EAI Endorsed Transactions
on Energy Web

Research Article EAI.EU

Geo-Tagged Spoofing Detection using Jaccard Similarity

Shweta Koparde[1, *], Vanita Mane[1]

[1]Dept of Computer Engineering, Ramrao Adik Institute of Technology, D Y Patil Deemed to be University, Nerul, India

Abstract:

In recent years, position evaluation of mobile devices has developed as an essential part of social movement. Meantime, the criminals may interfere with the information of geographical position (geo-position), and they can adjust the geo-position for their convenience. Therefore, it is important to identify the authenticity of geo-position. In this paper, an instant messaging platform-based geo-tagged spoof image detection system is created using Jaccard similarity. With the help of a Fuzzy filter, the input, as well as spoofing images, are subjected to camera footprint extraction, and their corresponding outputs are fused by Dice Coefficient. Moreover, the input as well as spoofed images is subjected to geotagged process, and their corresponding geotagged input, and geotagged spoofed images are fused by Tanimoto similarity. At last, the fused images from Dice Coefficient, and Tanimoto similarity are employed for the spoof detection process, where the Jaccard similarity compares the two images using Dicerete Cosine Transform (DCT). Consequently, the spoofed images are detected, and their effectiveness is measured in terms of accuracy, False Positive Rate (FPR), and True Positive Rate (TPR), as well as the corresponding values are attained like 0.099, 0.892, and 0.896 respectively.

Key words: Spoofing detection, Dicerete Cosine Transform, Tanimoto similarity, Jaccard similarity, Fuzzy filter

Received on 17 July 2023, accepted on 12 October 2023, published on 26 October 2023

doi: 10.4108/ew.4239

[1]Corresponding author. Email: kopardeshweta21@gmail.com

1. Introduction

Images are essential in modern image processing applications, and it was widely used in numerous fields, like intelligence, crime detection, court, military, news, journalism, media, education, and the medical field. The use of numerous software packages causes image manipulation, making the image's truthiness extremely difficult to determine. These are commonly referred to as spoofed images [1]. In smart devices, users have initiated the saving of private details using their face image unlock sequence. In such cases, third-party authentication can collect personal information using spoofed images [2][3]. As a result, spoof [4] image detection is an important domain for validating image authenticity [5]. Furthermore, the advancement of modern instant messaging technology has enabled the modification of follow-up patterns upon artificial joint replacement [6]. The portion of media posted to the web is rising rapidly, since social networking sites have emotionally attached millions of Internet users, numerous people have incorporated these sites into their everyday lives. Social network services have evolved into a worldwide problem as their popularity has grown [7]. It is one of the important aspects of technology that enables people to generate, distribute, cooperate, and interact with each other. Because of the nature of this innovation, it is simple for individuals to produce and submit or interact with their work to a small group of people, a much larger audience, or the entire world. [8].

Location-based facilities are growing popular in the digital world. The operation of adding geographical information to the internet based on the current location of the mobile app is known as geotagging. Besides, it plays a vital role in people's daily lives [7]. The user's location on social network systems is a valuable source of information, allowing for several applications including social unrest forecasting, location-based service recommendation [9][10], as well as migration flow analysis [11]. Geographic information remains ineffective in assisting people to make social connections and managing social networks. Since geographic data is crucial for every person who lives in a community, not just in requesting locations, but also in numerous social life situations. [7]. Furthermore, the validity of geo-location data is more, if the geo-location spoofing

