







Comparison of Fine-Tuned Networks on Generalization for Face Spoofing Detection

Swapnil R. Shinde¹, Sudeep D. Thepade², Anupkumar M. Bongale^{3*}, Deepak Dharrao⁴

¹ Department of Computer Science and Information Technology, Symbiosis Institute of Technology, Pune Campus, Symbiosis International (Deemed University), Pune 412115, Maharashtra, India

² Department of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune 411017, Maharashtra, India

³ Department of Artificial Intelligence and Machine Learning, Symbiosis Institute of Technology, Pune Campus, Symbiosis International (Deemed University), Pune 412115, Maharashtra, India

⁴ Department of Computer Science and Engineering, Symbiosis Institute of Technology, Pune Campus, Symbiosis International (Deemed University), Pune 412115, Maharashtra, India

Corresponding Author Email: anupkumar.bongale@sitpune.edu.in

(This article is part of the Special Issue **AI-Powered Finance: Exploring the Impact of AI in FinTech**)

Copyright: ©2024 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/ria.380110>

ABSTRACT

Received: 9 September 2023

Revised: 22 November 2023

Accepted: 29 December 2023

Available online: 29 February 2024

Keywords:

biometrics authentication, deep convolutional neural network, face liveness, transfer learning, VGG network

Spoofing is a primary security concern for all the organizations and researchers across the globe. Security can be achieved through different mediums; authentication is one such important medium. Biometric Authentication is considered as an important and strong form that's difficult to break. Biometric authentication mainly includes two mechanisms, viz. Physiological and Behavioral. Physiological traits include the face, fingerprint, retina, iris, palm geometry, etc. Face Recognition has many application areas due to its ease of implementation, and they can be easily fooled or spoofed, termed as Face Spoofing Attack. Face spoofing attacks are viz. 2D and 3D attacks, 2D Attacks include Fake photo, Warped photos, Video display and 3D attacks performed using 3D masks. Deep learning methods have proved beneficial for detecting spoofing attacks; these methods use fine-tuned and pre-trained models. The paper compares the proposed fine-tuned VGG16 and RESNET-50 architectures and their generalization performance of Face Spoofing Detection. The 3D MAD and NUAA Imposter Dataset are used to validate the performance for two color spaces viz. RGB and YCBCR; the results are obtained for both color spaces. RGB color space is related to human visual system but it's not invariant to illumination on the other hand YCBCR separates chrominance and luminance part which makes it illumination invariant and face recognition systems have reflectance issue. Cross-dataset evaluation is an important metric for face liveness detection. The paper presents cross dataset results on the above datasets with the lowest HTER of 18%. The fine-tuned VGG-16 architecture gives the best values for cross-dataset evaluation when trained on 3D MAD and tested for NUAA imposter dataset and same is true for RESNET-50 architecture.

1. INTRODUCTION

Biometrics is considered the most secure and robust method for authenticating an individual as it's simple to implement and difficult to break; it includes mainly two mechanisms, viz. Physiological and Behavioral. Face recognition [1] is a widely used and incorporated mechanism for achieving security goals in different application areas of high impact. Physiological traits include the face, fingerprint, retina, iris, palm geometry, etc. Authentication systems [2] use Face Images; face recognition systems (FRS) are subject to spoofing attacks. Deep learning methodology has proved useful and important for biometrics [3] pre-trained architectures such as VGG-16, RESNET-50 etc. have shown higher accuracy up to 95% [3] and have been implemented for real time FRS. It has not only improved the system's performance but has also helped to reduce the time complexity of the entire process of biometric

implementation. 3D face recognition systems have advantages over 2D systems such as invariant to face position, expression, and occlusion. It's widely used in applications such as surveillance, human computer interaction, access control etc. Face Recognition systems security is compromised through spoofing attacks. Spoofing attacks use mechanisms to break the authentication system to get access to confidential data. Different attack methods for face spoofing are primarily categorized into 2D and 3D attacks. The 2D [1] and 3D attack methods include Printed photos, Image Display, Video Replay Attack & 3D Mask attack [4]. 3D attacks are performed using 3D mask made from different materials such as silicon, resins which have smooth surface that makes it easy to fool the FRS. 3D Attack detection can be performed by extraction of relevant and useful features from face images with State of The Art (SOTA) mechanisms. The most comprehensive approach is based on texture [5] and shapes features of 3D face

images.

The broad categorization of the systems for 3D face presentation attack detection [6] is as software-based or hardware-based, or hybrid (software and hardware). The 3D mask is made of other materials such as latex, silicone, and resin; these mask materials also affect the recognition systems to a greater extent. The key issue in face liveness detection [5] systems based on mask attacks is reflectance differences and illumination variations introduced during the capture process. The software-based systems mainly involve extracting meaningful and insightful features from the data using different methodologies such as Shape, Texture, Color, and Hybrid methods to extract information for detecting 2D and 3D spoof attacks [3]. Many researchers have also tested deep learning-based feature extraction and classification in the past; it has shown improvements over traditional machine learning approaches. The deep methods mainly use Convolutional Neural Networks (CNNs) [7] for deep learning tasks; scratch and pre-trained models have been experimented with to improve face recognition performance. The pre-trained models use many layers and take a lot of time to train; they perform well but add a lot of overhead that needs to be considered while using these models.

The paper presents Comparison of two pre-trained architectures for detecting 2D and 3D attacks. The VGG-16 [8] and ResNet-50 [6] model is fine-tuned and applied to the 2D and 3D attack datasets. The results are evaluated based on the standard performance metrics and compared with the existing systems proposed in the literature.

