International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-08, Issue-03, June 2022

Face Spoofing Detection System Using Principal Analysis with Improved CNN Model

Shafiqullah Khaliqyaar, Shaifali Sharma & Shreya Kalta

Research Scholor, Alakh Prakash Goyal Shimla University, India. shafiqullahkhaliqyaar@gmail.com

Abstract: Facial spoofing assaults have attracted considerable attention due to criminals utilizing various tactics such as distorted photographs, cropped images, 3D masks, and so on to fool face recognition systems easily. Deep learning models provide solid solutions for improving the security measures of biometric systems, yet, achieving the advantages of multilayer features remains a considerable difficulty. This study proposes a hybrid approach for building feature representations by combining ResNet with higher discriminative strength to address this constraint. Two forms of the residual learning framework are used as deep feature extractors to extract useful features. Second, the ultimately linked layers are employed as distinct feature descriptors. Following the facial borders and elements extracted from the actual image, the next stage is to detect the individual. Face spoofing detection is used to evaluate persons by automatically analyzing their attributes using computer-based technologies. The principal analysis with an improved CNN model has been employed for the face spoofing detection technique. The results have been generated by matching the facial feature sets within the CASIA-FASD dataset. The suggested method was implemented in the MATLAB simulator, and a complete performance study was carried out. Finally, the resulting data were analyzed and compared to current methodologies. With the fast advancement of facial recognition technology, most present algorithms can perform admirably in unconstrained circumstances. However, detecting face spoofing assaults remains a difficult challenge; hence face anti-spoofing has emerged as one of the most significant study areas in the community. Though several anti-spoofing models have been presented, their generalization power often worsens in complex appearance changes, such as backdrop, lighting, different spoofing materials, and low picture quality, for hidden attacks.

Keywords: Deep learning, improved CNN Model, Facial spoofing, CASIA-FASD, MATLAB.

I. INTRODUCTION

Most current facial recognition systems are now vulnerable to spoofing attempts—Spoofing happens when someone attempts to circumvent a biometric face system by presenting a bogus face in front of the camera. For example, in one study, researchers compared the danger of onlineisocial network-basedifacial disclosureiagainst the most recent version of six commercial face authentication systems. While just 39 per cent of photographs shared on social networks may be effectively spoofed, the comparatively modest number of acceptable images was enough to mislead 77 per cent of users' facial authentication software.**Yu, Z., et al.,(2021) [1]** A female invader using a unique make-up also succeeded in deceiving a facial recognition system in a live demonstration at the International Conference on Biometrics (ICB 2013). These two instances, among many more, demonstrate how vulnerable facial recognition systems are to spoofing attacks.

Face recognition has been impressively integrated into most biometric systems as advanced deep learning technology. As a result, facial biometric systems are extensively employed in various applications, including mobile phone authentication, access control, and face recognition. Payment, Face-spoofing assaults, in which fabricated faces used to be authenticated by the biometric system, are becoming an unavoidable danger. Face-spoofing detection has therefore become a fundamental necessity for any face recognition system. Technique for detecting phoney faces.While face anti-spoofing techniques have garnered aloof research to determine whether most face-spoofing detection, whether the photographed face is genuine or phoney approaches are skewed toward a particular style of presenting attack or presenting device; failure to identify different types of spoofing situations. **Parkin, A., et al., (2019) [2]**

Face anti-spoofing strategies have gotten a lot of attention, with numerous anti-spoofing methodologies being proposed in retrospective research. Traditional image-based techniques focus on picture quality and characteristics. Therefore, they use hand-crafted features like LBP, SIFT, HOG, and and SURF with shallow classifiers to distinguish between natural and artificial

DOI : 10.35291/2454-9150.2022.0307

faces. Their universality is limited because these hand-crafted characteristics are constrained to specific spoofing patterns, scene circumstances, and spoofing devices. **Sun, W., et al.,(2020) [4]** Deep approaches based on Convolutional Neural Networks have recently emerged as an alternate strategy for increasing the effectiveness of antispoofing strategies by learning a discriminatory representation from start to finish. While data-driven feature learning improves spoofing detection performance, these methods fail to capitalize on the nature of spoofing patterns, including skin details, color distortion, more designs, glassy reflection, shape deformation, and build models for the current dataset and fail to generalize in cross-dataset settings. They are susceptible to lighting and illumination distortion because they are constructed on controlled and biassed datasets. As a result, overfitting and poor generalizability to novel patterns and contexts plague these models. While several machine learning models have been created to detect artifacts in spoof photos, their performance in actual applications is still far from ideal due to the following issues**.** **Fatemifar, S., et al., (2022) [5]** First, spoofing attack datasets are limited and biassed to certain ambient and capture circumstances compared to other computer visionitasks such as picture classification. Large-scale labeled datasets such as ImageNet exist. They gathered for a specific assault scenario, such as a reply-attack, or they collected with regulated lighting and illuminance settings with a restricted number of subjects, i.e., faces. Second, there are many attack types, and new attack scenarios, such as adversarial instances, are discovered regularly. Most offered models are optimized for a single scenario or dataset, and their effectiveness on previously encountered attack types (data) is inaccurate. **Liu, A., et al., (2019) [3]**

Third, current deep models are designed for semantic-rich computer vision tasks such as object identification and picture captioning, rather than anti-spoofing, based on low-level characteristics. As a result of their attempt to learn high-level semantic properties, these models fail to catch excellent spoofing patterns. As a result, establishing a task-specific model with a low-level discriminator is greatly sought. It offers a dual-channel neural network that learns optimum features directly to distinguish between fake and genuine faces to address these issues. The proposed model employs deep and broad channels to learn a low-dimensional latent space for the face spoofing problem.

On the other hand, the deep channel learns data-driven characteristics that distinguish between real and faked faces by employing a CNN architecture particularly built for spoofing detection. The latter, i.e., broad channel, uses hand-crafted features already popular for spoofing detection tasks (in frequency, texture, and temporal) and smoothly integrates them into the deep channel's low-dimensional latent space. The proposed system was thoroughly tested on multiple spoofing detection datasets to assess its efficiency.

