated using a Software-Defined Radio (SDR) in MATLAB to generate CAF images as the dataset and Python software to implement the model and dimensionality reduction algorithm. Simulations were conducted on a laptop with the following specifications:

- Processor: Core i7-12650H 2.3 – 4.2 GHz
- Graphics card: RTX 3070
- RAM: 16GB

The proposed method was compared to a baseline model based on the architecture in [39], a proposed TCNN model with training parameters as shown in Table 1 and network architecture as shown in Table 2, and a method from [38] that utilizes a complex NN architecture similar to VGG16. The results were evaluated based on the following metrics:

Table 1 Training Parameters for TCNN.

Parameters	**Value**
Batch size	16
Learning rate	0.001
Epochs	100
Loss function	Binary cross entropy
Optimizer	Nadam

Table 2 Network architecture.

TCNN network	**Base network**
Conv layer 2*2 Re-Lu	Conv layer 2*2 Re-Lu
Max polling 2*2	Max polling 2*2
1. Multi-head attention Dropout 0.1 2. Layer normalization 3. Fully connected Re-Lu 4. Fully connected Re-Lu Dropout 0.1 5. Layer normalization	1. Conv layer 3*3 Re-Lu 2. Max pooling 2*2 3. Fully connected Re-Lu
Dropout 0.5	Dropout 0.5
Fully connected Sigmoid	Fully connected Sigmoid

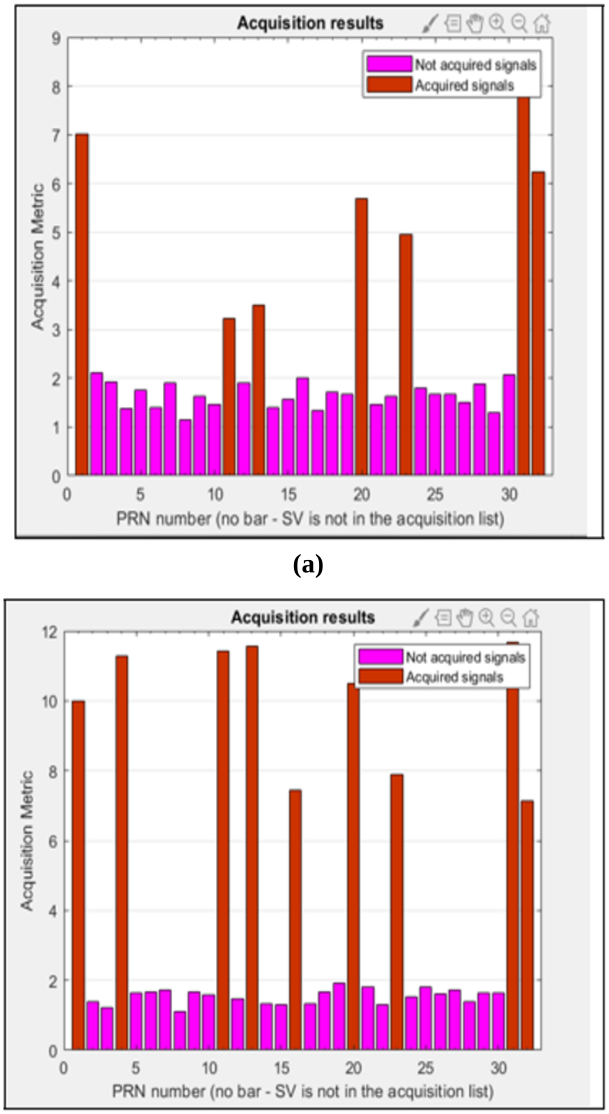
The dataset for this study consisted of 3507 CAF images from acquired PRNs as shown in Fig. 12. The dataset was divided into two classes:

- **Original Signal:** 1713 images representing the genuine PRN signals.
- **Spoofed Signal:** 1794 images representing the spoofed PRN signals.