The Key contribution of the research includes the following:

- The paper presents Fine-tuned VGG-16 and ResNet-50 network for generalization in attack detection with improved performance and compares performance with SOTA methods.
- The paper compares the color space-based results of the proposed fine-tuned architectures and their pre-trained architecture for 2D and 3D attack dataset.
- Cross-dataset evaluation results presented and analyzed for the proposed fine-tuned architectures are quite promising.

The following sections of the paper focus on Survey, Proposed System, Experimentation Results, and Analysis with their Discussion.

2. RELATED WORK

Some recent works that use pre-trained models for face liveness detection are discussed in the following section.

The authors [8] have proposed a system based on YCBCR and CIELUV color space that uses VGG-Face architecture for spoof detection. The authors denoised the face images and converted them to the above color space before passing them to the VGG-Face. Face detection was performed using MTCNN (Multi-task Cascaded Convolutional Neural Network), and denoising was performed using non-local means denoising. The VGG-Face CNN is a modified VGG-16 that uses the average pooling layer as the end layer instead of the classification layer to extract the Deep Features. MTCNN is a cascaded network that achieves best results for the error metrics compared to the SOTA methods.

Deep learning has evolved rapidly over the past decade, with new algorithms developed for extracting deep features in various contexts. Researchers have found success using deep

learning models for detecting attacks against faces in images and videos. The authors [9] extracted features using two CNN models (VGG16 & ALEXNET). The activation features of the first fully connected layer (fc6 or fc7) were obtained and concatenated. The SVM classifier performs the features classification; result comparison is performed in terms of standard metrics.

A unique system has been proposed by Hao et al. [10], face liveness detection is done before face recognition based on customer identity information. The Siamese Network is trained on pairs of images, followed by feature extraction & matching by the Alexnet model. The pair of images consists of 2 real images or 1 real and 1 fake image; this pair combination enlists valuable features and performs matching to identify real and fake. This unique system incorporates Face recognition module in its working which is of great advantage.

In one method, the authors [11] have applied a nonlinear diffusion-based additive operator scheme to enhance edges. These diffused images are forwarded to CNN to extract complex features using three different models: CNN-5, ResNet50, and InceptionV4; the result presented an analysis that InceptionV4 performs better than other CNN models. The Accuracy achieved was 100% for learning rate of 0.01 by Adam Optimizer for 10 epochs with a categorical cross-entropy loss function for InceptionV4. Computation time was longer for InceptionV4, although the Accuracy was high.

Recent research in Convolutional Neural Networks is based on defining multi-channel CNNs [12], where channels refer to different types of input-to-face images, such as RGB images, grayscale images, thermal images, infrared, etc. Different devices take different pictures and videos. The different channel combinations result in a more robust framework. One of the main drawbacks of multi-channel CNN is that the channels must be aligned perfectly to capture data. Alignment can be difficult to do when there are lots of interfering signals.

Another research involves designing an attention-based system with a Two Stream Convolution Neural Network (TSCNN) [13] using RGB and Multi-Scale Retinex Space (MSR). In the attention-based system, features are extracted from RGB and MSR space using the RESNET-18 model, combined, and then passed FC and SoftMax to classify and match to get values for different parameters such as APCER, BPCER, HTER, EER, etc. Deep Learning models outperform hand-made feature models for machine learning in all the papers discussed in this section.

The authors [14] have proposed a system that fuses the handcrafted features with in-depth features to improve the generalization capability of face spoofing detection. The fused architecture extracts texture features using LBP and its variant and in-depth features using Deep CNN architecture for the color space YCBCR and LUV; these are passed to the SVM classifier for classification. The generalization is tested by performing the cross-data set evaluation of the standard parameters. Four datasets are used for testing, and the proposed architecture results are improving compared to the existing models.

The recent research in 2D and 3D attack detection using deep learning mainly focuses on fine-tuning the existing pre-trained deep learning models to improve the performance and deal with all the attack scenarios. Exploration of existing pre-trained models to devise a generalized detection model is the need of the future for face presentation attack detection. Color Space comparisons have been performed in literature for generalization in attack detection for both 2D and 3D attacks.

The paper presents use of two color spaces with fine-tuning of pre-trained models to improve the detection performance compared to the SOTA methods.

3. PROPOSED FINE-TUNED ARCHITECTURES

The proposed system consists of Fine-tuned VGG-16 and Fine-tuned ResNet50 architectures to evaluate the 2D and 3D attack datasets. These two pre-trained architectures are best suited for image classification tasks and have been trained on image dataset too. Face spoofing detections proposed in literature make use of the trained layers of these architecture to achieve higher performance. The generalized block diagram of the proposed system for face spoofing detection is shown in Figure 1 below.

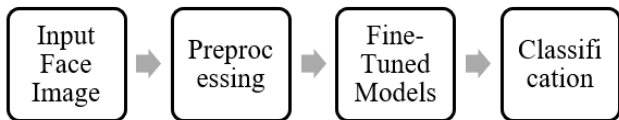


Figure 1. Block diagram of proposed system

3.1 VGG-16 fine-tuned

The VGG-16 [8] architecture consists of 16 layers in all with 13 Convolution and 3 fully connected layers which is trained on 1000 different classes and best used for image classification tasks. VGG-16 architecture with fine-tuning is shown below in Figure 2; it has 13 Convolution layers with 5 max-pooling layers & 2 dense layers, 1 Flatten layer; the total count of layers is 21. Out of this, only 16 layers have a weight assigned and used for feature extraction and

classification of the input data, All the convolution layers i.e. trainable layers are made false except the last 3 as these layers provide key features for the input images for better classification. The Datasets considered for evaluation are the 3D MAD [15] dataset and the NUA A Imposter [16] dataset.

