Face-Anti-spoofing Based on Liveness Detection

Shivani Mangal and Khushboo Agarwal

Abstract Many applications, like crossing points, banking, and mobile banking, are now using Face Recognition (FR) systems. The widespread usage of FR systems has heightened concerns about the security of face biometrics against spoofing assaults, in which a picture or video of a valid user's face is employed to attain unauthorized access to resources or activities. Even though numerous FAS or liveness detection techniques (which identify if a face is live or spoofed at the moment of acquisition) have been developed, the problem remains unsolved because of the complexity of identifying discriminatory and operationally affordable spoof characteristics and approaches. Furthermore, particular facial sections are frequently repetitive or correspond to image clutter, resulting in poor overall performance. This paper proposed a neural network model for face-anti-spoofing which outperforms the other models and shows an accuracy of 0.91%.

Keywords Face Anti Spoofing · Face recognition · Convolutional neural network

S. Mangal (✉) · K. Agarwal
Computer Science and Engineering, Madhav Institute of Technology and Science, Gwalior, India
e-mail: 122shivanimangal@gmail.com

K. Agarwal
e-mail: ka.agarwals@mitsgwalior.in

J. Hemanth et al. (eds.), *Intelligent Cyber Physical Systems and Internet of Things*,
Engineering Cyber-Physical Systems and Critical Infrastructures 3,
https://doi.org/10.1007/978-3-031-18497-0_19

1 Introduction

Biometrics technology has gained in popularity as a result of the quick expansion of Internet technologies, and it is now extensively used in intelligence protection, criminal proceedings, financial and social stability, clinical training, and other disciplines. The face identification system is more simply accepted by the public than extant biometric identification systems owing to its excellent security, genuineness, and non-contact, and has formed an important research path for academics and industries [1]. The face recognition (FR) technology, on the other hand, is open to malware activity by unauthorized users, posing a serious threat to the system's integrity. As a result, creating a facial anti-spoofing system with higher identification performance, quick response time, and high robustness is critical [2].

The method of determining whether the recently collected facial picture is from a living human or a deceiving face is known as face anti-spoofing (FAS) detection. FAS research has been particularly engaged in recent times both domestically and overseas, owing to its significant academic significance. Printing, video replay and 3D mask attacks are the most popular spoofing assaults. Real and misleading faces have some variations, which are mostly expressed in image texture data, movement details, and perspective details [3]. We can create several FAS systems to identify the actual and counterfeit faces by taking benefit of these distinctions. FAS identification research has progressed fast in recent years, yielding numerous useful research outcomes. This study will examine the methodology based on deep learning (DL), as well as the technique's merits and weaknesses, as well as the FAS development trend.

With DL's continued advancement and remarkable performances in the field of FR, an increasing number of investigators have used FAS to investigate more comprehensive techniques for combating face deception. DL, as opposed to the old manual feature extraction (FE) technique, may autonomously learn photos, retrieve more critical and plentiful facial features, and assist in effectively distinguishing real from fake faces.

They first suggest a (CNN) [4] to extract features in FAS, which paved the way for a new branch of DL in the field of FAS [5]. The recognition impact was significantly lower than that of conventional approaches because the technologies were not yet established. Furthermore, the superiority of DL in feature extraction prompted a significant amount of research to pursue DL-based FAS. FAS based on DL has progressively advanced through network updates, TL [6], a combination of various characteristics, and domain generality, and has now exceeded the previous technique due to the unwavering dedication and repetitive tries of several researchers [7].