The spoofing scheme employed in this work involved a six second delay of the original signal with itself. This delay was introduced using the Eq. (1):

$$S_S(t) = S_A(t) + S_A(t-6) \tag{1}$$

In Eq. (1), t denotes time in seconds, S_A (t) and S_S (t) denote the authentic satellite signal and spoofing signal, respectively.



(a)

(b)

Fig. 12 Acquisition results in the absence (a) and presence (b) of spoofed signals.

In the following, in Figs. 13 to 18, the results related to the simulation are provided.

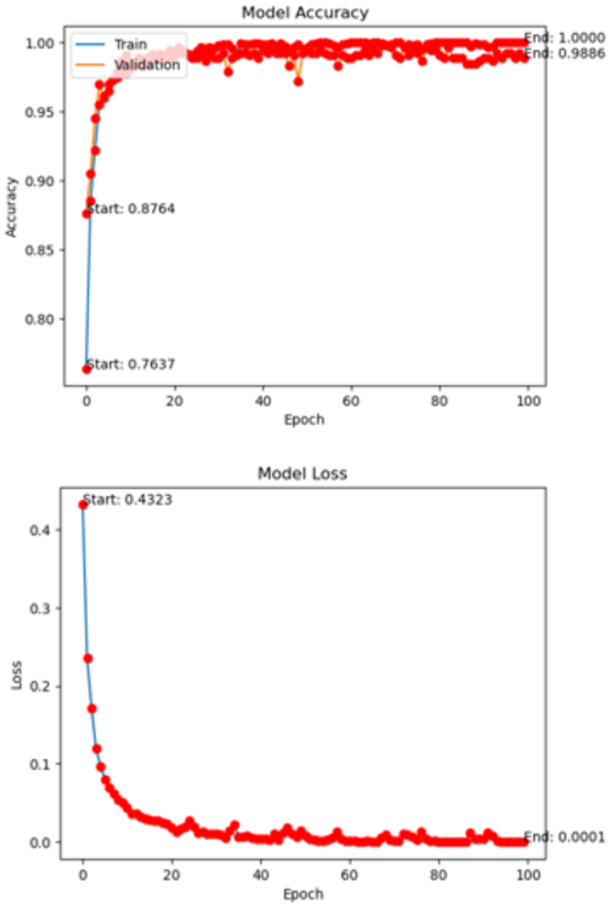


Fig. 13 Accuracy of CNN training with the application of dimensionality reduction algorithm for input images with dimensions 141 * 5714.

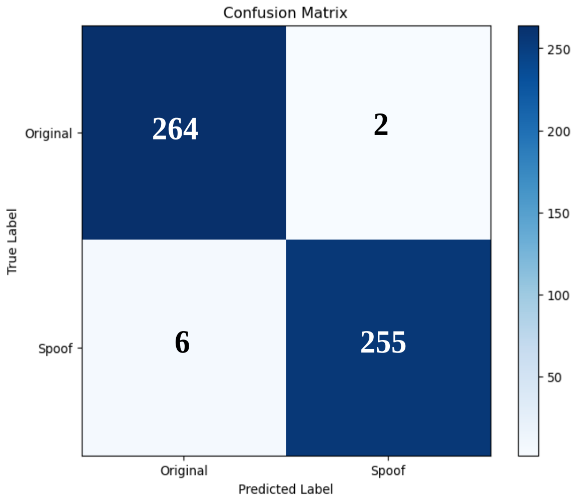


Fig. 14 Confusion matrix of the CNN model with the application of dimensionality reduction algorithm for input images with dimensions 141 * 5714.