RGB color space is related to human visual system but it's not invariant to illumination on the other hand YCBCR separates chrominance and luminance part which makes it illumination invariant. Thus, the RGB and YCBCR color space are used in proposed system. The input consists of images of size 64*64*3 consisting of face images of fake and real subjects. Fine-tuned VGG-16 architecture consists of two Fully Connected layers of 4096 units and 1072 units; a Dropout layer with 20% dropouts is added before the classification layer. The Adam Optimizer was used for the VGG-16 architecture with a learning rate of 10⁻⁴.

3.2 ResNet-50 fine-tuned

The ResNet-50 architecture is one the deep network architecture with 50 layers that has strong feature representation capability with higher classification accuracy. It connects lower layer to upper layer that resolves gradient issue. The Resnet-50 fine-tuned architecture is shown below in Figure 3. The top layers are removed and replaced with a single Dense layer of 512 units instead of two dense layers as compared to its original architecture for better parameter quantity. All the convolution layers i.e. trainable layers are made false except the last 3 layers and combined with new output layers to perform the classification task. Adam Optimizer used for the fine-tuned architecture with a learning rate of 10⁻⁴.

Comparison of various parameters for the proposed architectures is shown in Table 1 below.

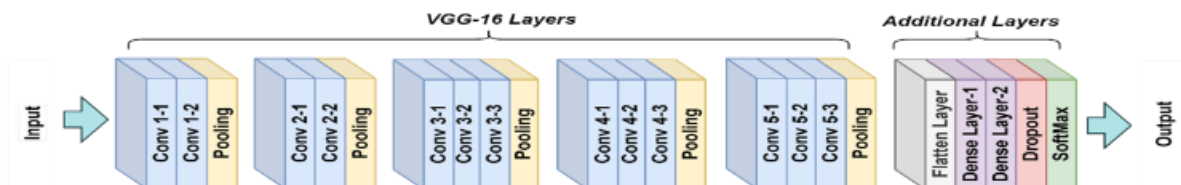


Figure 2. Proposed fine-tuned Vgg-16 architecture

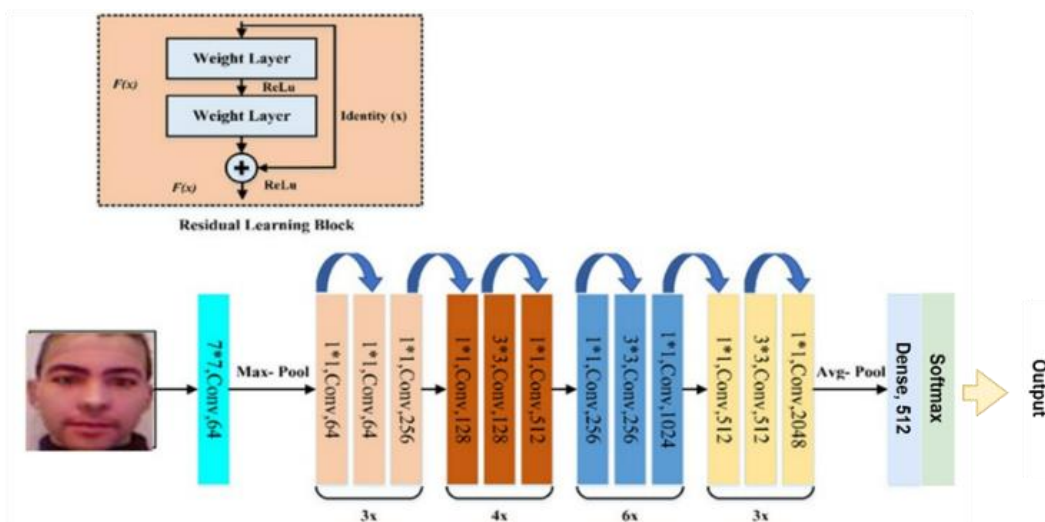


Figure 3. Proposed fine-tuned ResNet-50 architecture

Table 1. Comparison of proposed architectures

Parameters	VGG-16 Fine-Tuned	ResNet-50 Fine-Tuned
Number of Blocks	21	51
Input Size	64*64*3	64*64*3
Trainable Parameters	15,146,642	1,054,210
Optimizer	Adam	Adam
Learning Rate	10 ⁻⁴	10 ⁻⁴

4. RESULTS AND DISCUSSION

This section presents the results obtained for the proposed architecture for two datasets viz. 3D MAD [16] and NUAA [17] imposter. 3D MAD dataset is the most widely used publicly available 3D attack dataset that has been used by many researchers to validate the Spoofing attack scenarios. NUAA is a 2D attack dataset with photo print attacks used to validate 2D attacks.

Dataset for two different color spaces with Epoch values set to 50 and 60. Evaluation metrics used are Accuracy, Bonafide Presentation Classification Error Rate (BPCER) [17], Attack Presentation Classification Error Rate (APCER) and Half Total Error Rate (HTER) [18] which are the standard metrics set for Spoof detection. The result and analysis are discussed in terms of the fine-tuned proposed systems, cross-dataset evaluations and comparison with the state of the art methods

implemented for generalization of spoof attack detection. The objective is to comment on the improved performance of the proposed systems in terms of detection of both 2D and 3D face spoof attacks.