[12][13] method is widely used or criminals utilize false geo-position data, the negative impact of such malevolent variation will be incalculable [14]. In past decades, deep learning methods (DL), particularly deep convolutional neural networks (DCNN), have achieved outstanding results in spoof [15][16] detection processes and classification techniques. DL-based methods, as compared to traditional computer recognition approaches, eliminate the hand-crafted concept, and pipeline and have influenced several well benchmark assessments, such as the ImageNet Large Scale Visual Recognition Challenge (ILSVRC) [8]. In addition, the popularity of the DL method in computer vision has become a spike of research interest and exploring DL for addressing the issues of spoof image detection activities [17]. Aditya et al. (2023) introduced a novel fusion model, F2PMSMD, designed to identify fake profiles in multimodal social media datasets. The model collects various user information, such as profile pictures, username characteristics, and activity metrics, and uses a Genetic Algorithm (GA) for feature selection. It employs a combination of classifiers including Naïve Bayes, Multilayer Perceptron, Logistic Regression, Support Vector Machine, and Deep Forest. The F2PMSMD model achieves impressive performance with 98.5% accuracy, 94.3% precision, 94.9% recall, and a 94.7% F-measure, making it suitable for deployment on various social media platforms to detect fake profiles [24]. Mangla et al. (2023) present a low-cost EyeWriter system designed as an assisting aid for individuals who are unable to communicate verbally. The system allows users to form words and sentences by writing letters with their eyes, providing a voice to those who have difficulty speaking. It utilizes artificial intelligence, OpenCV, Python, Python frameworks, dlib, neural networks, and computer vision techniques. Importantly, the system is cost-effective and doesn't require specialized hardware. Simulation results indicate the system's feasibility for real-world deployment, offering promising prospects for improving the lives of non-verbal individuals [25].

The objective of this research is to make an effective system for detecting spoof images. This method utilized the dice coefficient for fusing the input image and the spoof image after the footprint extraction process. Similarly, the Tanimoto similarity is employed to fuse the geo-tagged input image as well as the geo-tagged spoofed image. Afterward, the fused images from dice coefficient and Tanimoto similarity are subjected to a Spoof image detection process using Jaccard similarity.

The key contributions of this paper are illustrated below:

- The spoofed image is detected by fusing the outcome of both the dice coefficient and Tanimoto similarity using Jaccard Similarity with DCT.

The portion of this paper configuration is as follows: Section 2 includes a review of the literature on conventional approaches to spoof image detection as well as their advantages and risks, to help the users to develop an extremely good module. Section 3 explains the problem statement and the proposed techniques are deliberated in section 4. Section 5 defines and discusses the proposed model's outcomes. Section 6 describes the conclusion part of this work.

2. Motivation

Geo-tagged spoofing is a cybercrime, in which the hackers utilize fake images instead of original images in order to gather geo-based information. Hence spoof image detection is needed, and a lot of conventional techniques were employed for the same. Still, they are expensive and time-consuming. Therefore, the cost-effective approach of similarity-based spoof image detection technique is used here.

2.1. Literature Survey

Seongkyun Jeong*et al.* [18] developed the Cumulative sum (CUSUM) -based Global Navigation Satellite System (GNSS) for image spoofing. This method was used to identify the spoofing signals excluding the use of any additional hardware setup, but its execution time was extremely high. Yongxin Liu *et al.* [19] devised the Deep Neural Network (DNN) for Reliable Identity Verification and Spoofing Detection. This method was considered to prevent other Cyber-Physical frameworks, but it was computationally complex. Sondos Fadl*et al*. [20] modeled the 2D CNN for video forgery detection. Here, a feature vector of the entire video was created using the fusion-based structural similarity index (SSIM). It was also used in real-world applications. Despite this, because of the complicated environment, this technique was unable to provide consistently improved results. Vinolin and Sucharitha [1] devised the Dual adaptive-Taylor-rider optimization-based deep CNN (DA-Taylor-ROA-based DCNN) for video forgery discovery. Here, the training process was short, but it did not segregate the nasty operation and blameless restoring behavior.

3. Problem Statement

Spoofed image detection refers to the way of determining original images. Here, the user gathers the input image $D_{1-input}$ and sent it to user B via social media (WhatsApp). The image received by B's phone is denoted as $D_{1-Spoofed}$. Then, it is tough to detect whether the original image is $D_{1-input}$ or $D_{1-Spoofed}$. Sometimes such mistakes happen when it is accumulated from social networks; therefore, geospatial image is used to improve performance. The Spoof image detection system is shown in figure 1.