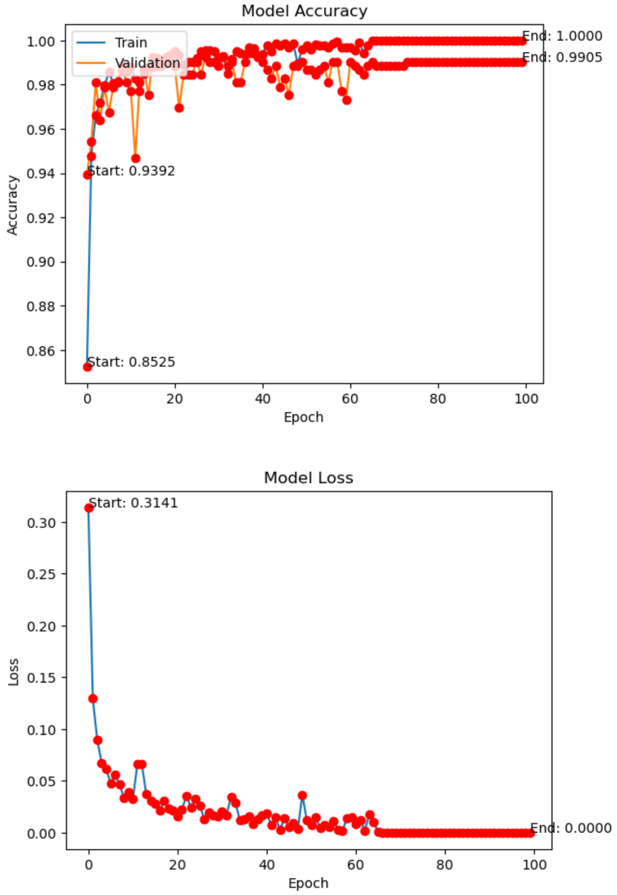


Fig. 15 Training accuracy of TCNN with the application of dimensionality reduction algorithm for input images with dimensions 141 * 5714.

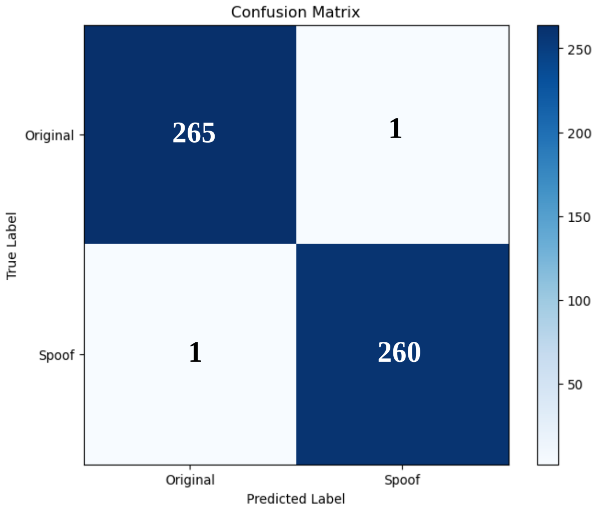


Fig. 16 Confusion matrix of the TCNN model with the application of dimensionality reduction algorithm for input images with dimensions 141 * 5714.