2 Related Work

Despite significant developments in facial recognition systems, face spoofing remains a significant risk. Most academic and corporate FR systems can be fooled by the following: an image, a video, a 3D face model of a genuine user; a reverse-engineered face image from the template of a genuine user; a sketch of a genuine user, etc. We present a quick summary of published facial impersonation recognition techniques. CNN has proven superior to alternative learning frameworks in a variety of computer vision tasks. For facial pictures, a distinctive feature representation approach known as HGC-CNN is employed to identify face spoof attacks with color photos. It's a multi-feature learning system that combines capsule NN and hypergraph regularisation concepts. Capsule NN can incorporate a variety of characteristics, including intensity values, LBP, and picture quality. Hypergraph regularisation can also be employed to learn relationships between samples. The expressive ability of extracted features is improved even more when locality information is included. SVM was utilized in the studies since the new representation is consistent with existing classifiers. The suggested approach outperformed the prior approach on FSA detection with color photos, according to experimental data on the NUAA database and the Multispectral spoofing database [4]. An another approach that combines two CNN streams presented by Yousef Atoum et al. They utilize both the whole-facial image and regions taken from a similar face to differentiate the spoof from live faces, as with most previous methods in face anti-spoofing that only use the entire face to identify presenting attacks. The first CNN streaming is based on the characteristics of patches collected from different face areas. This stream proves to be resistant to all types of presentation attacks, particularly on lower-resolution face photos. The second CNN stream uses the whole facial image to estimate face depth. The outcomes of this CNN's trials suggest that our depth estimation, especially on higher-resolution images, can produce impressive outcomes [8]. Gene LBPnet, a novel technique for CNN based on LBP for face spoofing detection, is presented by Karuna Grover & Rajesh Mehra. On the NUAA dataset, this methodology outperformed previous state-of-the-art algorithms. Using various assessment parameters, it has been demonstrated that the suggested approach provides excellent accuracy (98%) and a low Equal Error Rate, leading to improved recognition of spoofing attacks and thereby improving system security spoofing attempts [9]. To mutually assess the complexity of face pictures and the rPPG signal of face footage, the suggested system integrates CNN and RNN structures. To discriminate between real and fake faces, the approximated depth and rPPG are combined. They also provide a new FAS database for faces that includes a wide range of lighting, subject, and pose variants. The SiW dataset, which covers more subjects and modifications than previous datasets, is introduced. Lastly, they illustrate the technique's advantage in the experiment [10]. For face liveness identification, Zahid Akhtar et al. propose seven unique strategies for obtaining exclusionary patches in a facial image. A particular classifier is given the properties of specified discriminative picture patches. For the ultimate categorization of authentic and spoof faces, the categorization outcomes of these regions are pooled using a majority-voting-based scheme. In comparison to prior efforts, experiment outcomes on two publically accessible datasets reveal comparable outcomes [11]. To improve the security level of a FAS system, they introduced a novel model for identifying liveness attack images in this article. The variation between the attributes of actual and false faces is taken into account in the approach. As a result, integrating types of image information improves attack effectiveness greatly when compared to using a single approach [12].

3 Proposed Methodology

- Step 1: Collect the CASIA v2 image dataset which is freely available.
- Step 2: Cleaning the data and removing the noisy data.
- Step 3: Identifying and removing noisy images and perform data shuffling.
- Step 4: Reshaping the data features, and samples and splitting them into training and testing.
- Step 5: Passing the data into the training model.
- Step 6: Train and test samples (3331, 833) for fake and real images and split into 70% for training and 30% for testing.
- Step 7: After completion of training measure performance parameters accuracy, recall and precision (Fig. 1).

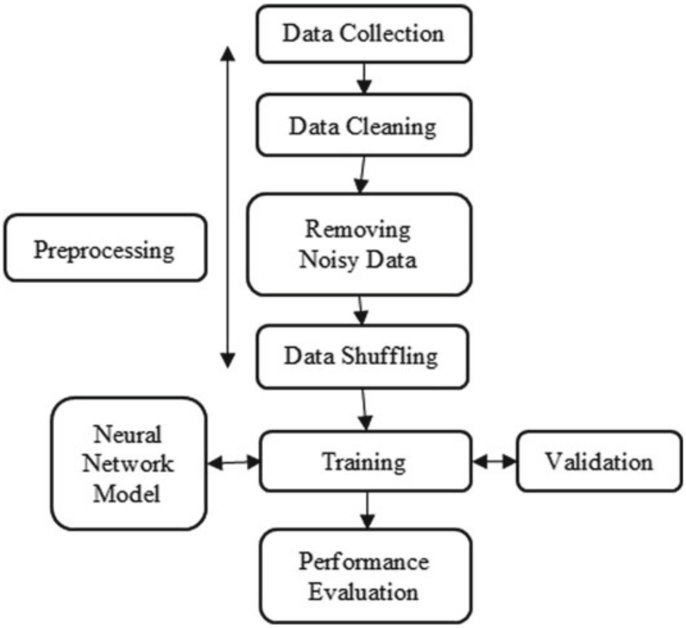


Fig. 1 Flow chart of proposed methodology

3.1 Dataset Gathering

The suggested method is evaluated using the CASIA v2 picture dataset, which is frequently used to identify image forgery and is freely available. There are 4795 photos in all, with 1701 legitimate and 3274 fake.

