National College of Ireland

Classification of Spoofing Attack Detection using Deep Learning Algorithms

MSc Research Project
Data Analytics

Shreya Verma
Student ID: x20229291

School of Computing
National College of Ireland

Supervisor: Dr. Catherine Mulwa

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Shreya Verma
Student ID:	x20229291
Programme:	Data Analytics
Year:	2022
Module:	MSc Research Project
Supervisor:	Dr. Catherine Mulwa
Submission Due Date:	15/08/2022
Project Title:	Classification of Spoofing Attack Detection using Deep Learning Algorithms
Word Count:	XXX
Page Count:	25

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	
Date:	14th August 2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Classification of Spoofing Attack Detection using Deep Learning Algorithms

Shreya Verma
x20229291

Abstract

The spoofing attack detections are mostly used in day to day lives, like payment application, security application, phone password, bank account payment and so many with the advancement of the technology the spoofing attacks and cyber attacks are increasing very fast and with the newer technology the spoofing attack are not easily detected by the photos and videos of the authenticated person. The attacks take the photos of the particular person from the social media or any networking site and use the as the fake photo to hack the person's credentials and the passwords which may cause the cyber attacks and spoofing attacks. In photo frames and live photo the some temporal features like facial movement like eye movement, mouth movement are very difficult to detect. The main objective of our study is to provide the classification of the Biometric spoofing attack detection using deep learning algorithms. The convolution neural network is used to detect the biometric spoofing attack detection the models which were used for research are MobileNetV2, VGG16, ResNet50, regular CNN model to extract the facial feature and provide the accurate results. The study of the research also explains the classification of the images, computer vision techniques and the image predictions for the spoofing attack detection. The main objective is to identify the spoofing attack detection

1 Introduction

The spoofing attack detection is widely used in the, identification system, password and security for the individual person and biometric face recognition system. Now a day as we all use the laptop and the mobile phones has the face authentication system such as Toshiba and ASUS laptops George et al. (2019). As the technology increases the attacks assaults are also increasing. The hackers and the attackers use the printed images or the photos of the individual person. There are so many software's and applications are there that are mostly used to make the fake photos after that the attackers takes the images and upload it on the untrusted websites, unknown databases, and the uncontrolled remote authentication system. The reason of all this attacks increases the criminality in the various places of the world. As an example the attackers take the photos of the individual person and upload it on the fake social networking site. To address this issue and to overcome the spoofing attack the biometric spoofing attack detection this research is performed. For software based attack detection we need human interaction and participation the software based attack detection system takes much time to detect the spoofing attack. To detect the spoofing attack using software based biometric detection system it

is so expensive to install and deploy. To overcome this issue and reduce the time taken to detect the spoofing attack we were using deep machine learning algorithms using this techniques the spoofing attack detection is cost-effective and for this it does not require any human interaction.

The most of the spoofing attack detection required printed photos and live photos which can be replayed and recorded. There is very less amount of research has been done in the spoofing attack detection. Facial movements in live photos and videos are very difficult to identify the spoofing attacks. Hadid (2014) The motivation of this research is to reduce the time take to detect the spoofing attack and provide better accuracy. This research has been performed to detect the spoofing attacks that the images are real or fake images. According to the literature study, earlier work on spoofing attack detection relied on the visual appeal and texture of the images. The idea to investigate the convolution neural network for the classification of actual and fake images came from previous work and the literature review for the detection of spoofing attacks. The prior research and analysis did not adequately compare and draw conclusions about which algorithm would be most effective for spoofing attack detection. The research's primary goals are to learn about the deep convolution neural network, picture pre-processing, machine learning techniques, computer vision application in the convolution neural network, and comparison of the various machine.

The objective of the research topic in section 1.1 is to provide a crucial reference for improvements in the detection of biometric spoofing attacks.

1.1 Research Question

"To what extend can the detection of biometric spoofing attack detection be improved using deep machine learning algorithms (MobileNetV2, Vgg16, ResNet50, CNN, EfficientNet-LSTM?

Sub RQ: "Can hybrid classification and detection models for biometric spoofing attack detection improve the accuracy of models performance?

To answer the research question and sub research question, all the objectives related to the research is mentioned in section 1.2 and the implementation and evaluation of the all the objectives are presented in the section 4.

1.2 Research Objective and Contribution

The main objective is to detect the biometric spoofing attack

Obj 1. Critical review of the literature review to detect the spoofing attack.