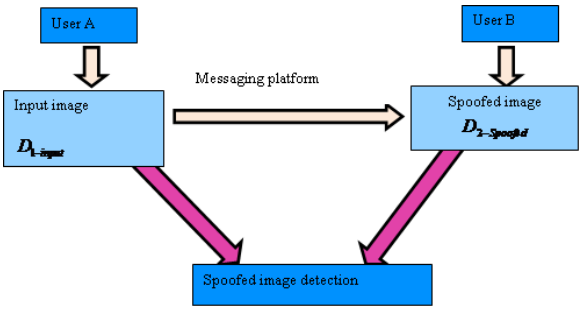


Figure1. Outline of the spoofed image detection

4. The proposed method for geo-position Spoofing Detection

The primary purpose of this research is to design and develop spoofing detection in an instant messaging platform using Jaccard similarity. Initially, each input image and spoof input image is subjected to the camera footprint extraction, which is done using a fuzzy filter [21]. Thus, the fuzzy filter output is considered as output-1 and output-2. Consequently, these two filtered outputs are fused using dice coefficient and it is considered as output 3. Afterward, the input image and spoof image with Geo-tagged are fused by Tanimoto similarity, where Tanimoto similarity output is considered as output 4. Finally, dice coefficient output and Tanimoto similarity output are transferred to the spoof image detection module. Here, a Spoof image is detected using Jaccard similarity [22]. Figure 2 illustrates the block diagram of spoofing detection in an instant messaging platform using Jaccard similarity.

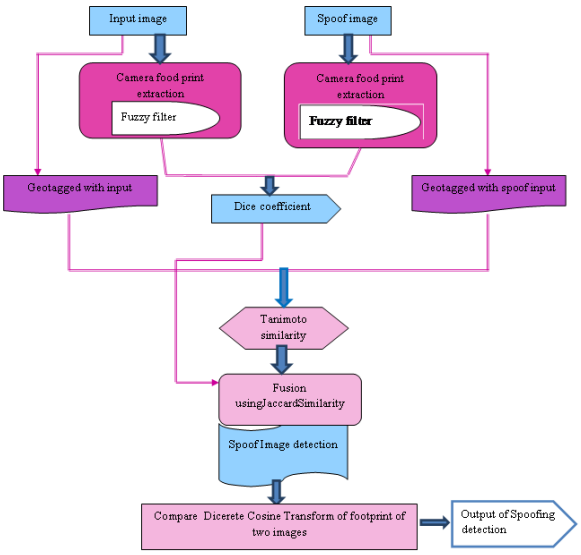


Figure 2. Shows the block diagram of spoofing detection in instant messaging platform using Jaccard similarity

4.1. Data Acquisition

Image acquisition is the primary step of image processing, and it is used to retire the image from the database. Here, the images attained from the dataset D is represented as,

$$D = \{D_1, D_2, ..., D_m, ...D_r\} \quad (1)$$

Here, the dataset D contains D_r images and the m^{th} image is indicated as D_m. Moreover, the image D_1 contains the input image $D_{1-input}$ and spoofed image $D_{1-Spoofed}$ for further processing. The original set of input images are denoted as $D_{1-input}$. The similar image D_1 is uploaded in social media, thus producing the corresponding spoofed image is called spoofed image $D_{1-Spoofed}$.

4.2. Camera footprint extraction

The images $D_{1-input}$ and $D_{1-Spoofed}$ are fed to the camera footprint extraction process. Here, the footprints are extracted using a fuzzy filter [21], and the operations of the filter is based on fuzzy rules. Furthermore, the fuzzy operator is made up of two cascaded subunits that use fuzzy reasoning. Here, the first subunit is termed as action detection module that detects noise pulses by taking luminance variances between the neighboring pixels, and the probable correction term is determined. Moreover, the second subunit is called as action adaptation module amends the correction values to progress the detailed preservation. Furthermore, this module is used to avoid minor luminance corrections, which are nearly unusable for minimizing the noise effects and degrade the quality of textures. Here, the input image $D_{1-input}$ and spoofed image $D_{1-Spoofed}$ are fed to fuzzy filtering, and the images that come after camera footprint extraction is denoted as $I_{footprint}$ (from input image) and $J_{foot\,print}$ (from spoofed image).

4.3. Fusion of camera footprint extracted images using Dice-Coefficient

For spoofed image detection, the footprint-extracted images $I_{footprint}$ and $J_{foot\,print}$ are fused by Dice-Coefficient. Moreover, the similarity between these two images is measured by a dice coefficient and is expressed below,

$$C(M,N) = \frac{2*|M \cap N|}{|M|+|N|} \quad (2)$$

where, $C(M,N)$ signifies the dice similarity measure, M denotes the footprint extracted input image $I_{footprint}$,

and N denotes the footprint extracted spoofed image $J_{footprint}$. The output image obtained by the dice coefficient is represented as SP_1.