4.1 VGG-16 pre-trained and proposed fine-tuned architecture results

The Graph in Figure 4. Shows the results obtained on **3D MAD** for the pre-trained VGG-16 architecture and the proposed Fine-tuned VGG-16 architecture in terms of RGB and YCBCR color space [19]. The best accuracy obtained is 100% for pre-trained architecture and 99.08% for proposed fine-tuned model for the RGB color space for Epoch 60 whereas the proposed fine-tuned architecture performs best for the YCBCR color space for Epoch 50 with accuracy of 95.14%.

In terms of the other performance metrics the best value for HTER is 0 for Epoch 60 for RGB [20] color space and 0.68% for the proposed architecture as can be seen in below Figure 5.

NUAA: - The best accuracy obtained is 94.11% for the proposed fine-tuned model for the RGB color space for Epoch 60 whereas the pre-trained architecture performs best for the YCBCR color space for Epoch 60 with accuracy of 88.44% as shown in Figure 6. In terms of the other performance metrics the best value for HTER [21] is 6.69% for Epoch 60 for RGB color space on proposed architecture and 10.44% for the pre-trained architecture as can be seen in below Figure 7.

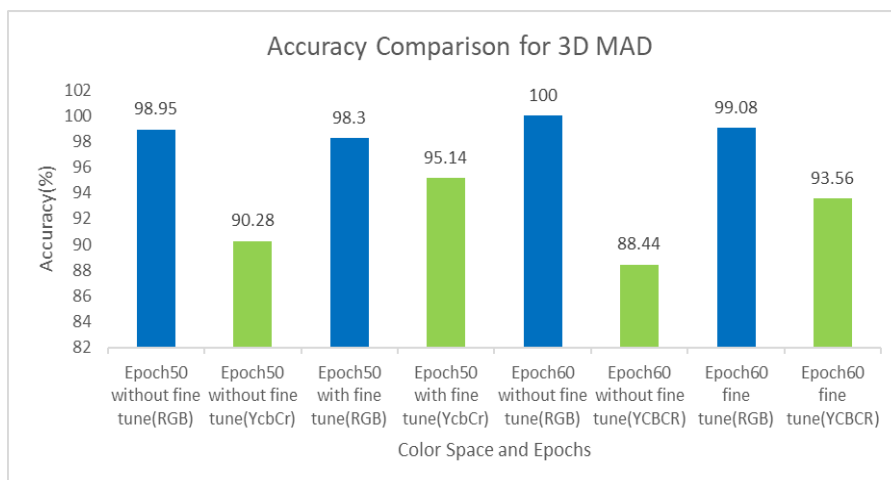


Figure 4. Accuracy comparison results for VGG-16 for 3D MAD dataset

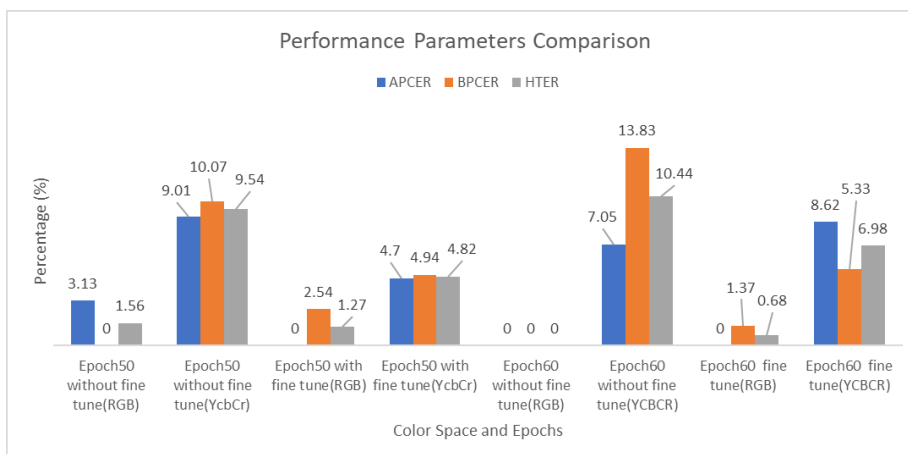


Figure 5. Performance metrics comparison for VGG-16 for 3D MAD dataset

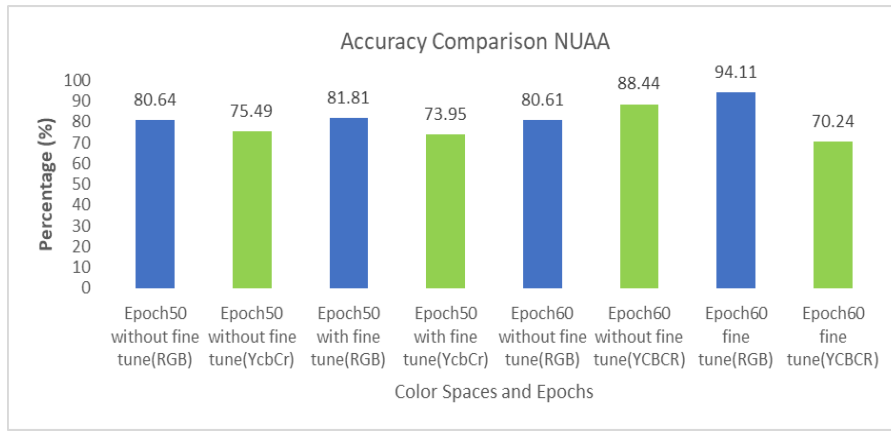


Figure 6. Accuracy comparison results for VGG-16 for NUAA dataset

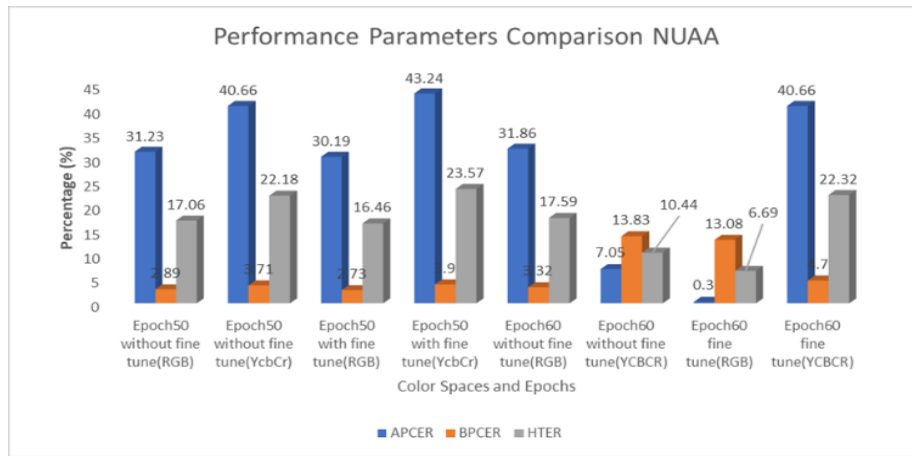


Figure 7. Performance metrics comparison for VGG-16 for NUAA dataset

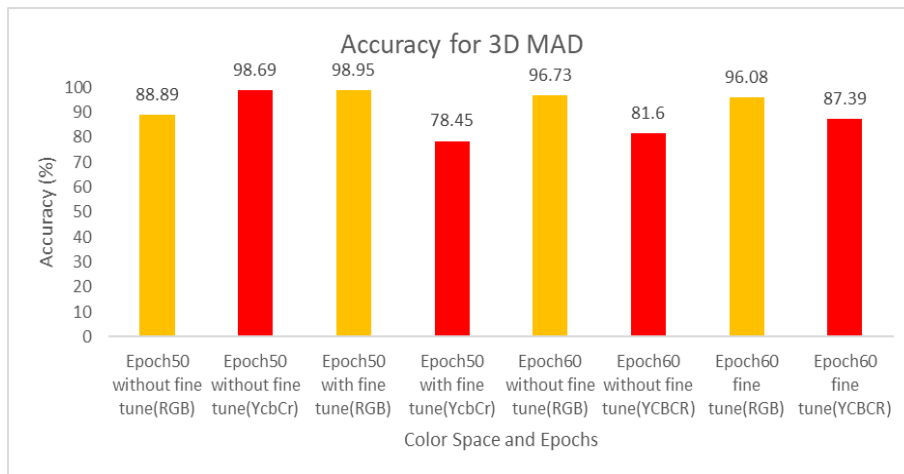


Figure 8. Accuracy comparison for ResNet-50 for 3D MAD dataset

4.2 ResNet-50 pre-trained and proposed fine-tuned architecture results