Obj 2. Prepare data for analysis, Identify the long term use of biometric spoofing attack detection and the analysis of the spoofing attack detection algorithms which will reduce the time complexity of the particular algorithms and the spoofing attack detection technology.

Obj 3.Implementation, Evaluation and results of the classification model using deep machine technologies.
Obj 3.1:Implementation, Observation, and Findings of MobileNetV2.
Obj 3.2:Implementation, Observation, and Findings of VGG-16.
Obj 3.3:Implementation, Observation, and Findings of ResNet50.
Obj 3.4:Implementation, Observation, and Findings of CNN.
Obj 3.5:Implementation, Observation, and Findings of EfficientNet-LSTM.

Obj 4.Comparison of Developed Models based on their accuracy and loss score.

Obj 5.Comparison of Developed Models with the Existing Models.

Obj 6.Spoofing attack Detection using different CNN Models.

Obj 7.CNN-LSTM Hybrid Architecture in Image Classification.

The following section investigates previous research on employing hybrid models to detects spoofing attacks. In parts 3 and 4 of the study, the technique and procedure are provided, which include a full review of the dataset selection, pre-processing of the data, and deep learning algorithms used. Sections 5 and 6 of the articles contain a discussion of the project's implementation, evaluation methodologies, and outcomes. The paper's last section 7 finishes with an overall overview as well as recommendations for future research.

2 Literature Review of Spoofing Attacks detections from (2000-2022)

2.1 Introduction

In the spoofing attack detection the images are real or fake it is very important and to classify the spoofing attack images the different researchers have applied various deep machine algorithms and the mostly used deep machine learning algorithm is convolution neural network and the reason of using this technique is that it provide the very good performance and improvement is done comparison of all the models. This spoofing attack detection provide the classification of the images between the real and fake images and it is binary classification.

In this literature review section it is related to the previous related work of the image classification and spoofing attack detection using deep learning algorithms. This section is divided in three different sections 1) Face Spoofing attack detection using CNN techniques. 2) Spoofing attack detection using hybrid CNN models. 3) Comparison and conclusion of the various previously performed spoofing attack detection algorithms.

2.2 Investigation of Spoofing attack detection using CNN Techniques

To achieve higher accuracy and avoid the overfitting in the models the data augmentation techniques is use in the deep learning models to train the data. Kumar et al. (2017) for face liveliness detection has used the sequential convolution network. For this detection he has performed the classification and feature extraction for the liveliness detection. The data pre-processing and feature extraction techniques have been applied to the dataset of the live images. The classification performed in this research is the binary image classification to detect the live and the fake images and three convolution neural network layer for the classification and sigmoid activation function is used. After the implementation of the CNN models the evaluation and results of the all the models are compared based on the classification report of the models and classification report the comparison of the accuracy, precision and recall percentage has been compared in the research and in the results concluded as that if in the classification report if the value of all the measures are less, than while training the model, the classifier need more data to train well in cross validation. The accuracy of the testing data and the training data is compared which is 96% and 94% and it is well good to accept the model for the face liveliness detection.

The image pre-processing is the initial step of the image classification. The image pre-processing is performed to resize the image and normalize the image pixels for the training data and to achieve good accuracy. de Souza et al. (2019) performed the pre-processing for the iris image classification. In pre-processing the images are normalize into the ring-shape and the region into the unified coordinate system. In the pre-processing implementation part the images are resize into the different pixels sixe for the better performance of the model.

In pre-processing there are several different data augmentation methods are there to applied. In Li et al. (2018) for pre-processing the data the eight data augmentation methods are applied. For classification of the face liveliness detection in the project the author applied the VGG16 model for the better accuracy and efficiency. In the evaluation and result part compared the accuracy of the model with several different convolution neural network model and the reason of using the data augmentation techniques in this research is to improve the accuracy of the model.

In computer vision, recognition system and detection system the multi-tasking learning is mostly used in the deep machine learning algorithms because using this quality of the images and the experimental performance of the research achieved accurate result as per the previous techniques. Abdullakutty et al. (2021) for the research used different convolution neural network models which are MobileNetV2, EfficientNet and ResNet for the facial recognition system. The facial recognition is the classification system in which the classification is done based on the real or fake image. It is a binary classification. After the implementation performed of all the models the evaluation and results of the machine learning algorithms are done based on the classification report the most important aspect considered for this research is accuracy. The comparison is done based on the validation data accuracy and the training data accuracy. So for the model EfficientNetB0 Model the validation accuracy is 95% and this number is good fit for the model. After this in the second part of the classification the author included the age and gender classi-