3.2 Data Pre-processing

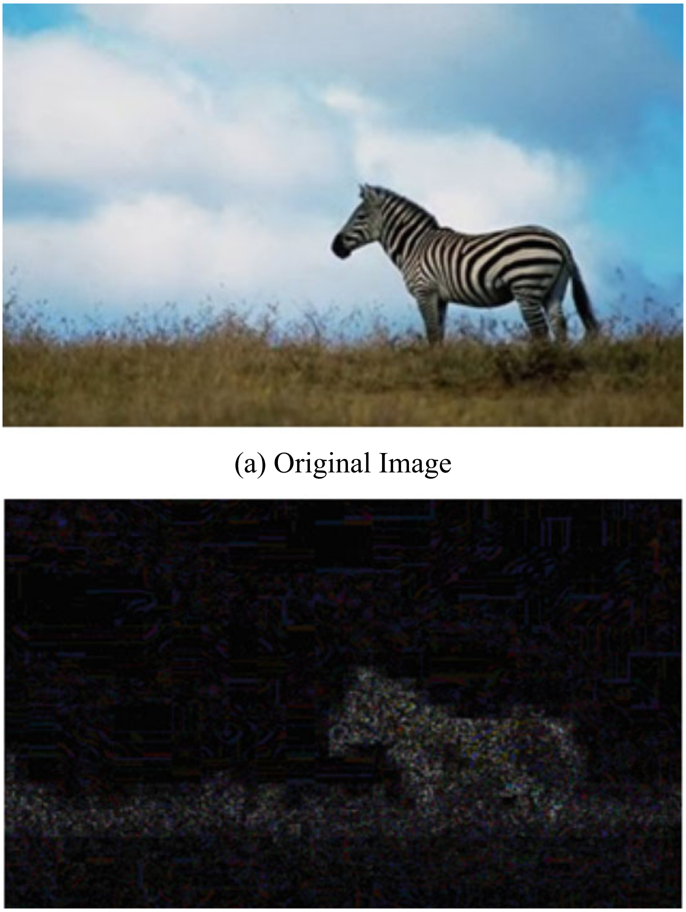
The goal of pre-processing is to optimize graphic data by overwhelming unwanted deformities or improving particular graphic properties that are important for subsequent processing and evaluation.

(a) Data cleaning is the act of determining and restoring (or eliminating) corrupted or erroneous information from a record set, table, or database. It includes recognizing insufficient, improper, faulty, or redundant data and then updating, changing, or deleting the dirty or imprecise data.
(b) Checking Noisy Images: Image noise is a sort of ambient sound that produces erratic changes in image intensity or color details. The image detector and circuits of a scanner or digital camera can make it. Movie coarse and the inevitable impulse noise of an optimal photoelectron can likewise cause image noise. We can check the original and noisy images in the dataset and convert all the images to error analysis for better performance.
(c) Data Shuffling: The shuffling strategies try to jumble up data while retaining logical linkages among columns if desired. It rearranges data from data inside a feature (for example, a column in pure flat format) or a collection of attributes randomly (e.g. a set of columns). Figure 2 shows the original and ELA image.

3.3 Model Parameter

Figure 3 shows the model parameter and explain is below:

(1) *Conv2D:* Conv2D is a 2-D convolution layer that produces a sequence of results by twisting a convolution kernel with the layers' data [13].
(2) *Max-Pooling:* Pooling that chooses the largest component from the section of the feature map encompassed by the filters is known as max pooling. As a consequence, the result of the max-pooling layer would be an FM with the most important characteristics of the previous FM [14].
(3) *Dropout Layer:* Dropout is a strategy for avoiding overfitting in a model. At every iteration of the training stage, Dropout consists of setting the outbound edges of hidden nodes (Hidden components are made up of neurons) to 0 [15].
(4) *Flatten Layer:* The process of converting data into a 1D array for usage in the following layer is known as flattening. The CL result is flattened to produce a