The ResNet-50 fine-tuned architecture performs best for Epoch 50 on **3D MAD** dataset with an accuracy of 98.95% on RGB color space. and its pre-trained architecture achieves best accuracy of 98.69% for the same Epoch on YCBCR [22] color space as can be seen in below Figure 8. In terms of the other performance metrics the best value for HTER is 0.88% for Epoch 50 for RGB color space on proposed architecture and 2.64% for the pre-trained architecture as can be seen in below

Figure 9.

NUAA: - The Fine-tuned ResNet-50 architecture performs best for the NUAA dataset too, it achieves the highest accuracy of 94.22% for the YCBCR color space for Epoch 60 and 92.57% for RGB color space for Epoch 50 for its pre-trained model, refer Figure 10. The other performance metrics also achieve HTER as low as 5.78% for the Fine-tuned model on the YCBCR color space and 6.92% on the RGB color space, as shown in Figure 11.

The best results for NUAA dataset are obtained for the YCBCR color space for all the performance metrics for the

fine-tuned model whereas for 3D MAD dataset the best results are obtained on the RGB color space as can be seen from the above discussion.

The overall results discussion clearly state that the Proposed architectures perform extremely well for detection of both the types of attacks 2D and 3D attacks. The minimum accuracy obtained is 78.45% for 3D MAD and maximum is 99.08% for RGB color space which clearly indicates generalization capability of the proposed architectures. The same is true for NUAA dataset too which has minimum accuracy of 70.24%

and maximum value as 98.95%. The lowest HTER value obtained is 0.67% which indicates a low error rate. Next, we present the comparison of results with the SOTA methods.

4.3 Comparison of proposed system with the state of art methods

The proposed fine-tuned architecture results are compared with the existing State of Art (SOTA) [23] methods used on the same datasets; Table 2 below shows the same.