This paper's primary contributions are as follows:

- Create a well-generalized model that is resistant to environmental changes and datasets.
- Propose deep architecture based on low-level spoofing characteristic patterns.
- Compare the efficiency of each approach on some of the datasets that are accessible.
- To deal with newly created or unknown assaults, use the strengths of both CNN and hand-crafted features.

1.1 Authentication System

During registration, a biometric system records a sample of a user's biometric trait using an appropriate sensor—for example, a camera for the face. It then collects significant properties from the biometric sample, such as fingerprint minutiae, using a software technique known as a feature extractor. **Fatemifar, S., et al., (2022) [5]**The extracted characteristics are saved in a database as a template alongside other identifiers such as a name or an identifying number. The user must give another biometric sample to the sensor to be authorized. The query is made out of features derived from this sample. The system then compares the stated identification template to a biometric matcher. The matcher produces a match score representing how similar the template and query are. The system accepts the identity claim only if the match score exceeds a predetermined threshold. Protecting the biometric templates contained in the system database is a vital step in reducing the security and privacy issues associated with biometric systems. At the same time, concerns can be minimized by keeping templates decentralised. There are advantages and downsides to both biometric feature transformation and biometric cryptosystems. **Nagpal, C., et al., (2019) [9]** Matching is typically simple in a feature transformation scheme, and it may even be possible to build transformation functions that do not affect the features of the original feature space. However, it can be challenging to identify an adequate transformation function that is non invertible while still tolerant to intrinsic intra-user biometric variability. While safe sketch generation approaches for biometric cryptosystems based on good information-theoretic principles are known, the problem is to express the biometric characteristics in conventional data forms such as binary strings and point sets. As a result, one major research subject is developing algorithms that translate the original biometric template into standardized data

DOI : 10.35291/2454-9150.2022.0307

formats such as fixed-length binary strings or point sets while preserving discriminative information.

1.2 Face Spoofing

Face spoofing/liveliness is using another person's identity for illegal purposes. According to a recent assessment, face spoof assaults have become extremely damaging to society, particularly in bank frauds, social media, etc. Many ways have been employed to counter these attacks, but the downsides of these solutions are difficult to eliminate. Printing assaults, video attacks, and 3-dimensional mask attacks are examples of face spoof attacks. In printing assaults, the attacker utilizes a printed image of the target to impersonate him in front of the camera. The attacker utilizes a brief video clip of the victim in the video attack, which is more difficult than the printed assault. Most present facial recognition systems are known to be sensitive to spoofing attempts. **Chen, H., et al.,(2019)[11]** Spoofing happens when someone attempts to circumvent a biometric face system by presenting a bogus face in front of the camera. For example, researchers examined the danger of online social network-based facial disclosure against the most recent version of six commercial face authentication systems (Face Unlock, Facelock Pro, Luxand Blink and Fast Access). While just 39 per cent of photographs shared on social networks may be effectively spoofed, the comparatively modest number of acceptable images was enough to mislead 77 per cent of the 74 users' facial authentication software. Spoofing is just a false acceptance attack in which attackers present forged evidence to the biometric system to achieve authentication. It is relatively simple to launch such an assault on the facial recognition system since images and videos of the individual may be quickly accessed on social networking sites or shot from a distance.

1.3 Different Attacks of Face Spoofing System

Face spoofing may be accomplished in two ways: 2D and 3D spoofing. Both spoofings are further subdivided into assaults such as picture attacks, video attacks, and 3D mask attacks. Thanks to social internet networks, photos and videos are freely accessible, and films may be taken from mobile phones or other digital devices. There are two sorts of assaults on the facial recognition system. *(i) Presentation Attacks:* Presentation assaults are carried out at the sensor level, without the requirement for access to the system's guts. Presentation assaults are linked to solely biometric flaws. In these assaults, intruders employ an artefact, often fake (e.g., a face photo, a mask, a synthetic fingerprint, or a printed iris image), or attempt to replicate the characteristics of real users (e.g., gait, signature) to gain unauthorized access to the biometric system. Because "biometric qualities are not secrets," attackers know that many biometric data revealing people's faces, eyes, voices, and behaviour is publicly available. They utilize that information to evade face recognition systems using the examples below.

- Attackers mimic the user by using an image of the user.
- They imitate the user by using a video of the user.
- Alternatively, hackers can create and use a 3D representation of the assaulted face, such as hyper-realistic mask.

(ii) Indirect Attacks: Indirect attacks can be launched against the database, matches, communication lines, etc. The attacker needs access to the system's interior in this form of attack. Indirect attacks may be stopped using measures connected to "traditional" cybersecurity rather than biometrics. Thus, we won't cover them in this piece.

Most cutting-edge facial biometric systems are vulnerable to simple assaults if presentation attack detection mechanisms are not included. **Mohammed Khammari et al., (2019) [12]**

Face recognition systems are often spoofable by providing the camera with an image, video, or 3D mask of a targeted individual. Alternatively, you might utilize cosmetics or plastic surgery. However, because of the great exposition of the face and the inexpensive cost of high-resolution digital cameras, employing images and videos is the most prevalent kind of assault. (i) *Photo attacks*: The picture attack is a type of 2D spoof in which an attacker shows a photo to a biometric modality to gain access to the system, such as the screen of a mobile phone, tablet, or laptop. Photographic masks are a substantially more advanced sort of photo attack in which high definition printed pictures with cut-out eyes and mouths are used. The imposter is situated behind the attacker throughout the attack so that certain facial motions, such as eye blinking, are replicated.