4.3. Fusing of Geotagged input and spoofed input image using Tanimoto similarity

In this stage, the input image with geotagged, and the spoof image with geotagged are fused by the Tanimoto coefficient. The Tanimoto coefficient is a metric to measure the similarity of two images. It can be simply demarcated as the fraction of the intersection of the two sets of images over the union of those images. Moreover, the Tanimoto similarity of geo-tagged input and spoofed images are represented as,

$$T(R,X)=\frac{R.X}{\|R\|^2+\|X\|^2-R.X} \tag{3}$$

Where, R indicates the geo-tagged input image, and X represents the geo-tagged spoofed image. Moreover, the output image SP_2 is obtained.

4.4. Fusion of Dice Coefficient and Tanimoto similarity measured images

Fusion is the process of integrating two images into a single image that includes the characteristics of both images. Here, the image obtained using a dice coefficient and images comes from Tanimoto similarity are fused to obtain the new images SP, and it can be expressed as,

$$SP=\frac{1}{2}\left[SP_1+SP_2\right] \tag{4}$$

where, the output of the dice coefficient is denoted as SP_1, and the outcome of Tanimoto similarity is specified as SP_2.

4.5. Jaccard similarity for spoofed image detection

Jaccard Similarity [22] is a common proximity measurement used to evaluate the images as spoofed or not spoofed. If the fused image SP is less than the threshold value, it is considered as spoofed image. Otherwise, it is necessary to find which one of the images (input image $D_{1-input}$ or spoofed image $D_{1-Spoofed}$) is spoofed by applying certain conditions. Here, the Jaacard similarity is used to detect the spoofed image, where the following condition is employed to detect the spoofed image,

$$if \begin{pmatrix} Jaccard(DCT(I_{foot\,print}),DCT(Original) \\ < Jaccard\left(DCT\left(J_{foot\,print}\right),DCT\left(Original\right)\right) \end{pmatrix}, D_{1-in}$$

$$else$$

$$D_{1-Spoofed}\ \ is\ \ spoofed\ \ image \tag{5}$$

The Jaccard Similarity utilized the following mathematical expression to detect the spoofed image,

$$J(U,V)=\frac{|G\cap V|}{|G\cup V|} \tag{6}$$

where G indicates the original image, and V represents the footprinted image(it is either $I_{footprint}$ or $J_{foot\,print}$).

5. Results and discussion

The Jaccard similarity-based spoof image detection is accessed with the aid of metrics and its efficiency is revealed by comparing it with other existing approaches. Moreover, this section examines the Jaccard similarity-based spoof image detection method.

5.1. Experimental setup

Implementation of the proposed Jaccard similarity-based spoof detection is performed using MATLAB tool.

5.2. Dataset description

The assessment of Jaccard similarity-based spoofed image detection is performed using European Cities 1M database [23], in which 909,940 geo-tagged images are presented, and it was gathered from 22 European cities. A subclass of 1,081 images from Barcelona is categorized as 35 groups shown in a similar scene, where 17 groups indicate the landmark, and the remaining 18 groups are non-landmark scenes.

5.3. Evaluation metrics

The proposed Jaccard similarity-based spoofed image detection is examined to reveal its performance by employing various measures, like testing accuracy, FPR, and TPR, that are described here.

a) **Testing Accuracy**: The accuracy parameter is employed for describing the ratio of the exact value of Jaccard similarity-based spoofed image detection to the overall detection, and is given by,

$$Accuracy = \frac{\rho_1 + \rho_2}{\rho_1 + \rho_2 + \rho_3 + \rho_4} \quad (7)$$

where, the total count of spoofed images is specified as ρ_1 the number of reliable images are represented as ρ_2, ρ_3 denotes the number of images detected faultily as reliable images, and ρ_4 implies the total count of images faultily specified as spoofed images.

b) TPR: TPR is used to indicate the fraction of the definite number of spoofed images to the entire quantity of spoofed images identified, and is represented by,