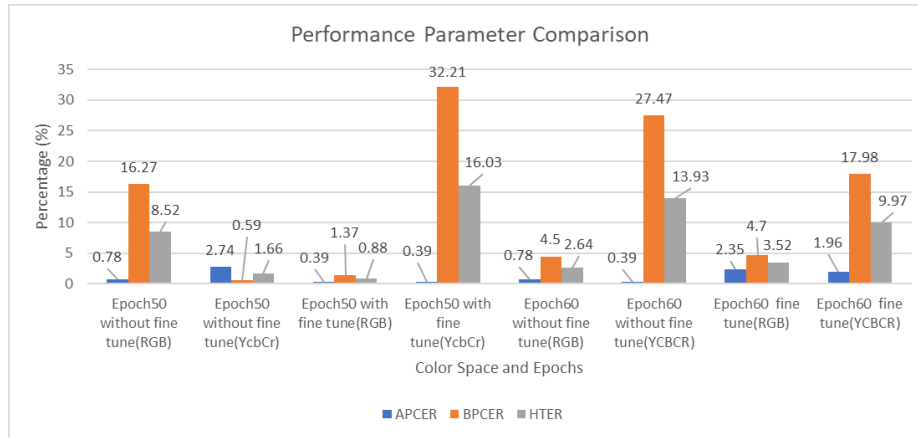


Figure 9. Performance metrics comparison for ResNet-50 for 3D MAD dataset

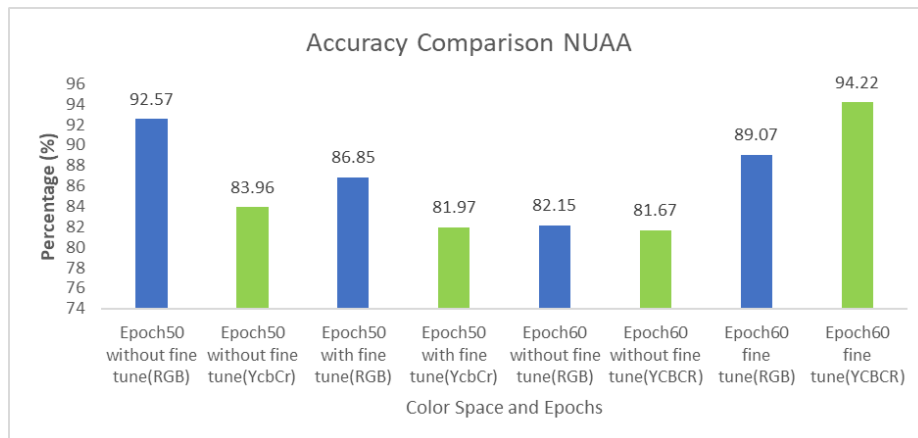


Figure 10. Accuracy comparison for ResNet-50 on NUAA dataset

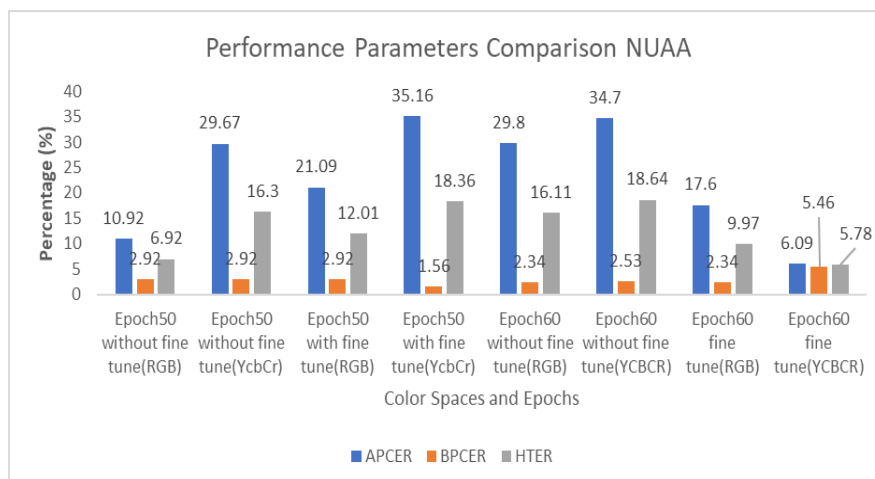


Figure 11. Performance metrics for ResNet-50 on NUAA dataset

The proposed system achieves best HTER of 0.67% which is quite good compared to the existing method for the 3D MAD dataset and 5.78% for NUAA dataset that needs to be improved. The proposed fine-tuned networks perform extremely well both for the handcrafted features [24, 25] and VGG features as can be seen in Table 2.

Cross Dataset Results:

The cross-dataset results are satisfactory for the proposed architectures as can be seen in Table 3. The best accuracy obtained is 76.68%, which is quite promising and indicates a lower error rate in detection as low as 18.66%. Thus, the architecture achieves the objective of improving the generalization capability in spoof detection on 2D and 3D attacks.

Color Space Comparison and Model Performance:

The RGB Color space [26] for Epoch 60 on 3D MAD dataset achieves highest results using VGG-16 whereas

YCbCr color space for Epoch-60 dataset achieves best results on NUAA dataset using ResNet-50 as can be seen in above graphs. In terms of the models VGG-16 is trained on ImageNet dataset that consists of color images (RGB) and achieves a good accuracy, in the proposed system the fine-tuned VGG-16 also reflects the same results. 3D MAD dataset consists of high color variations of RGB color space, thus VGG-16 achieves best results on RGB compared to YCBCR. On the other hand, NUAA dataset has low color variation compared to 3D MAD thus NUAA has higher results when fed to the ResNet-50 [27] architecture. Thus the color space and the architecture used are crucial in terms of the model performance, based on the properties of the architectures used we have achieved the expected results.