(ii) Video attacks: This is a more complex variation of a photo assault. In this assault, the attacker records a video of the actual person using a mobile, tablet, and digital camera, and then, during facial recognition, the attacker plays that video and gains access to the biometric modality owing to the correct movement of the face portion. As a result, these assaults are more difficult to identify and detect. *(iii) 3D Mask Attacks:* The attacker builds a 3D reconstruction of the face and presents it to the sensor/camera in this type of attack. Because of the 3D, this assault is a more complex variation of video and photo attacks. In a 3D mask assault, the attackers create a 3D mask of the actual person, making it more difficult to locate a genuine person. Because the 3D structure of the face provides a superior option for identifying the genuine individual, these assaults are less common than the other kinds. 3D masks are often composed of several characteristics and score-based approaches.

DOI : 10.35291/2454-9150.2022.0307

1.4 Existing Model

The RGB colour space has three colour components: red, green, and blue; YCbCr colour space has brightness and saturation information; and HSV colour space has three colour components: hue, saturation, and brightness. Each colour space has unique information and properties. The RGB colour space has rich spatial information that most closely mimics human-seen colours, but the YCbCr and HSV colour spaces contain more sensitive information to brightness. The RGB colour space can be converted into HSV and YCbCr using the following formula.

Existing approaches transform RGB face photos to the YCbCr and HSV colour spaces, and spoofing images are categorized by applying an LBP to each colour space. However, because it uses a 6-channel colour space, this approach requires more processing. This study employs a three-channel colour space consisting of Cb, S, and V to deduce several face traits. The suggested solution strives for high-speed processing and resilience against illumination variations in face anti-spoofing.

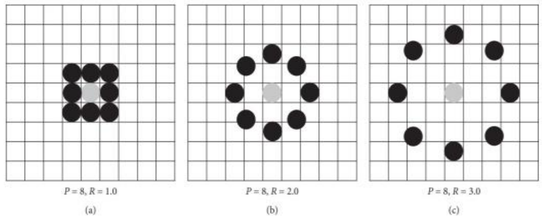


Figure 1. Example of a local binary pattern

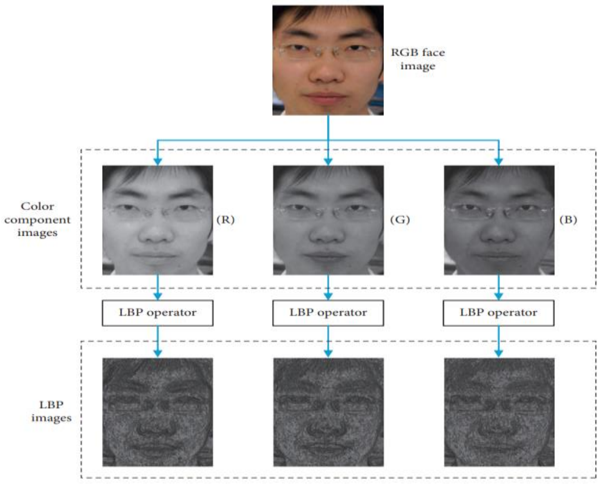


Figure 2. Visualization of LBP operation performed on each colour band image.

The following are some of the benefits of this approach: (i) The suggested technique decreases false detection by employing a three-channel colour space that expresses enough face feature information. (ii) The suggested technique requires less memory and has fewer feature dimensions, allowing for faster processing.

The proposed model suggested an analysis based on the concept that deformable part models are convolutional neural networks. It discusses the following points in this paper. (i) Other dimension reductions and deep learning (DL) classification algorithms are being examined in an anti-face spoofing detection system. (ii) To create the filtering and principal component analysis (PCA) approach for extracting and optimizing the trustworthy feature sets in matrices. (iii) To categorize or detect face spoofing photographs using an Ant-lion with CNN classification algorithm. (iv) To assess and compare performance measures such as HTER, EER, FAR, FRR, etc. To identify and extract facial characteristics, the anti-face-spoofing detection approach is used. The edges must be recognized in the submitted image to obtain the picture's refined edges. Following the facial borders and features extracted from the real image, the next stage is to detect the individual. Face spoofing detection is used to evaluate persons by automatically analyzing their attributes using computer-based technologies. For the face spoofing detection technique, the CNN model will be employed. The results will be generated by matching the facial feature sets with the CASIA-FASD dataset. The suggested method was implemented in the MATLAB simulator, and a full performance study was carried out. Finally, the resulting data were analyzed and compared to current methodologies.

II. Related Works

Youngjun Moon et al., (2021) [10] proposed an antispoofing face method that used CNN learning and inference and assembled important criteria by retrieving texture information from the face image colour space using an LBP The CASIA-FASD dataset was used for performance verification. Images from videos were extracted and classified as published image attacks, cut picture attacks, and video replay threats. These images from the CASIA-FASD data - set were used for training and evaluation. It was established that the proposed approach could be used effectively in edge environments. We intend to verify the efficiency against another well-known face spoof set of data in the future. We also intend to run performance tests between datasets. **Chen, H., et al., (2019) [11]** suggested an inattention-based two-stream convolutional network for detecting face spoofing to discriminate between authentic and false faces. The suggested method uses complementary features (RGB and MSR) derived from CNN models (MobileNet and ResNet-18), which are subsequently fused using the attention-based fusion method. Under different lighting situations, the adaptively weighted features carry more discriminative information. The author tested face spoofing algorithms on three tough databases, namely CASIA-FASD, REPLAY-ATTACK, and OULU-NPU, which demonstrated competitive performance in both ntra and inter-database.

DOI : 10.35291/2454-9150.2022.0307

The fusion technique studies have shown that the attention model can obtain promising outcomes on feature fusion. The cross-database assessments demonstrate the efficacy of combining RGB and MSR information. **Mohammed Khammari et al., (2019) [12]** proposed a countermeasure against face-spoofing assaults. The proposed approach employs a deep CNN architecture with a mix of LBP and SWLD descriptors, SVM with non-linear kernel. To train classifiers On the REPLAY-ATTACK dataset, complete classification between real access and imposter assaults was accomplished, as was a highly competitive performance on the CASIA dataset. Other filtering approaches and network topologies will be investigated to adapt the model to new data (for example, identifying spoofing attacks using facial masks and 3D models), and more research will be conducted to reduce the number of characteristics. **K Balamurali et al., (2021) [13]** developed the model in which identified face was denoised and then transformed to the YCbCr and CIELUV colour models before being fed through the VGG-Face architecture to extract face embeddings for each colour space.