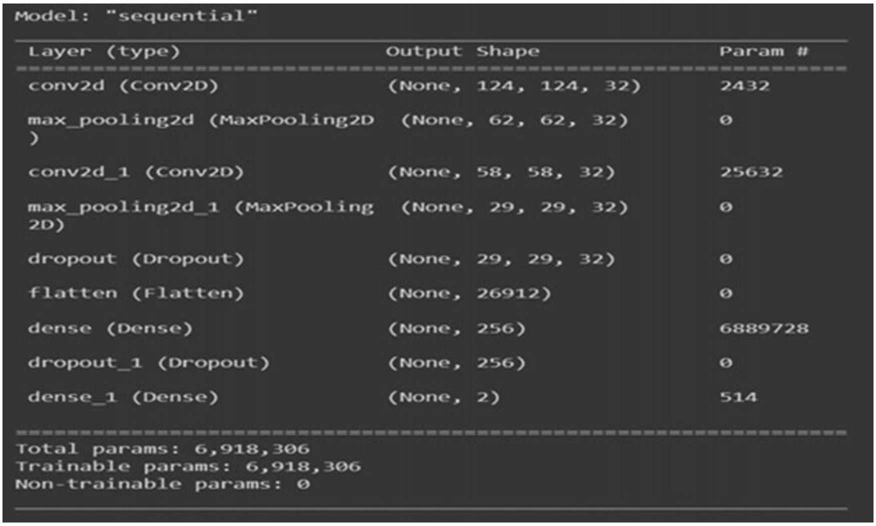
(a) Original Image

(b) ELA Image

Fig. 2 Figure showing the original and ELA image

single long feature representation. It's also related to a fully-connected layer, which is the definitive classification technique [16].

(5) *Dense Layer:* A DL in any NN is tightly linked to the layer before it, indicating that each of the layer's neurons is linked to each of the layer's neurons. It is the most commonly used layer in ANN. The outcome of the DL is an 'm' dimensional array. As a consequence, the layer is typically used to change the dimensionality of the vector. The vector is also subjected to processes such as rotation, scale, and translation by these layers [17].



```
Model: "sequential"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 conv2d (Conv2D)             (None, 124, 124, 32)      2432

 max_pooling2d (MaxPooling2D  (None, 62, 62, 32)       0
 )

 conv2d_1 (Conv2D)           (None, 58, 58, 32)        25632

 max_pooling2d_1 (MaxPooling  (None, 29, 29, 32)       0
 2D)

 dropout (Dropout)           (None, 29, 29, 32)        0

 flatten (Flatten)           (None, 26912)             0

 dense (Dense)               (None, 256)               6889728

 dropout_1 (Dropout)         (None, 256)               0

 dense_1 (Dense)             (None, 2)                 514

=================================================================
Total params: 6,918,306
Trainable params: 6,918,306
Non-trainable params: 0
_________________________________________________________________
```

Fig. 3 Model parameter

The neural network model is sequentially trained. The employed NN model with layers is shown in Fig. 3. The dataset is separated into the training of 70% and testing of 30% images for fake (3331) and Real (833) images. The NN is trained and used the RELU and Sigmoid as the activation function. The first layer of the network is the conv2D layer with 2432 parameters, after that the max-pooling2D layer is employed proceeding again to conv2D and max-pooling layer. The dropout, flatten and dense layers were then employed in a cascade manner. Table 1 shows the hyper parameters of training where the ADAM optimizer is used with 20 epochs for a batch size of 32.

Table 1 Hyper parameters of training

Optimizer	ADAM
Loss function	Binary cross-entropy
Metrics	Accuracy
Epochs	20
Batch size	32
Validation split	0.2
Shuffle	True

4 Simulation Result

4.1 Performance Matrix

Precision and accuracy: The degree to which a measured value is near its true value is known as accuracy. Precision refers to how closely all of the measured values are related. To put it another way, accurateness is the proportion of right categories to total classifications.

Recall/Sensitivity: Sensitivity is defined as the proportion of true positives to the whole number of actual positives. Similarly, specificity, also known as the true negative rate, is the proportion of genuine negatives to total negatives [18].