fication and for this the model used is Mobile-Net CNN model and the accuracy obtained from the MobileNet for gender and age classification is 13% and 97%. The convolution neural network is fine-tuned. For the different recognition model video based and emotions recognition they used MoblileNet and EfficeintNet for the feature extraction and for the classification different machine learning algorithms are used which are random forest and support vector machine. The comparison of the accuracy is done based on the single images and the grouped images and in the result the single image classification provide higher and better accuracy compared to group based facial recognition images. In the conclusion and the result part of the CNN model the identity feature of the pre-trained convolution neural network model is not suitable. The ResNet model which is used for the face recognition and it gives higher accuracy compared to the group based CNN models. Daniel & Anitha (2021)The multi-task CNN models provide better and accurate results for the detection related problems and it reduces the risk of the model overfitting and provide the better and accurate results.

In machine learning technology the deep fake image detection is one of the most advanced and mostly used techniques. GAN generative adversarial networks technology are used for the fake image creation. In so many fake image detection algorithms the GAN techniques are used to create the fake images. Toprak & Toygar (2021) done research for the fake image detection using several machine learning models and in the dataset for the fake images the GAN technique is used to create a fake images for the prediction of the fake and real images. Different convolution neural network models are used for the fake image detection which are Vgg16, Vgg19, DenseNet169, DenseNet201, DenseNet121 and ResNet50. For the comparison with the different models the author also implemented the custom model in which is included various layer like dropout, padding which are almost different from other models and it is not included in the previous models. The Evaluation of all the models are done based on the classification report which includes accuracy, precision, recall, F1 score and ROC curve graph. The 99% of the accuracy is obtained from the Vgg16 model compared to the other custom models.

Supervised learning techniques are used in data preparation to improve the performance of deep neural network algorithms. Biggio et al. (2015) proposed different deep neural network models the combination of the two models which are InceptionNet and ResNet. Other models are also trained which are Inception version 3, Squeezenet and Alexnet for the face recognition of the historical photographs. Siamese network is used to compare relatively similar different images are, however it lacks a categorization layer. The transfer learning model's performance is compared to that of various pre-trained models, and the best performing model is chosen for the subsequent experiment. Among all the models, the InceptionResNet-v1 fared best. Evaluation based on memory, precision, F1 score, and accuracy. For this model, the accuracy attained using InceptionResNet-v1 was 99%, which is substantially superior. Alexnet and Squeezenet both the models performed well for the same dataset. The conclusion from the paper is that for large dataset InceptionResNet-v1 not performed well but Alexnet and Squeezenet showed good results. InceptionResNet-v1 did not perform well for the huge dataset, while Alexnet and Squeezenet demonstrated good results, according to the paper's conclusion. For feature extraction and classification of goat face identification, Shibel et al. (2022)suggested a convolution neural network model. In data pre-processing, the image is first made grayscale and then cropped to only show the forehead in order to extract features. The goat

face is then identified using the YOLOv4 real-time object detection algorithm. For feature extraction, a proprietary convolution neural network with seven convolution layers is employed, and the final layer includes Softmax for image categorization. The author compared the findings with and without pre-processing procedures, but the dataset with pre-processing stages yielded a better result with increased performance and higher accuracy. The findings without pre-processing steps were compared by the author, but the dataset with pre-processing stages yielded better results with increased performance and higher accuracy. In the end, the customized CNN model outperformed the competition. Convolution neural network provides better results and improved accuracy for facial feature extraction and identification.

2.3 Critical Review of Spoofing Attack Detection using CNN-LSTM Techniques

While classifying the image as real or fake is done using LSTM, sequential feature extraction from each frame is done using CNN. A mixture of diffusion techniques and a particular convolution neural network was used by **?** to apply the CNN-LSTM architecture for facial liveliness detection on static image and video frames. put in place two unique end-to-end liveliness detection systems. The first method employed an alpha trainable network to create a smooth diffused image since smoothness is a crucial component for facial liveliness detection. The CNN model was then given this image after batch normalization, and on two distinct datasets, it achieved accuracy rates of 97.50% and 99.0%. The outcome is more accurate compared to a higher value when the smoothness diffusion value is lower. Feeding the diluted image.