The retrieved face embeddings were then concatenated and sent to SVC, which distinguishes real and fake faces. The proposed approach for spoof detection obtained a test accuracy of 99.6 per cent and specificity of 99.5 percent. **Akinori F. Ebihara et al., (2021) [14]** suggested a technique based on the SpecDiff descriptor obtained the best PAD accuracy among previous flash-based algorithms execution and speed about six times quicker than that of a DNN by leveraging speculation diffusion reflection from a subject's face. Only one visible-light camera and a flashlight are required for the algorithm. A simple collection of 1K picture pairings per class with binary labels was sufficient to train the classifier using the SpecDiff descriptor, allowing the PAD technique to be easily and widely used. Experiments on actual devices demonstrate that the method has a feasible degree of performance on mobile devices without the requirement for computationally costly processing equipment. **Seyedkooshan Hashemifard et al., (2021) [15]** presented a dual-channel technique that utilises both the CNN and colour texture descriptor domains. According to the results, the strategy outperforms similar prior methods, but it also appears to be a viable way to extract well-generalized and resilient features for use in cross-dataset studies while avoiding biases between datasets. One interesting future lead would be to apply transfer learning for the CNN channel with more advanced topologies. Other descriptors might also be added to the other channel to improve the depiction of the anti-spoofing problem.

III. PROBLEM DEFINITION

Shefali et al. 2021 [16] discussed that face is a part of biometrics, and face recognition is utilized in BS (biometric systems) to identify and secure an individual. Most, Face security or authentication systems are prone to SAs (Spoofing attacks) such as relay attacks, attacks using three-dimensional masks, etc. So, the face anti-spoofing method is becoming essential in these systems. Face verification in BS is a famous field for research. There are several limitations, such as; (i) Different viewpoints (ii) Occlusions, and (iii)Age variation of person, along with factors like lighting situations.

The existing model is based upon the prolonged deep learning model using CNN and PCA method to determine the face spoofing in the face recognition applications. The existing model is evaluated on CASIA-FASD and Relay attack IDIAP datasets and is observed with half the total error rate (HTER), FAR, FRR, etc. On the contrary, HTER and FAR are observed as minimum than the existing model, showing improvement. The accuracy of the existing relay model is 99.0 per cent which shows a significant difference in improvement. Similarly, the FAR (0.045) is significantly lower than the FRR (0.032), which shows the underperformance of the existing model. The existing model uses the PCA feature extraction method and the CNN classifier, which can be further improved by using the improved optimization with the PCA feature extraction method. CNN model has defined superior performance in dealing with difficult CV (computer-vision) issues and issues related to face images.

Also, the performance of face spoofing detection models using CNN is lower for the CASIA-FASD dataset compared to the IDIAP dataset in another study. The CASIA-FASD face spoofing dataset contains higher-order variability than the CASIA-FASD dataset, which challenges the face spoofing detection schemes. Hence, the focus of this research can be kept on the CASIA-FASD dataset and IDIAP dataset. The main problems analyzed by the author [16]: (i) High error rate (ii) High time consumption (iii) High costly (iv) Overfitting issue

IV. RESEARCH METHODOLOGY

In this section, the main objective points are: (i) To analyze the several dimension reduction and deep learning (DL) classification methods in the anti-face spoofing detection system. (ii) To develop the filtration and principal component analysis (PCA) technique to extract the reliable feature sets in matrices and optimize the feature vectors. (iii) To implement an Ant-lion with CNN classification method to classify or detect the face spoofing images. (iv) To evaluate and compare the performance metrics with HTER, EER, FAR, FRR, etc. Figure 3 defines the proposed system starts the face image

DOI : 10.35291/2454-9150.2022.0307

acquisition procedure in which the image is uploaded in the GUI-MATLAB, which has to be utilized with the Ant –lion-CNN algorithm. The anti-face-spoofing detection technique is utilized to detect and extract face features. The edges have to be detected in the uploaded image to get the refine edges of the image. A further step is to detect the person after the face edges and feature extraction from the real image. Face spoofing detection is the procedure utilized to verify the people by analyzing their properties automatically using computer-based methods. The CNN model will be used for the face spoofing detection procedure. The face detection method will produce the outcomes by matching the face feature sets with the CASIA-FASD dataset. Afterwards, the proposed algorithm was implemented in the MATLAB simulator, and thorough performance analysis was performed. Finally, obtained results have been analyzed and compared with the existing techniques.

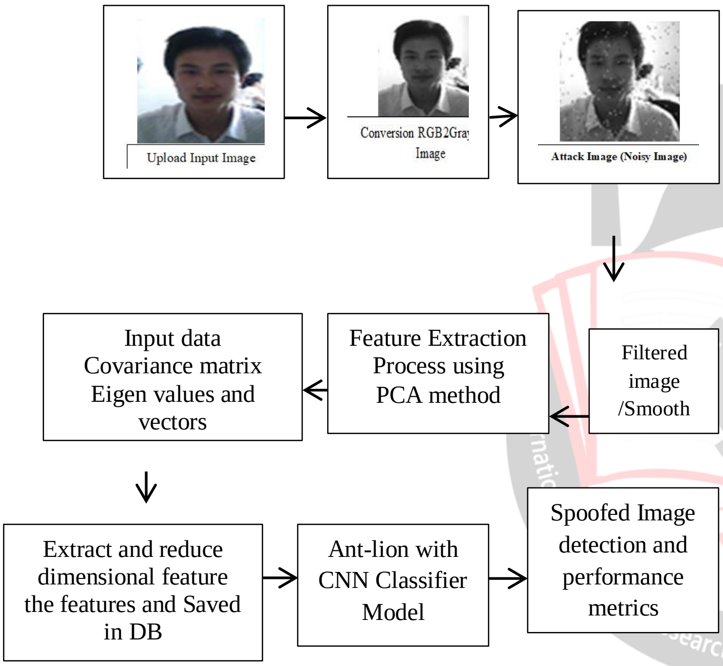

Upload Input Image
Conversion RGB2Gray Image
Attack Image (Noisy Image)
Filtered image /Smooth
Feature Extraction Process using PCA method
Input data Covariance matrix Eigen values and vectors
Extract and reduce dimensional feature the features and Saved in DB
Ant-lion with CNN Classifier Model
Spoofed Image detection and performance metrics