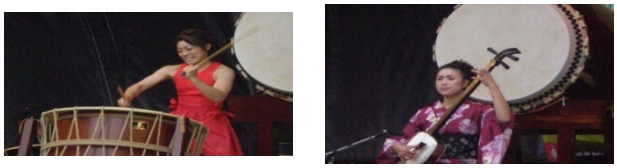
$$TPR = \frac{\rho_1}{\rho_1 + \rho_3} \quad (8)$$

a) FPR: FPR is calculated by the number of spoofed images grouped as positive and the entire quantity of spoofed images, it is expressed as,

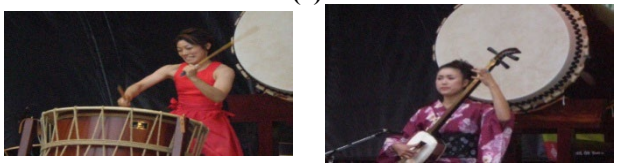
$$FPR = \frac{\rho_2}{\rho_2 + \rho_1} \quad (9)$$

5.4. Experimental result

The experimental result of Jaccard similarity-based spoof detection is displayed in figure 3. Here, the original image is shown in figure 3 a), and the original camera footprint image is deliberated in figure 3 b). Moreover, figure 3 c) denotes the spoofed input image, and figure 3 d) indicates a spoofed camera footprint image.



(a)



(b)

(c)

(d)

Figure 3. Experimental result of designed Jaccard similarity-based spoof detection a) original image b) original camera footprint image c) spoofed image d) spoofed camera footprint image

5.5. Comparative techniques

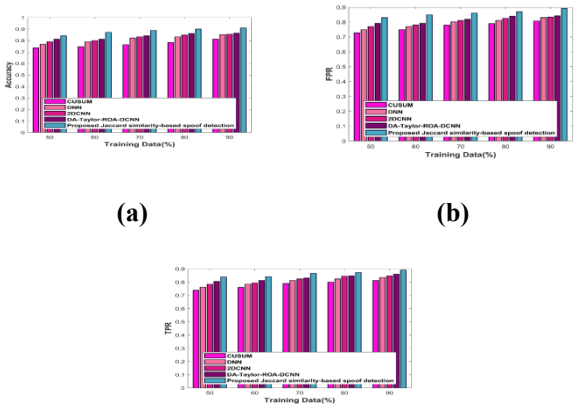
The effectiveness of Jaccard similarity-based spoof detection is evaluated and it compares with various traditional techniques, such as CUSUM [18], DNN [17], 2DCNN [20], DA-Taylor-ROA-based DCNN [1] to reveal the enhanced performance of the developed method with numerous assessment metrics, like accuracy, TPR and FPR.

5.6. Comparative assessment

The Jaccard similarity-based spoof detection ion is examined by comparing its performance with the numerous existing approaches to training data, and K-fold variation.

i) Assessment using training data

In figure 4, an analysis of Jaccard similarity-based spoof detection is performed in terms of training data variation. Here, the metrics like accuracy, FPR, and TPR are employed to reveal the performance. Figure 4 a) demonstrates the assessment related to the accuracy parameter using training data variation. At 60% training data, the accuracy of Jaccard similarity-based spoof detection is 0.871, while the accuracy is less in other existing approaches such as 0.745 for CUSUM, 0.789 for DNN, 0.799 for 2DCNN, and 0.810 for DA-Taylor-ROA-based DCNN. Here, the Jaccard similarity-based spoof detection reached 14.44%, 9.497%, 8.262%, and 7.027% of a performance improvement than other existing techniques. In FPR-based evaluation, the Jaccard similarity-based spoof detection is displayed in figure 4 b). Here, the FPR of 0.870 is achieved by Jaccard similarity-based spoof detection method, and the other existing approaches gathered the value of 0.789, 0.811, 0.825, and 0.839 respectively. Therefore, Jaccard similarity-based spoof detection provided 9.317%, 6.807%, 5.137%, and 3.585% of improved performance than others. Likewise, in TPR-based evaluation using 50% of training data is shown in figure 4 c). Here, the proposed Jaccard similarity-based spoof detection attained the TPR of 0.838, and the other existing techniques achieved values like 0.738 0.761, 0.783, and 0.804. This shows the performance of Jaccard similarity-based spoof detection is 11.96%, 9.173%, 6.631%, and, 4.09% better than other approaches.