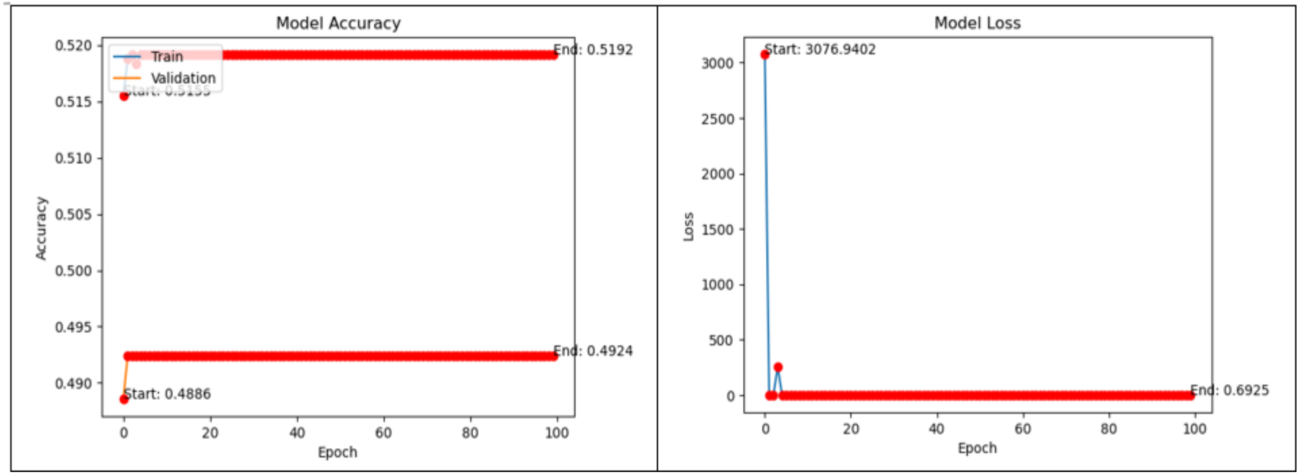


Fig. 17 Training accuracy of the CNN without applying the dimensionality reduction algorithm for input images with dimensions 141*5714.

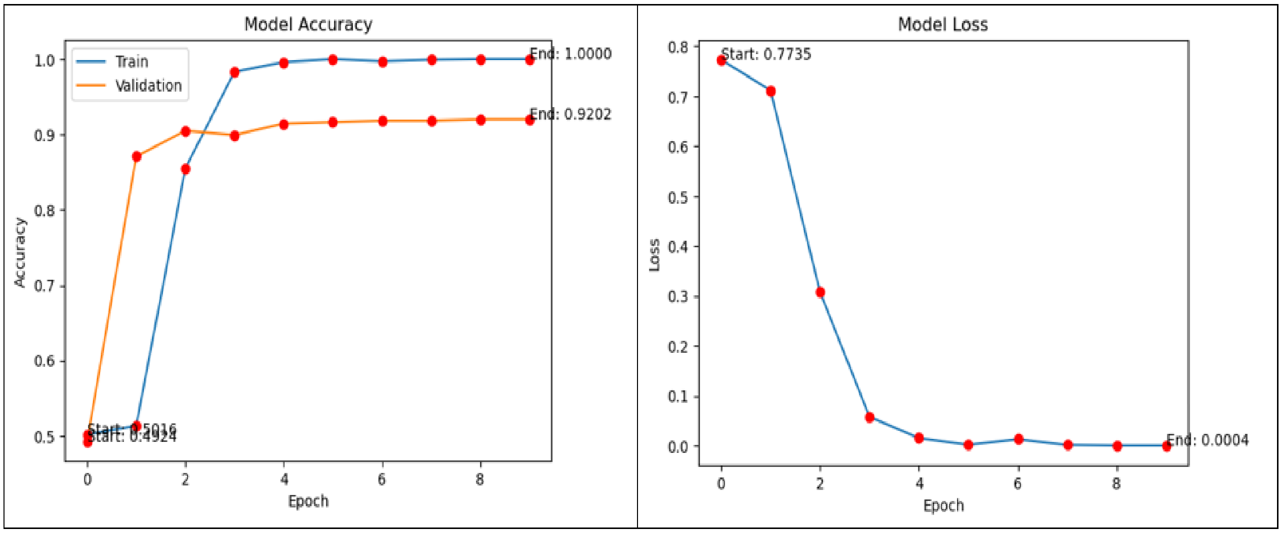


Fig. 18 Training accuracy of the TCNN without applying the dimensionality reduction algorithm for input images with dimensions 141*5714**.**

As illustrated in Figs. 13 to 18 and Table 3, employing the proposed dimensionality reduction algorithm in conjunction with the baseline CNN model leads to a significant improvement in test accuracy of 98.87% and a substantial reduction in total training time of 98.67% compared to using the original image dimensions.

The proposed TCNN model demonstrates superior classification performance compared to the baseline CNN model, even when using the original image dimensions. This improvement is evident in an 83.16% increase in accuracy.

Utilizing both the proposed dimensionality reduction algorithm and the TCNN model achieves even further improvements, surpassing the baseline CNN model with both original and reduced dimensions and the TCNN model with original dimensions. This combined approach results in accuracy enhancements of 99.24%, 1.16%, and 9.83%, respectively.