Figure 3. Proposed Work Flow Chart

The research techniques of detecting face spoof detection system are applicable to classify the input as fake and normal face image. This proposed work a system to detect the face spoof in different phases that is described as:

(i) ***Face image pre-processing step:*** The staging phase is to detect or classify the face spoof. An upload input image database created from a reliable data source is used for input in the detection system. CASIA-FASD dataset was designed to collect the face images. The attack or noise is eliminated from the images by dispensation the face input images to complete the efficient performance. This step aims to panel a digital face image into various edges. This method is used to identify the objects and the information from the face photos; this process contributes to optimizing the complexity when the image is studied.

(ii) ***Feature extraction Step:*** The results attained are measured as edge detection. So, these steps objectives to extract the attributes from this chosen field. It is a procedure in which a class of attributes so that the following processing becomes simple and several attributes like colour, text, etc. These features are used to recognize the face. At present, various techniques are defined to extract the attributes. These techniques are reliable for developing a detection system. Feature sets derived from the PCA method are normally used for data dimensionality reduction. Their dimensions might be optimized without a significant loss of data. The use of PCA takes the benefits of V (Eigenvectors) features to determine chosen object orientation.

(iii) ***Classification or Detection Step:*** The main purpose is to develop an effective and robust face spoof detection system with better reliable quality. It is vital to have an optimized classifier for optimized extracted feature sets. All the dataset with spoof and real face images is separated into different layers such as training and testing set built by combining all real and spoof samples. The Ant-Lion with CNN model is first trained using training face samples and then analyzed on testing samples. The evaluated feature is then fed to optimized CNN classifiers. Ant-Lion with CNN is the command that is utilized for CNN implementation. The AL-CNN model is trained to classify the different categories. It comprises various HLs (hidden layers) like CL (convolutional layer), AF (Activation function), PL (pooling layer), and FCLs (fully-connected layers) among the input and final output layer. The neurons in the HL learn the features of the face input images and finally predict the categories that are spoof or genuine. The OL (output layer) predicts the face input image and gives the percentage of resembling face input image to each category. The category with maximum accuracy is the final output outcome. BP (backpropagation) structure is utilized to tune the network for the precise outcome. The architecture is shown in figure 4.

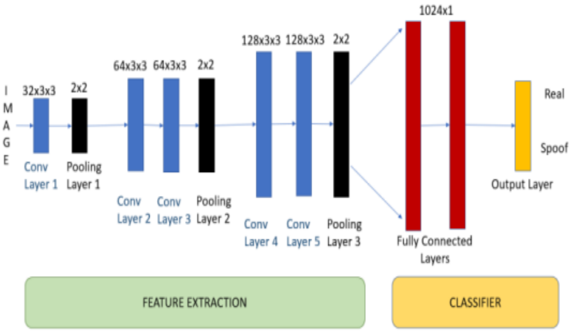


Figure 4. AL-CNN model

DOI : 10.35291/2454-9150.2022.0307

V. Experimental Analysis

The proposed model has used the **MATLAB** Simulation tool. MATLAB software is a PL (programming language) as other PLs developed. The full form of MATLAB is *"Matrix Laboratory."* It gives the mathematical computing and 4th generation PL. It executes the MATLAB code files. There is a CW (command window) in MATLAB.

CASIA-FASD dataset is a spoofing attack dataset that comprises three categories of attacks: (i) Printed with cut eyes, (ii) warped printed, and (iii) video attack photographs. The input samples are taken with different categories of cameras: (i) High, (ii) Normal, and (iii) Low quality.

Figure 5. CASIA-FASD Dataset [17]

Performance metrics: The proposed work considered the HTER (half total error rate) in the CASIA-FASD database to calculate the research model. HTER [18] is evaluated utilizing the FAR (false acceptance rate) and FRR (false rejection rate) in the spoof database, both of which are shown below. The HTER rate evaluation is defined as follows:

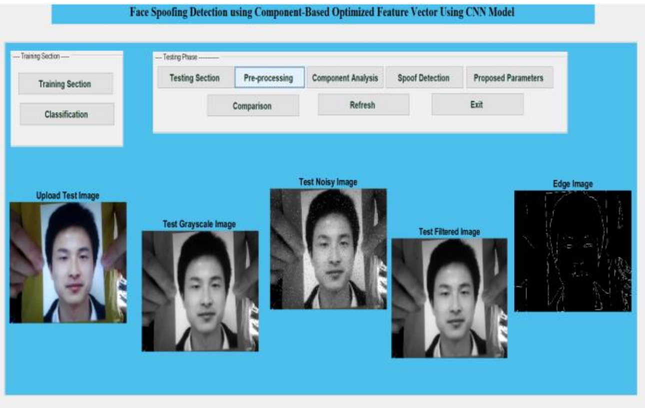
$$HTER = \frac{Far+Frr}{2} \qquad (i)$$

The FAR [19] is considered how likely the BSS (biometric security system) will inaccurately accept an access effort by an unofficial operator. A system's FAR normally is shown as the ratio of the number of FAs separated by the number of verification attempts.