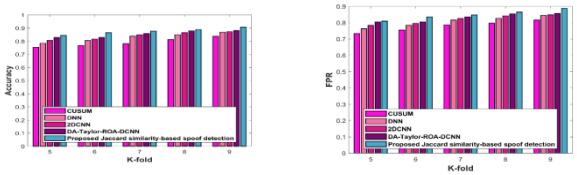
(a) (b)

(c)

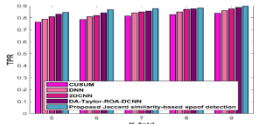
Figure 4. Comparative evaluation of Jaccard similarity-based spoof detection with respect to training data variation a) Accuracy b) FPR c) TPR

ii) Assessment considering K-Fold values

The assessment of Jaccard similarity-based spoof detection related to the K-Fold value is displayed in figure 5. Here, the accuracy, FPR, and TPR metrics are considered for performance estimation. In figure 5 a), the accuracy-based assessment is displayed. If the K-Fold =6, the accuracy of Jaccard similarity-based spoof detection is 0.864, while the accuracy value is 0.767, 0.806, 0.817, and0.828 in CUSUM, DNN, 2DCNN, and DA-Taylor-ROA-based DCNN methods. Hence, the proposed Jaccard similarity-based spoof detection achieved 11.27%, 6.746%, 5.486%, and 4.232% of a performance improvement than other existing techniques. Likewise, the FPR-related estimation is deliberated in figure 5 b). If the K-Fold value is set as 9, the FPR value of Jaccard similarity-based spoof detection is 0.887, where the other existing techniques attained the FPR values of 0.816, 0.845, 0.848, and 0.857 respectively. Moreover, the performance improvement of 8.084%, 4.768% 4.38278%, and 3.440% is attained by Jaccard similarity-based spoof detection. In addition, the TPR-related comparative assessment is deliberated in figure 5 c). Here, the TPR values of 0.785, 0.809, 0.820, 0.839, and 0.867 are obtained by CUSUM, DNN, 2DCNN, DA-Taylor-ROA-based DCNN, and Jaccard similarity-based spoof detection methods. Here, the Jaccard similarity-based spoof detection method attained 9.403%, 6.662%, 5.421%, and 3.206% of a performance improvement than other existing techniques.



(a) (b)



(c)

Figure 5. Comparative evaluation of Jaccard similarity-based spoof detection with respect to different K-Fold values a) Accuracy b) FPR c) TPR

5.7. Analysis with AUC score

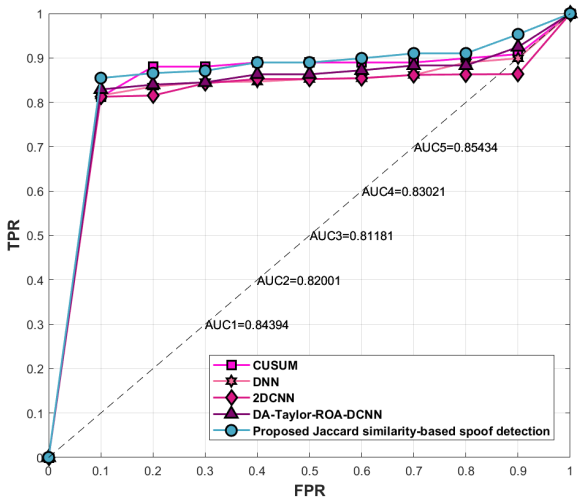


Figure 6. AUC-ROC score study

Figure 6 shows the AUC score study. Assuming FPR=0.9, the TPR produced by the proposed Jaccard similarity-based spoof detection is 0.9532, while those for CUSUM is 0.90, DNN is 0.899, 2DCNN is 0.86, DA-Taylor-ROA-DCNN is 0.924.