F1-Score: When a model's accuracy is greater than 90%, it is considered to be accurate, we also include the F1 score as a statistic that provides a better indication of cases that have been wrongly classified. The harmonic mean of precision and recall is employed to compute this. When TP and TN are more significant, accuracy is utilized. When the class distribution is unequal and FP and FN are more important, the F1 score is a better statistic [19]. All of the metrics formulas are as shown below.

$$accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

$$precision = \frac{TP}{TP + FP} \tag{2}$$

$$recall = \frac{TP}{TP + FN} \tag{3}$$

$$F\text{-}score = \frac{2}{1/precision + 1/recall} \tag{4}$$

$$specificity = \frac{TN}{TN + FP} \tag{5}$$

$$sensitivity = \frac{TP}{TP + FN} = recall \tag{6}$$

4.2 Confusion Matrix

In a classification issue, a Confusion Matrix is a tabular representation of prediction outcomes with count values split down by class. It demonstrates how a classification model performs while making predictions, as the name implies. It reveals the types of errors made by the classifier as well as the errors themselves [20]. Better and worse classification results are represented by the points above and below the line, accordingly. The matrix is shown in Fig. 4.

Figure 5 shows the accuracy and loss graphs for the evaluated results. Table 2 shows the comparison of the base and proposed results with the proposed system accuracy of 0.91.

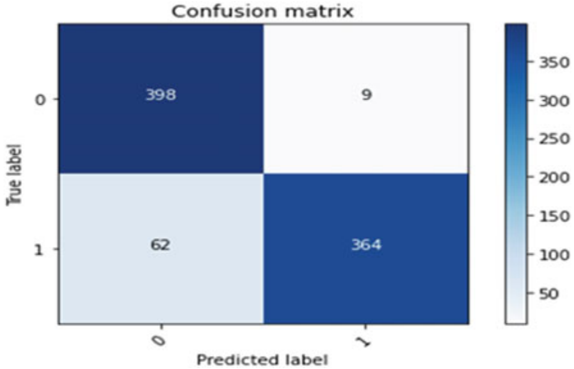


Fig. 4 Confusion matrix showing the true and the predicted label

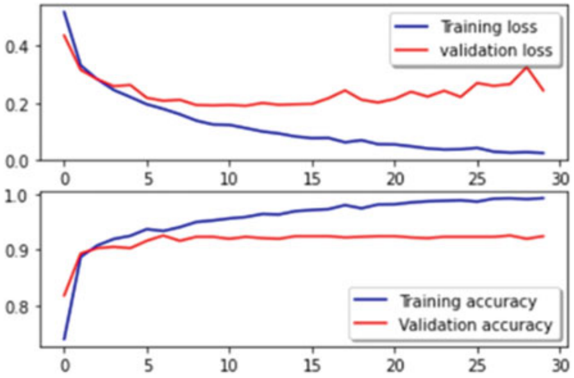
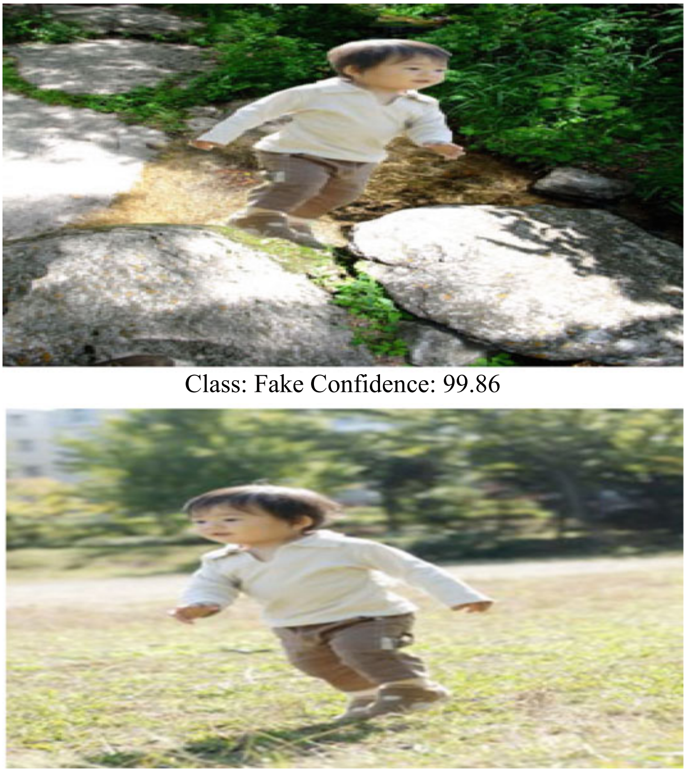