FRR [20] is considered how likely the BSS will accurately reject an unofficial operator's access effort. Generally, a system's FRR is shown as the ratio of FRs separated by the number of verification attempts.

Lesser HTER values define good performance, where HTER is shown using only misclassification ratios. Moreover, the EER (equal error rate) defines the rate at which the false rejection and acceptance rate values converge to another, where a small value also defines good performance.

EER rate parameter is a BSS method utilized to program the threshold values for the FAR and FRR. When the rates are equal, the normal value is the EER. Lower the ERR, the better accuracy of the BS.



Face Spoofing Detection using Component-Based Optimized Feature Vector Using CNN Model

Figure 6. (i) Input Image (ii) Converted Image (iii) Noisy Image (iv) Filter Image, and (v) Edge Image

Figure 6 shows the face input images with various faces defined; the spoof detection process is repeated for every detected face for the defined input face image and classifies every face individually. Figure 6(i) shows the input face image uploaded. Figure 6(ii) shows the conversion of the face image, which is colour, into a black and white image. Figure 6(iii) shows the attack image. After that, figure 6(iv) shows the filtered image. It removes the attack information in the uploaded image. It calculates the smooth and noise-free image shown in figure 6(iv). Figure 6(v) shows the edge detection image.

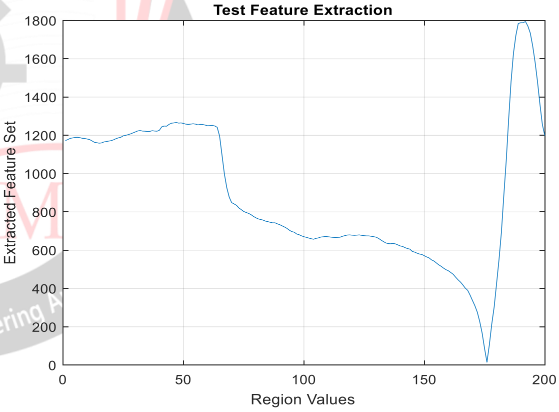


Figure 7 The graphical representation using feature extraction

Figure 7 defines the graphical representation using the PCA algorithm's feature extraction process. These techniques are reliable for developing a detection system. Feature sets derived from the PCA method are normally used for data dimensionality reduction. Their dimensions might be optimized without a substantial loss of data. The use of PCA takes the benefits of V (Eigenvectors) features to determine chosen object orientation.

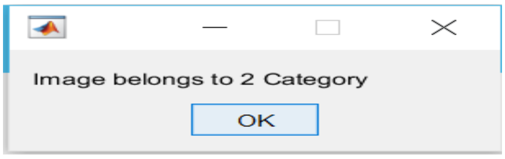


Image belongs to 2 Category

Figure 8. Detection Category: Fake or Spoof Image

DOI : 10.35291/2454-9150.2022.0307

As defined in figure 8, the attributes of the testing and testing face images are studied with the help of a text-based feature extraction method. The Optimized-CNN classifier is applied to detect or classify the best match defined in the form of the matched face image.

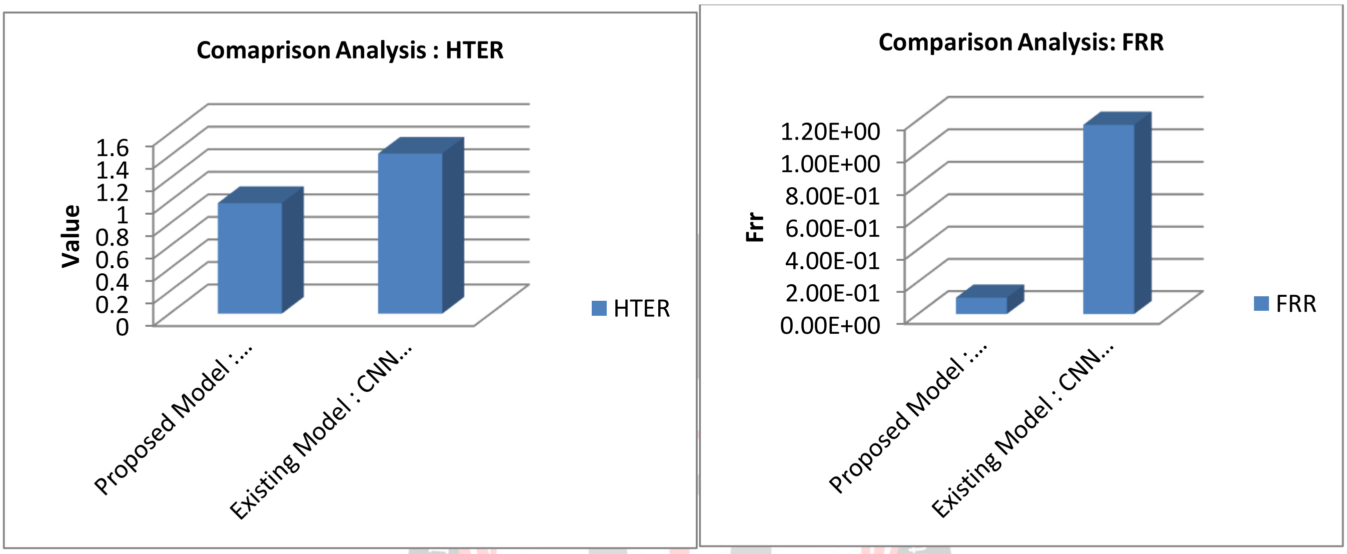
Table 1. Proposed Metrics: Component-based AL-CNN classifier Model