The proposed method outperforms existing approaches, achieving a 2% accuracy improvement over reference [39] and a 14.5% improvement over reference [38].

7 Conclusion

Processing CAF images with their original dimensions using a large dataset can significantly increase spoofing detection time. This can lead to inefficiencies in real-time applications. To address this challenge, we introduced a novel dimensionality reduction algorithm called peak mapping for reducing the dimensionality of CAF images. This algorithm not only significantly reduces detection time, but also enhances detection accuracy. To further improve accuracy, we proposed a modified CNN model, namely TCNN. The experimental results demonstrate that TCNN achieves a notable improvement in spoofing detection accuracy. The combination of the proposed dimensionality reduction algorithm and the TCNN model offers a promising approach for efficient and accurate spoofing detection in GPS signals. This approach significantly reduces processing time while maintaining high detection accuracy.

Table 3 Results Comparison.

	With dimension reduction and CNN model for 100 epochs	Without dimension reduction and CNN model for 100 epochs	With dimension reduction and TCNN model for 100 epochs	Without dimension reduction and TCNN model for 10 epochs
Test accuracy [%]	98.48	49.52	99.62	90.7
Training data accuracy at end of training [%]	100	51.92	100	100
Validation data accuracy at end of training [%]	98.86	49.24	99.24	92.92
Total training time for 100 epochs [s]	45	2790	90	458
Average training time per epoch [s]	0.4	30	1	42
Average training time per iteration [s]	0.003	0.2	0.006	0.27
Test data detection time [s]	0.001	1	0.002	1
Validation data loss at end of training	0.0001	0.6925	0.0000	0.0004

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

M. J. Jahantab: Conceptualization, Methodology, Software, Data curation, Visualization, Investigation, Original draft preparation. **S. Tohidi**: Data curation, Visualization, Investigation. **M. R. Mosavi and A. Ayatollahi**: Supervision, Investigation, Reviewing and editing.

Funding

No funding was received for this work.

Informed Consent Statement

Not applicable.

References

[1] D. Dardari, E. Falletti, and M. Luise, “Satellite and Terrestrial Radio Positioning Techniques: A Signal Processing Perspective,” Academic Press, Boston, 2011.

[2] M. G. Amin, P. Closas, A. Broumandan, and J. L. Volakis, “Vulnerabilities, Threats, and Authentication in Satellite-based Navigation Systems,” *Proceedings of the IEEE*, Vol. 104, No. 6, pp.1169-1173, 2016.

[3] D. Dardari, P. Closas, and P. M. Djurić, “Indoor Tracking: Theory, Methods, and Technologies,” *IEEE Transactions on Vehicular Technology*, Vol. 64, No. 4, pp. 1263-1278, 2015.

[4] N. Williams, P. B. Darian, G. Wu, P. Closas, and M. Barth, “Impact of Positioning Uncertainty on Connected and Automated Vehicle Applications,” *SAE International Journal of Connected and Automated Vehicles*, Vol. 6, No. 12-06-02-0010, pp. 155-168, 2022.

[5] Z. M. Kassas, P. Closas, and J. Gross, “Navigation Systems Panel Report Navigation Systems for Autonomous and Semi-autonomous Vehicles: Current Trends and Future Challenges,” *IEEE Aerospace and Electronic Systems Magazine,* Vol 34, No. 5, 2019.

[6] K. Yu, S. H. Fang, A. Broumandan, P. Closas, G. Retscher, and A. Dempster, “Apecial Section: Positioning and Navigation in Challenging Environments,” *IEEE Access,* Vol 11, pp. 12636-12639, 2023.

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

[8] 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.

[9] 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).

[10] R. Ioannides, T. Pany, and G. Gibbons, “Known Vulnerabilities of Global Navigation Satellite Systems, Status, and Potential Mitigation Techniques,” *Proceedings of the IEEE,* Vol 104, No. 6, pp.1174-1194, 2016.