Fig. 5 Figure showing the loss and accuracy graph

Table 2 Comparison of the base and the proposed results

Results	Base Paper	Proposed
Recall	0.81	0.85
Precision	0.86	0.97
F1 Score	0.81	0.91
Accuracy	0.85	0.91



Class: Fake Confidence: 99.86

Class: Real Confidence: 99.56

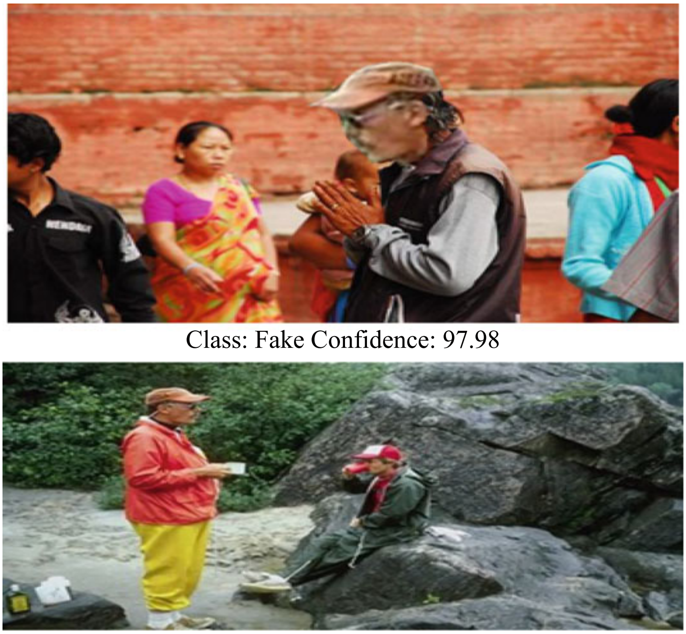
Fig. 6 An example of a resultant image compared with the original image

The precision, recall, and f1-score of the proposed model are 0.97, 0.85, and 0.91. The fake and real confidence of the resultant images is shown below.

Figures 6, 7 and 8 shows fake and real confidence images for spoofing techniques with duplicate photographs of people whose original images areas maintained in a database. It means that if an intruder wanted access to the authorized system, he or she may have used these several techniques.

5 Conclusion

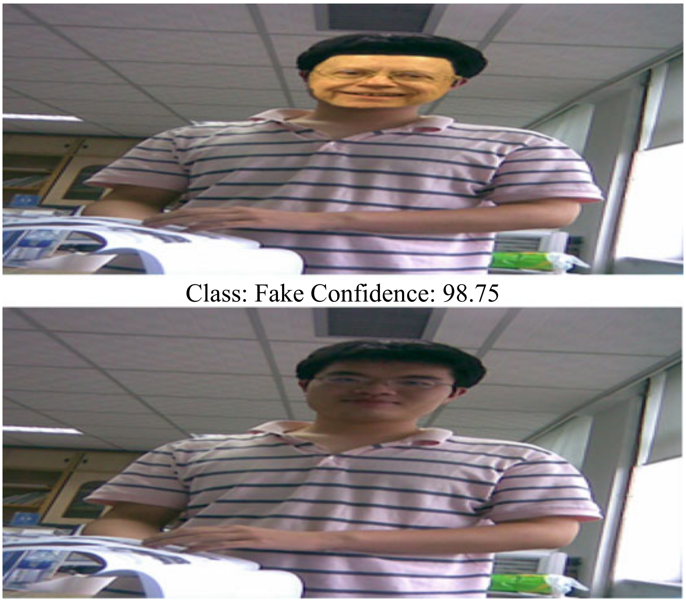
Face Recognition has become an essential technique for achieving protection as AI has become more widely used in real life. FAS has become a pressing issue in the fight against harmful attacks. The research of face spoofing identification has been continuously monitored and revised, from the starting of manual FE methods based on image texture, image quality, and depth information, to using DL to instantly extract



Class: Fake Confidence: 97.98

Class: Real Confidence: 99.95

Fig. 7 An example of a resultant image compared with the original image



Class: Fake Confidence: 98.75

Class: Fake Confidence: 98.11

Fig. 8 An example of a resultant image compared with the original image

features, merged with network up-gradation, feature assimilation, and domain generalization, and the efficiency and effectiveness of identification have now attained a significant state.