Parameters	**Values**
Accuracy	99.008
HTER	0.9812
EER	1.88
FAR	0.0098
FRR	0.18

Table 2: Comparison Analysis of the proposed and existing model

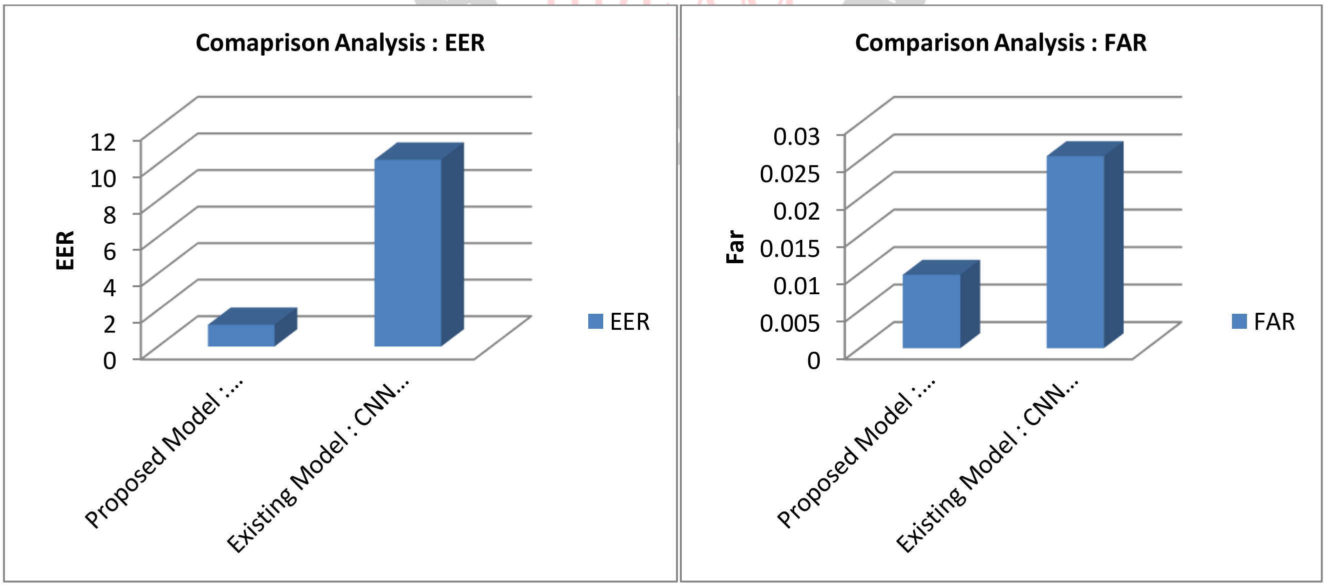
Parameters	**Proposed Model: Component-based AL-CNN model**	**Existing Model: CNN model**
EER	1.88	10.22
FAR	0.0098	2.56
FRR	0.18	1.17
HTER	0.9812	1.42
Accuracy	99.008	97.54

Table 1 shows the proposed model performance metrics with an accuracy rate value of 99.008 percent, EER value of 1.88, FAR value of 0.0098, and FRR value of 0.18. Table 2 shows the comparison between proposed and existing models. This proposed model has attained a high accuracy rate and reduced the error rate , FAR, and FRR rate compared with the existing model.



(i) (ii)

Figure 9 (i) Comparison analysis with proposed and existing model: HTER and (ii) Comparison analysis with proposed and existingomodel: FRR



(i) (ii)

Figure 10 (i) Comparison analysis with proposed and existing model: EER and (ii) Comparison analysis with proposed and existing model: FAR

DOI : 10.35291/2454-9150.2022.0307

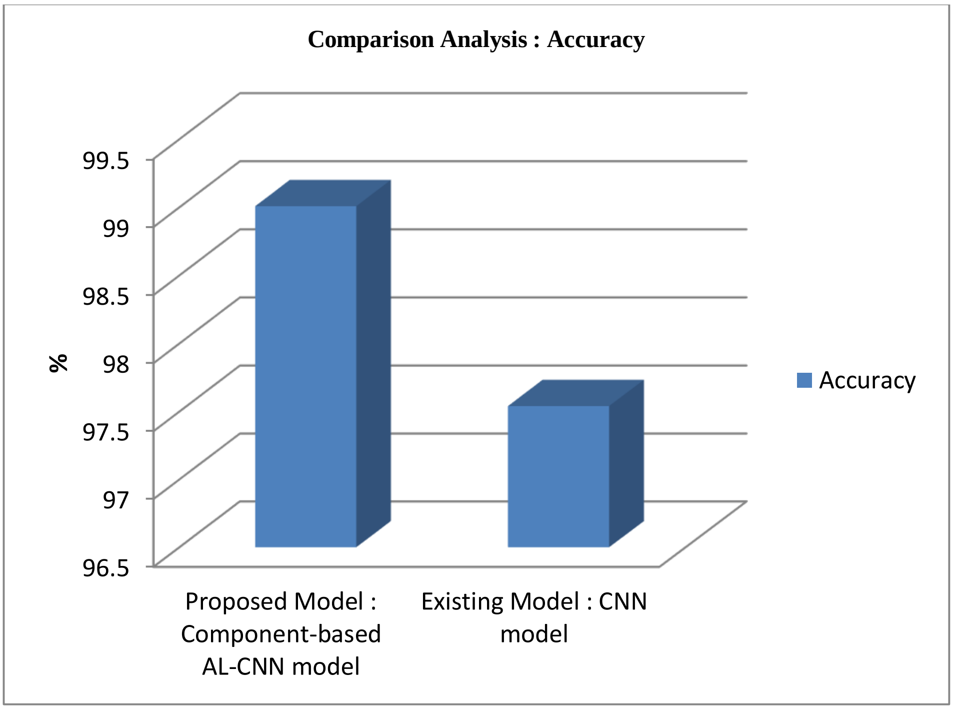


Figure 11. Comparison Analysis with Proposed and Existing model: Accuracy Rate

Figure 9(i),9(ii),10(i), and 10 (ii), show the analysis of the performance of Component-based AL-CNN model and Existing model using CNN classifier model concerning HTER, FAR, FRR, and EER rate. It validates that the component-based AL-CNN model gives minimum values of the performance metrics compared to the CNN model. Figure 10 shows that the component-based AL-CNN classifier model gives maximum values of the performance metrics compared to the CNN model.