5.8. Analysis using confusion matrix

Table 1. Confusion matrix

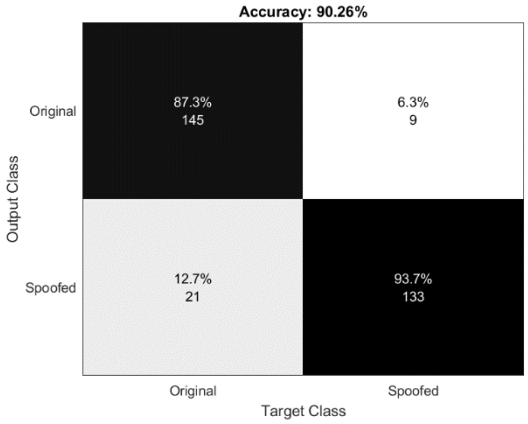


Table 1 illustrates the confusion matrix of the proposed Jaccard similarity-based spoof detection. Out of 308 images, the proposed technique correctly predicted 145 images as original images, and 133 images as spoofed images.

5.9. Comparative discussion

This section describes the comparative discussion of Jaccard similarity-based spoof detection. The devised approach is examined to reveal its effectiveness relating to numerous existing techniques in terms of training data, and k-fold. The valuation is performed by means of accuracy, FPR, and TPR, and the estimated values are presented in Table 2. Hence, it is noted that the proposed method attained the finest accuracy of 0.909, FPR of 0.892, and TPR of 0.891 in 90% training data. Moreover, the maximum accuracy, FPR, and TPR values of 0.907, 0.887, and 0.896 are obtained when the K-Fold value=9.

Table 2. Comparative result of Jaccard similarity-based spoof detection

Variations	**Metrics**	**CUSUM**	**DNN**	**2DCNN**	**DA-Taylor-ROA-based DCNN**	**Jaccard similarity-based spoof detection**
Training data	***Testing accuracy***	0.811	0.851	0.854	0.863	0.909
	FPR	0.808	0.829	0.833	0.841	0.892
	TPR	0.811	0.834	0.847	0.859	0.891
K-Fold	***Testing accuracy***	0.838	0.869	0.873	0.881	0.907
	FPR	0.816	0.845	0.848	0.857	0.887
	TPR	0.837	0.861	0.874	0.886	0.896

6. Conclusion

The instant messaging platform-based geo-tagged spoofing detection system is employed to avoid the occurrence of cybercrime activities. In this work, image spoofing detection is developed by Jaccard similarity-based technique. The presents of Fuzzy filter offered the footprint extraction of input as well as a spoofed image from the corresponding input and spoofed images. Moreover, the Dice Coefficient provided the fusion process effectually. Likewise, the Tanimoto similarity fused the geo-tagged input, and geo-tagged spoof images come after the footprint extraction process. For measuring the similarity of fused images from Dice Coefficient, and Tanimoto similarity, Jaccard similarity is employed here. Furthermore, the utilization of DCT performs the spoof image detection process. Therefore, the spoofed images are detected, and their efficiency is revealed to accuracy, FPR, and TPR, where the superior value of accuracy, TPR, and FPR are 0.909, 0.892, and 0.891. In the future, various hybrid DL techniques as well as different optimization techniques will be employed to enhance the performance of the system with more precise output.

References

[1] Vinolin V, Sucharitha M, Dual adaptive deep convolutional neural network for video forgery detection in 3D lighting environment. The Visual Computer 2021, 37(8), 2369-2390.

[2] Taneja A, Tayal A, Malhorta A, Sankaran A, Vatsa M, Singh R,: Fingerphoto spoofing in mobile devices: a preliminary study. In proceedings of IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS) 2016, 1-7.

[3] Koh J.Y, Nevat I., and Wong L.: Geo-Spatial Location Spoofing Detection for Internet of Things. IEEE Internet of Things Journal 2016.

[4] Zhou W, Lv Z, Deng X, and Ke Y.: A New Induced GNSS Spoofing Detection Method Based on Weighted Second-Order Central Moment. IEEE Sensors Journal 2022, 22(12), 12064-12078.

[5] Jayan T.J, Aneesh R.P: Image quality measures-based face spoofing detection algorithm for online social media. In proceedings of 2018 International CET Conference on Control, Communication, and Computing (IC4), 2018, 245-249.

[6] Zheng Q.Y, Geng L, Ni M, Sun J.Y, Ren P, Ji Q.B, Li J.C, Zhang G.Q: Modern instant messaging platform for postoperative follow-up of patients after total joint arthroplasty may reduce re-admission rate. Journal of Orthopaedic Surgery and Research 2019. 14, 1-9.