[11] H. Sathaye, G. LaMountain, P. Closas, and A. Ranganathan, “Semperfi: Anti-spoofing GPS Receiver for UAVs,” in *Network and Distributed Systems Security (NDSS) Symposium,* 2022.

[12] F. Dovis, “GNSS Interference Threats and Countermeasures,” Artech House, Norwood, 2015.

[13] D. Borio, F. Dovis, H. Kuusniemi, and L. L. Presti, “Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers,” *Proc. IEEE*, Vol. 104, No. 6, pp. 1233-1245, Jun. 2016.

[14] T. E. Humphreys, J. A. Bhatti, and B. M. Ledvina, “The GPS Assimilator: a Method for Upgrading Existing GPS User Equipment to Improve Accuracy, Robustness, and Resistance to Spoofing,” in *Proceedings of the 23rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS),* Portland, OR, pp. 1942-1952, September 24, 2010.

[15] E. Kaplan, and C. Hegarty, “Understanding GPS: Principles and Applications,” Artech House, Norwood, 2005.

[16] P. Misra, and P. Enge, “Global Positioning System: Signals, Measurements and Performance,” Second Editions, 2006.

[17] J. B. Tsui, “Fundamentals of Global Positioning System Receivers: A Software Approach,” Wiley, Hoboken, 2005.

[18] D. Akos, J. Arribas, M. Z. H. Bhuiyan, P. Closas, F. Dovis, I. Fernandez-Hernandez, C. Fernández–Prades, S. Gunawardena, T. Humphreys, and Z. M. Kassas, “GNSS Software Defined Radio: History, Current Developments, and Standardization Efforts,” in *Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS),* pp. 3180-3209. 2022.

[19] P. Borhani-Darian, H. Li, P. Wu, and P. Closas, “Detecting GNSS Spoofing using Deep Learning,” *EURASIP Journal on Advances in Signal Processing*, No. 1, p. 14, 2024.

[20] D. Borio, “A Statistical Theory for GNSS Signal Acquisition,” Ph.D. Dissertation Polytecnico di Torino, 2008.

[21] 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," in *11th International Conference on Control, Automation and Systems*, pp. 1616-1619, Oct. 2011.

[22] E. Shafiee, M. R. Mosavi, and M. Moazedi, “Detection of Spoofing Attack using Machine Learning based on Multi-Layer Neural Network in Single Frequency GPS Recievers,” *The Journal of Navigation*, Vol. 71, No. 1, pp. 169-188, 2018.

[23] M. L. Psiaki and T. E. Humphreys, “GNSS Spoofing and Detection,” *Proceedings of the IEEE*, Vol.104, No. 6, pp. 1258-1270, 2016.

[24] Y. Gao, Z. Lv, and L. Zhang, “Asynchronous Lift-Off Spoofing on Satellite Navigation Recievers in the Signal Tracking Stage,” *IEEE Sensors Journal*, Vol. 20, No. 15, pp. 8604-8613, 2020.

[25] A. R. Baziar, M. Moazedi and M. R. Mosavi, “Analysis of Single Frequency GPS Receiver under Delay and Combining Spoofing Algorithm,” *Journal of Wireless Personal Communications*, Vol. 83, No. 3. pp. 1955-1970, 2015.

[26] M. R. Mosavi and Z. Shokhmzan, “Spoofing Mitigation of GPS Receivers using Normalized Least Mean Squares based Adaptive Filter,”

Iranian Journal of Electrical and Electronic Engineering, Vol.11, No.3, pp.1-11, 2015.

[27] A. J. Saarinen, “Students Hijack Luxury Yacht with GPS Spoofing,” *Journal of Secure Business Intelligence Magazine*, Vol. 30, pp. 81-91, July 2013.

[28] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, “GPS Vulnerability to Spoofing Threats and a Review of Anti-Spoofing Techniques,” *International Journal of Navigation and Observation*, Vol. 2012, Article ID 127072, pp. 1-16, 2012.