Higher the Epochs more is the training and best features are extracted by the hidden layers, thus tested the system with different number of Epochs and found Epoch 50 and 60 have good impact on model performance so used them for all the comparisons.

Table 2. Comparison of proposed fine-tuned architecture with SOTA methods

Technique	Dataset	HTER (%)
DWT+LBP (Block 16x16) (24,3) [14]	3D MAD	0.01
MS_LBP [3]	3D MAD	12.29
IDA [9]	3D MAD	13.88
LBPTOP [10]	3D MAD	5.41
Joint Discriminative Learning [11]	3D MAD	1.76
VGG16 [25]	3D MAD	0
Proposed VGG 16 Epoch 60 without fine tune RGB	3D MAD	0
Proposed VGG 16 Epoch 60 with fine tune RGB	3D MAD	0.67
VGG16 Ycbr+CIELUV with global pooling [8]	NUAA	0.368
Pretrained ResNet-50 Epoch 60 Fine-tuned model YCBCR	NUAA	5.78
VGG16 [23]	NUAA	28.41
VGG19 (Learning rate = 10-4, Scenario = "Original VGG") [24]	NUAA	18.7

Table 3. Cross dataset results

Architecture	Train	Test	Epoch	Accuracy (%)	APCER (%)	BPCER (%)	HTER (%)
Proposed Fine-Tuned VGG-16	3D MAD RGB	NUAA RGB	60	76.68	2.65	34.68	18.66
	NUAA	3D MAD	60	52.47	36.54	52.48	44.51
	YCBCR	YCBCR					
Proposed Fine-Tuned Resnet-50	3D MAD RGB	NUAA RGB	60	63.54	1.36	81.64	41.5
	NUAA	3D MAD	60	48.86	58.43	47.43	52.93
	YCBCR	YCBCR					

5. CONCLUSION AND FUTURE SCOPE

Face spoofing attacks are performed on the individuals or an organizations authentication system with an intent to steal, capture or hijack the data from the end systems. These attacks may lead to monetary losses along with losses to individuals personal/confidential data so detecting the attacks and mitigating them is researched over the globe. 2D and 3D attacks are performed on face recognition systems to break them and tamper with the systems authentication mechanisms. The solutions developed for detection of these attacks include software based, hardware based or fusion of software and hardware-based systems, this paper we have addressed and presented one such solution to improve the generalization of

spoof detection by modifying or updating the existing transfer learning models. The modifications are performed on the VGG-16 and ResNet-50 transfer learning models and fine-tuned architecture are proposed and evaluated for their generalization capabilities. The results are presented for the standard metrics used in spoofing attack detection and compared with the SOTA methods proposed in literature. The comparison is performed in terms of two-color spaces as both yield different sets of features when passed through the proposed architectures. The best accuracy obtained is 99.08% for RGB color space for 3D MAD dataset with fine-tuned VGG-16 with HTER of 0.67%. The comparison with SOTA methods clearly indicates that the proposed architecture performs well for both the attack categories and can be used

on any other 2D or 3D attack datasets available publicly.

The proposed system uses deep features extracted from the architecture whereas some of the SOTA methods in literature use handcrafted features so a combination of deep and handcrafted features can be a scope for studying the performance of these architectures or any systems proposed for generalization in spoof detection.