[7] Huang Q, Liu Y. On geo-social network services. In proceeding of 2009 17th International Conference on Geoinformatics, 2009, 1-6.

[8] Lee I, Cai G, Lee K.: Exploration of geo-tagged photos through data mining approaches. Expert Systems with Applications 2014, 41(2), 397-405.
[9] Bao J, Zheng Y, Wilkie D, Mokbel M.: Recommendations in location-based social networks: a survey. Geo Informatica 2015, 19, 525-565.
[10] Compton R, Lee C, Lu T.C, De Silva L, Macy M.: Detecting future social unrest in unprocessed twitter data:"emerging phenomena and big data". In procedings of 2013 IEEE International Conference on Intelligence and Security Informatics 2013, 56-60.
[11] Deligiannis N, Huu T.D, Nguyen D.M, Luo X.: Deep learning for geolocating social media users and detecting fake news. In NATO Workshop 2018.
[12] Varshosaz M, Afary A., Mojaradi B, Saadatseresht M, and Parmehr E.G. Spoofing Detection of Civilian UAVs Using Visual Odometry. International Journal of Geo-Information 2020, 9(1).
[13] Gao Y, and Li G. A Slowly Varying Spoofing Algorithm Avoiding Tightly-Coupled GNSS/IMU With Multiple Anti-Spoofing Techniques. IEEE Transactions on Vehicular Technology 2022, 71(8).
[14] Qiao T, Zhao Q, Zheng N, Xu M, Zhang L.: Geographical position spoofing detection based on camera sensor fingerprint. Journal of Visual Communication and Image Representation 2021, 81, 103320.
[15] Ke Y, Lv Z, Zhang C, Deng X, Zhou W, and Song D. Tightly Coupled GNSS/INS Integration Spoofing Detection Algorithm Based on Innovation Rate Optimization and Robust Estimation. IEEE Access 2022,10, 72444-72457.
[16] Gao Y. and Li G.: Two Time Spoofing Algorithms on GNSS Receiver Instrumentation of Modifying Satellite Clock Correction Parameters in Navigation Message. IEEE Transactions on Instrumentation and Measurement 2023, 72.
[17] Sun X, Wu P, Hoi S.C. Face detection using deep learning: An improved faster RCNN approach. Neuro computing 2018, 299, 42-50.
[18] Jeong S, Kim M, Lee J.: CUSUM-based GNSS Spoofing Detection Method for Users of GNSS Augmentation System. International Journal of Aeronautical and Space Sciences 2020, 21(2), 513-523.
[19] Liu Y, Wang J, Niu S, Song H.: Deep learning enabled reliable identity verification and spoofing detection. In proceeding of International Conference on Wireless Algorithms, Systems, and Applications, 2020, 333-345.
[20] Fadl S, Han Q, Li Q.: CNN spatiotemporal features and fusion for surveillance video forgery detection. Signal Processing: Image Communication2021, 90, 116066.
[21] Kwan H.K. Fuzzy filters for noisy image filtering. In Proceedings of the 2003 International Symposium on Circuits and Systems, ISCAS'03 4, IV-IV 2003).
[22] Cha S.H.:Comprehensive survey on distance/similarity measures between probability density functions. City 2007, 1(2), 1.
[23] European Cities 1M dataset available at, http://image.ntua.gr/iva/datasets/ec1m/index.html accessed on December 2022
[24] Aditya, B.L.V.S., Rajaram, G., Hole, S.R., Mohanty, S.N. (2023). F2PMSMD: Design of a Fusion Model to Identify Fake Profiles from Multimodal Social Media Datasets. In: Nandan Mohanty, S., Garcia Diaz, V., Satish Kumar, G.A.E. (eds) Intelligent Systems and Machine Learning. ICISML 2022. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 471. Springer, Cham. https://doi.org/10.1007/978-3-031-35081-8_2
[25] Mangla, M., Sayyad, A., Shama, N., Mohanty, S.N., Singh, D. (2023). An Artificial Intelligence and Computer Vision Based EyeWriter. In: Swarnkar, T., Patnaik, S., Mitra, P., Misra, S., Mishra, M. (eds) Ambient Intelligence in Health Care. Smart Innovation, Systems and Technologies, vol 317. Springer, Singapore. https://doi.org/10.1007/978-981-19-6068-0_43