[29] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, “GPS Spoofer Countermeasure Effectiveness Based on Signal Strength, Noise Power and C/N0 Measurements,” *International Journal of Satellite Communications and Networking*, Vol. 30, No. 4, pp. 181-191, 2012.

[30] J. Nielsen, V. Dehghanian, and G. Lachapelle, “Efectiveness of GNSS Spoofng Countermeasure Based on Receiver CNR Measurements,” *International Journal of Navigation and Observation*, Vol. 2012, pp. 1-9, 2012.

[31] S. Lo, D. De Lorenzo, P. Enge, D. Akos, and P. Bradley, “Signal Authentication, a Secure Civil GNSS for Today,” *GNSS Magazine*, Vol.4, No. 5, pp. 30-39, 2009.

[32] C. Lo and P. K. Enge, “Authenticating Aviation Augmentation System Broadcasts,” in *IEEE/ION Position, Location and Navigation Symposium*, Indian Wells, pp. 1018-1025, CA, USA, Mar. 2010.

[33] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, “Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-Antenna Receiver Defence Against a Portable Civil GPS Spoofer,” in *Proc. of ION Int. Technical Meeting of the Institute of Nav*, Anaheim, pp. 124-130, CA, USA, Jan. 2009.

[34] M. Pini, M. Fantino, A. Cavaleri, S. Ugazio, and L. L. Presti, “Signal Quality Monitoring Applied to Spoofing Detection,” in *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS)*, pp. 1888-1896, 2011.

[35] M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, “An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers,” in *Proc. of ION Int. Technical Meeting of the Satellite Division*, pp. 698-701, Portland, OR, USA, Sept. 2010.

[36] S. Tohidi and M. R. Mosavi, “Effective Detection of GNSS Spoofing Attack using A Multi-Layer Perceptron Neural Network Classifier Trained by PSO,” *25th International Computer Conference, Computer Society of Iran (CSICC)*, Tehran, Iran, pp. 1-5, 2020.

[37] S. Semanjski, I. Semanjski, W. De Wilde, and A. Muls, “Use of Supervised Machine Learning for GNSS Signal Spoofing Detection with Validation on Real-world Meaconing and Spoofing Data-part I,” *Sensors*, Vol. 20, No. 4, 2020.

[38] P. Borhani-Daria, H. Li, P. Wu, and P. Closas, “Deep Neural Network Approach to Detect GNSS Spoofing Attacks,” in *Proceedings of the ION GNSS Conference*, pp. 3241-3252, Sept. 21-25, 2020.

[39] K. Zarrinnegar, S. Tohidi, M. R. Mosavi, A. Sadr, and D. M. de Andrés, “Improving Cross Ambiguity Function using Image Processing Approach to Detect GPS Spoofing Attacks,” *Iranian Journal of Electrical and Electronic Engineering*, Vol. 19, No. 1, 2023.

[40] 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, 2020.

[41] N. Orouji and M. Mosavi, “A Multi-Layer Perceptron Neural Network to Mitigate the Interference of Time Synchronization Attacks in Stationary GPS Receivers,” *GPS Solutions*, Vol. 25, No. 3, pp. 1-15, 2021.

M. J. Jahantab received his B.Sc. degree in Electrical Engineering from K. N. Toosi University of Technology (KNTU) in 2022. He is currently pursuing the master’s degree in Digital Electronic Engineering at Iran University of Science and Technology (IUST). His research interests include artificial intelligence, image processing, global positioning system, signal acquisition, signal processing and GPS 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 600 scientific publications in journals and international conferences in addition to 13 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. Ayatollahi received his B.S. degree from Iran University of science and technology, Tehran, Iran, in 1974, the M.Sc. and the PH.D. degrees from the university of Manchester Institute of Technology (UMIST), England in 1985 and 1989 respectively. He works as a professor in the department of Electrical Engineering, Iran university of science and technology, Tehran. His research interests are in the areas of Medical Instrumentation, Ultrasound in Medicine.