References

1. Hashemifard S, Akbari M (2021) A compact deep learning model for face spoofing detection. [Online]. Available: http://arxiv.org/abs/2101.04756
2. Al-Huda Taha N, Hassan TM, Younis MA (2021) Face spoofing detection using deep CNN. Turkish J Comput Math Educ 12(13):4363–4373
3. Ming Z, Visani M, Luqman MM, Burie JC (2020) A survey on anti-spoofing methods for facial recognition with RGB cameras of generic consumer devices. J Imaging (6)12. https://doi.org/10.3390/jimaging6120139
4. Liang Y, Hong C, Zhuang W (2021) Face spoof attack detection with hypergraph capsule convolutional neural networks. Int J Comput Intell Syst 14(1):1396–1402. https://doi.org/10.2991/IJCIS.D.210419.003
5. De Souza GB, Papa JP, Marana AN (2021) Efficient deep learning architectures for face presentation attack detection. 112–118. https://doi.org/10.5753/sibgrapi.est.2020.12992
6. Khalid IA (2020) Transfer learning for ımage classification using tensorflow. Towards Data Sci
7. Zhang M, Zeng K, Wang J (2020) A survey on face anti-spoofing algorithms. J Inf Hiding Priv Prot 2(1):21–34. https://doi.org/10.32604/jihpp.2020.010467
8. Liu Y, Jourabloo A, Liu X (2018) Learning deep models for face anti-spoofing: binary or auxiliary supervision. In: Proceedings of the IEEE computer society conference computter vision pattern recognition, pp 389–398. https://doi.org/10.1109/CVPR.2018.00048
9. Das PK, Hu B, Liu C, Cui K, Ranjan P, Xiong G (2019) A new approach for face anti-spoofing using handcrafted and deep network features. In: Proceeding—IEEE ınternational conferences servey operations and logistics and ınformatics 2019, SOLI 2019, no November, pp 33–38. https://doi.org/10.1109/SOLI48380.2019.8955089
10. Akhtar Z, Foresti GL (2016) Face spoof attack recognition using discriminative ımage patches. J Electr Comput Eng. https://doi.org/10.1155/2016/4721849
11. Atoum Y, Liu Y, Jourabloo A, Liu X (2018) Face anti-spoofing using patch and depth-based CNNs. In: IEEE ınternational joint conference on biometrics (IJCB) 2017, vol 2018-Janua, pp 319–328. https://doi.org/10.1109/BTAS.2017.8272713
12. Grover K, Mehra DR (2019) Face spoofing detection using enhanced local binary pattern. Int J Eng Adv Technol 9(2):3365–3371. https://doi.org/10.35940/ijeat.b3834.129219
13. Pouyanfar S et al (2019) A survey on deep learning. ACM Comput Surv 51(5):1–36. https://doi.org/10.1145/3234150
14. Masita KL, Hasan AN, Shongwe T (2020) Deep learning in object detection: a review. In: 2020 International conference artificial ıntelligence big data, computing data communication system (icABCD 2020)—proceeding no. August, 2020. https://doi.org/10.1109/icABCD49160.2020.9183866
15. Manalu BU, Tulus, Efendi S (2020) Deep learning performance in sentiment analysis. In: 2020 4th International conference on electrical telecommunication and computer engineering (ELTICOM 2020)—proceeding, pp 97–102. https://doi.org/10.1109/ELTICOM50775.2020.9230488
16. Shirahatti AP, A survey of deep learning for sentiment analysis. V(I):1–7
17. Weng W, Zhu X (2021) INet: convolutional networks for biomedical image segmentation. IEEE Access 9:16591–16603. https://doi.org/10.1109/ACCESS.2021.3053408
18. ML (2020) Classification: precision and recall. Machine learning crash course. https://developers.google.com/machine-learning/crash-course/classification/precision-and-recall

19. R (2020) ROC Curves. Machine learning crash course. https://developers.google.com/machine-learning/crash-course/classification/roc-and-auc
20. Narkhede S (2018) Understanding confusion matrix. Towardsdatascience. https://towardsdatascience.com/understanding-confusion-matrix-a9ad42dcfd62