VI. Conclusion and Future Work

Deep learning models offer an effective anti-spoofing solution. However, because of limited training data and a time-consuming process, fine-tuning or creating a CNN model from the start remains difficult for face faking photos. This research has introduced a face anti-spoofing approach based on improved CNN learning and inference and built essential parameters extracting texture information from the face image colour space using an LBP. The CASIA-FASD dataset was utilized for performance verification. Images from videos were retrieved and classified as printed photo assaults, clipped photo attacks, and video replay attacks. These photos from the CASIA-FASD dataset were utilized for both training and testing. It was proven that isolating the colour space from the face picture and the Cb, S, and V colour spaces enhanced detection performance, which is important for anti-spoofing. Previous research often employed a 6-channel (YCbCr + HSV) colour system, which resulted in high computing expenses.

On the contrary, the suggested method decreases the computational load by focusing on only three colour space channels (Cb, S, and V). It intends to test the performance against another well-known face spoof dataset in the future. It will try to use pruning algorithms to compress convolutional neural networks to reduce the dimension of the feature and speed up detection.

References

[1] Yu, Z., Li, X., Shi, J., Xia, Z., & Zhao, G. (2021). Revisiting pixel-wise supervision for face anti-spoofing. IEEE Transactions on Biometrics, Behavior, and Identity Science.

[2] Parkin, A., & Grinchuk, O. (2019). Recognizing multi-modal face spoofing with face recognition networks. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops* (pp. 0-0).

[3] Liu, A., Li, X., Wan, J., Liang, Y., Escalera, S., Escalante, H. J., ... & Li, S. Z. (2021). Cross-ethnicity face anti-spoofing recognition challenge: A review. *IET Biometrics*, *10*(1), 24-43.

[4] Sun, W., Song, Y., Chen, C., Huang, J., & Kot, A. C. (2020). Face spoofing detection based on local ternary label supervision in fully convolutional networks. *IEEE Transactions on Information Forensics and Security*, *15*, 3181-3196.

[5] Fatemifar, S., Asadi, S., Awais, M., Akbari, A., & Kittler, J. (2022). Face spoofing detection ensemble via multistage optimisation and pruning. *Pattern Recognition Letters*, *158*, 1-8.

[6] Quan, R., Wu, Y., Yu, X., & Yang, Y. (2021). Progressive transfer learning for face anti-spoofing. *IEEE Transactions on Image Processing*, *30*, 3946-3955.

DOI : 10.35291/2454-9150.2022.0307

[7] Song, X., Zhao, X., Fang, L., & Lin, T. (2019). Discriminative representation combinations for accurate face spoofing detection. *Pattern Recognition*, *85*, 220-231.

[8] Jia, S., Hu, C., Li, X., & Xu, Z. (2021). Face spoofing detection under super-realistic 3D wax face attacks. *Pattern Recognition Letters*, *145*, 103-109.

[9] Nagpal, C., & Dubey, S. R. (2019, July). A performance evaluation of convolutional neural networks for face anti spoofing. In *2019 International Joint Conference on Neural Networks (IJCNN)* (pp. 1-8). IEEE.

[10] Moon, Y., Ryoo, I., & Kim, S. (2021). Face antispoofing method using color texture segmentation on fpga. *Security and Communication Networks*, *2021*.

[11] Chen, H., Hu, G., Lei, Z., Chen, Y., Robertson, N. M., & Li, S. Z. (2019). Attention-based two-stream convolutional networks for face spoofing detection. *IEEE Transactions on Information Forensics and Security*, *15*, 578-593.

[12] Khammari, M. (2019). Robust face anti-spoofing using CNN with LBP and WLD. *IET Image Processing*, *13*(11), 1880-1884.

[13] Balamurali, K., Chandru, S., Razvi, M. S., & Kumar, V. S. (2021, June). Face Spoof Detection Using VGG-Face Architecture. In *Journal of Physics: Conference Series* (Vol. 1917, No. 1, p. 012010). IOP Publishing.

[14] Ebihara, A. F., Sakurai, K., & Imaoka, H. (2021). Efficient Face Spoofing Detection With Flash. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, *3*(4), 535-549.

[15] Hashemifard, S., & Akbari, M. (2021). A compact deep learning model for face spoofing detection. *arXiv preprint arXiv:2101.04756*.

[16] Arora, S., Bhatia, M. P. S., & Mittal, V. (2021). A robust framework for spoofing detection in faces using deep learning. *The Visual Computer*, 1-12.

[17] Papers with Code - CASIA-FASD Dataset. (2022). Retrieved 30 May 2022, from https://paperswithcode.com/dataset/casia-fasd.

[18] Li, L., Feng, X., Xia, Z., Jiang, X., & Hadid, A. (2018). Face spoofing detection with local binary pattern network. *Journal of visual communication and image representation*, *54*, 182-192.

[19] Harsh Namdev Bhor, & Dr.Mukesh Kalla. (2022). Analysis Of Performance Comparison Of Intrusion Detection System Between Svm, Naïve Bayes Model, Random Forest, K-Nearest Neighbor Algorithm. 17(05), 128–144. https://doi.org/10.5281/zenodo.6601187

[20] Balamurali, K., Chandru, S., Razvi, M. S., & Kumar, V. S. (2021, June). Face Spoof Detection Using VGG-Face Architecture. In *Journal of Physics: Conference Series* (Vol. 1917, No. 1, p. 012010). IOP Publishing.

[21] Bhor, Harsh Namdev and Mukesh Kalla. “An Intrusion Detection in Internet of Things: A Systematic Study.” 2020 International Conference on Smart Electronics and Communication (ICOSEC) (2020): 939-944.

[22] Khammari, M. (2019). Robust face anti-spoofing using CNN with LBP and WLD. *IET Image Processing*, *13*(11), 1880-1884.

DOI : 10.35291/2454-9150.2022.0307