REFERENCES

- [1] Bhattacharjee, S., Marcel, S. (2017). What you can't see can help you-extended-range imaging for 3D-mask presentation attack detection. In 2017 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, pp. 1-7. <https://doi.org/10.23919/BIOSIG.2017.8053524>
- [2] Boulkenafet, Z., Komulainen, J., Hadid, A. (2016). Face spoofing detection using colour texture analysis. *IEEE Transactions on Information Forensics and Security*, 11(8): 1818-1830. <https://doi.org/10.1109/TIFS.2016.2555286>
- [3] Sikha, O.K., Bharath, B. (2022). VGG16-random fourier hybrid model for masked face recognition. *Soft Computing*, 26(22): 12795-12810. <https://doi.org/10.1007/s00500-022-07289-0>
- [4] Erdogmus, N., Marcel, S. (2014). Spoofing face recognition with 3D masks. *IEEE Transactions on Information Forensics and Security*, 9(7): 1084-1097. <https://doi.org/10.1109/TIFS.2014.2322255>
- [5] Edmunds, T., Caplier, A. (2018). Motion-based countermeasure against photo and video spoofing attacks in face recognition. *Journal of Visual Communication and Image Representation*, 50: 314-332. <https://doi.org/10.1016/j.jvcir.2017.12.004>
- [6] Kong, Y., Li, X., Hao, G., Liu, C. (2022). Face anti-spoofing method based on residual network with channel attention mechanism. *Electronics*, 11(19): 3056. <https://doi.org/10.3390/electronics11193056>
- [7] Hashemifard, S., Akbari, M. (2021). A compact deep learning model for face spoofing detection. *arXiv preprint arXiv:2101.04756*. <https://doi.org/10.48550/arXiv.2101.04756>
- [8] Balamurali, K., Chandru, S., Razvi, M.S., Kumar, V.S. (2021). Face spoof detection using vgg-face architecture. *Journal of Physics: Conference Series*, 1917(1): 012010. <https://doi.org/10.1088/1742-6596/1917/1/012010>
- [9] Şengür, A., Akhtar, Z., Akbulut, Y., Ekici, S., Budak, Ü. (2018). Deep feature extraction for face liveness detection. In 2018 International Conference on Artificial Intelligence and Data Processing (IDAP), Malatya, Turkey, pp. 1-4. <https://doi.org/10.1109/IDAP.2018.8620804>
- [10] Hao, H., Pei, M., Zhao, M. (2019). Face liveness detection based on client identity using Siamese network. In: Lin, Z., et al. *Pattern Recognition and Computer Vision. PRCV 2019.*, vol 11857. Springer, Cham. https://doi.org/10.1007/978-3-030-31654-9_15
- [11] Koshy, R., Mahmood, A. (2019). Optimizing deep CNN architectures for face liveness detection. *Entropy*, 21(4): 423. <https://doi.org/10.3390/e21040423>
- [12] George, A., Mostaani, Z., Geissenbuhler, D., Nikisins, O., Anjos, A., Marcel, S. (2019). Biometric face presentation attack detection with multi-channel convolutional neural network. *IEEE Transactions on Information Forensics and Security*, 15: 42-55. <https://doi.org/10.1109/TIFS.2019.2916652>
- [13] 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. <https://doi.org/10.1109/TIFS.2019.2922241>
- [14] Pinto, A., Goldenstein, S., Ferreira, A., Carvalho, T., Pedrini, H., Rocha, A. (2020). Leveraging shape, reflectance and albedo from shading for face presentation attack detection. *IEEE Transactions on Information Forensics and Security*, 15: 3347-3358. <https://doi.org/10.1109/TIFS.2020.2988168>
- [15] Chen, F.M., Wen, C., Xie, K., Wen, F.Q., Sheng, G.Q., Tang, X.G. (2019). Face liveness detection: Fusing colour texture feature and deep feature. *IET Biometrics*, 8(6): 369-377. <https://doi.org/10.1049/iet-bmt.2018.5235>
- [16] Erdogmus, N., Marcel, S. (2013). Spoofing in 2D face recognition with 3d masks and anti-spoofing with Kinect. In 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), Arlington, VA, USA, pp. 1-6. <https://doi.org/10.1109/BTAS.2013.6712688>
- [17] Tan, X., Li, Y., Liu, J., Jiang, L. (2010). Face liveness detection from a single image with sparse low rank bilinear discriminative model. In: Daniilidis, K., Maragos, P., Paragios, N. (eds) *Computer Vision – ECCV 2010*. *ECCV 2010. Lecture Notes in Computer Science*, vol 6316. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-15567-3_37
- [18] Menotti, D., Chiachia, G., Pinto, A., Schwartz, W.R., Pedrini, H., Falcao, A.X., Rocha, A. (2015). Deep representations for iris, face, and fingerprint spoofing detection. *IEEE Transactions on Information Forensics and Security*, 10(4): 864-879. <https://doi.org/10.1109/TIFS.2015.2398817>
- [19] Naveen, S., Fathima, R.S., Moni, R.S. (2016). Face recognition and authentication using LBP and BSIF mask detection and elimination. In 2016 International Conference on Communication Systems and Networks (ComNet), Thiruvananthapuram, India, pp. 99-102. <https://doi.org/10.1109/CSN.2016.7823994>
- [20] Raghavendra, R., Busch, C. (2014). Novel presentation attack detection algorithm for face recognition system: Application to 3d face mask attack. In 2014 IEEE International Conference on Image Processing (ICIP), Paris, France, pp. 323-327. <https://doi.org/10.1109/ICIP.2014.7025064>
- [21] Lucena, O., Junior, A., Moia, V., Souza, R., Valle, E., Lotufo, R. (2017). Transfer learning using convolutional neural networks for face anti-spoofing. In: Karray, F., Campilho, A., Cheriet, F. (eds) *Image Analysis and Recognition. ICIAR 2017. Lecture Notes in Computer Science()*, vol 10317. Springer, Cham. https://doi.org/10.1007/978-3-319-59876-5_4
- [22] Das, P.K., 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 2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Zhengzhou, China, pp. 33-38. <https://doi.org/10.1109/SOLI48380.2019.8955089>

- [23] Abdullakutty, F., Elyan, E., Johnston, P., Ali-Gombe, A. (2022). Deep transfer learning on the aggregated dataset for face presentation attack detection. *Cognitive Computation*, 14(6): 2223-2233. <https://doi.org/10.1007/s12559-022-10037-z>
- [24] Thepade, S.D., Dindorkar, M., Chaudhari, P., Bang, S. (2022). Face presentation attack identification optimization with adjusting convolution blocks in VGG networks. *Intelligent Systems with Applications*, 16: 200107. <https://doi.org/10.1016/j.iswa.2022.200107>
- [25] Joshi, S.A., Bongale, A.M., Olsson, P.O., Urolagin, S., Dharrao, D., Bongale, A. (2023). Enhanced pre-trained xception model transfer learned for breast cancer detection. *Computation*, 11(3): 59. <https://doi.org/10.3390/computation11030059>
- [26] Dharrao, D.S., Uke, N.J. (2019). Fractional Krill–Lion algorithm based actor critic neural network for face recognition in real time surveillance videos. *International Journal of Computational Intelligence and Applications* 18(2): 1950011. <http://dx.doi.org/10.1142/S1469026819500111>
- [27] Joshi, S.A., Bongale, A.M., Bongale, A. (2021). Breast cancer detection from histopathology images using machine learning techniques: A bibliometric analysis. *Library Philosophy and Practice*, 2021: 1-29.