The deep machine learning methodology's facial emotional recognition system is one of the most hard and fascinating fields since it provides insight into both human behavior and mental health. Nasiri et al. (2022) System for recognizing face emotions using deep machine learning using CNN-LSTM. The files include posed, unposed, and candid photos. The CNN-LSTM combo was utilized to feature and categorize the emotions into six separate groups. The datasets are normalized as part of the data pretreatment process. This study compares the outcomes of applying the CNN-LSTM architecture model to various datasets. In order to compare the results for the evaluation confusion matrix, accuracy, precision, and recall are used. For the CNN and LSTM layers, keras and tensorflow are employed. When comparing the results of the proposed model with those of the Multilayer Perceptron, CNN, and LSTM separately, it is shown that the suggested model performs significantly better than the MLP, CNN, and LSTM alone in classifying facial expressions. The suggested model, which combines CNN-LSTM for all three attributes, has superior accuracy, precision, and recall than any other models. The overall studies demonstrate that the proposed architecture outperforms cutting-edge facial emotion identification algorithms using the normal and candid image datasets.

The research is based on the identification of video violence using CNN LSTM combined with deep machine learning models. The dynamic image, which are movies with a succession of frames, uses both spatial and motion information for the identification or detection of objects in video frames as opposed to static images, which solely use spatial information to classify or detect fake images. Mansour & Abu-Naser (2022) For the fea-

ture extraction, CNN networks VGG16, VGG19, Inception v3, ResNet50, and Xception were mostly used. Each pixel in the two datasets used for the research—hockey battle data and crowded data—has a resolution of 360x288. CNN-LSTM was used to the unbalanced dataset for feature extraction and classification. The evaluation, which compared all four networks, was based on accuracy and the Kappa coefficient. As a result, Inception V3's kappa coefficients for the hockey battle dataset are superior to those of other networks, and Inception V3 and Xception are the two networks that produce the greatest results for the crowd dataset when compared to the other networks for the imbalanced dataset. The performance of Inception V3 was the best, and it is more accurate than RestNet50 and Xception. The kappa coefficient and accuracy are 90% and 0.83, respectively, which is the greatest among all relevant networks.

At order for the machine learning model to produce accurate results and perform better, data augmentation techniques are used in the data pre-processing stage. In a study, a CNN-LSTM hybrid deep machine learning model was utilized to detect vandalism Rupapara et al. (2021). Vandalism is the deliberate destruction of both public and private property by individuals. Following data preprocessing, the input picture data is sent to CNN for feature extraction, and the CNN's output is fed to LSTM for sequence prediction assistance. ResNet, which has 152 layers, is used by the convolution neural network to extract features, while LSTM, which has 4 layers, is utilized by the dense unit to recognize images. The results of the CNN-LSTM model and the standalone CNN are implemented on various datasets and compared. In contrast to the standalone CNN model's accuracy of 88%, CNN-accuracy LSTM's was higher at 98%. According to the study, the hybrid CNN-LSTM deep machine learning model is superior and produces more precise findings.

The simple linear clustering approach divides the images into uniform size, which is used to enhance image pre-processing. This algorithm is used to extract the super-pixels from the photos. In order to compare the performance of the two methods, Nasir et al. (2021) proposed a real-time driver tiredness detection system based on the CNN-LSTM model and feature-based detection algorithm. The pre-trained CNN model is used to extract the features from each super pixel as an input, and the output of the pre-trained CNN models is fed into the LSTM model for classification. When LSTM-based detection algorithm results are compared to feature-based detection algorithm results, the LSTM-based detection algorithm has a greater accuracy. This paper's conclusion is that when CNN-LSTM model is combined for feature extraction and classification, greater accuracy is obtained.

2.4 Identified Gaps and Conclusion

In conclusion of all the critical literature review for the spoofing attack detection the CNN models and CNN-LSTM models performs well. There are different models comparison is all done which explains the comparison of the existing models with all the developed models. For the image classification the CNN-LSTM hybrid model performed well compared to the other models. with the help of the data augmentation techniques the accuracy of the CNN models can be improved.

According to the results of the critical literature review there is need to develop the classification model for the biometric spoofing attack detection.

3 Spoofing Attack detection Methodology

3.1 Introduction

The proposed spoofing attack detection approach is within the scope of machine learning the various steps has been performed in the methodology part which explain the dataset and performed various transformation and pre-processing to the dataset to resize the image and provide good results. The previous research in the literature review as per the reference of (chapter 2) give the idea of exploring different machine learning models and the help to identify the different techniques used in the detection and recognition system.

In this methodology section this explains the proposed approach and solution for the research question and sub research question. This section is divided in different section which explains the design specification, flow of the process, model selection and evaluation, and the evaluation done based on which aspects. The section (3.2) presents the data selection for the spoofing attack detection. Section (3.3) provides the data pre-processing techniques and (3.4) provide the data transformation. The main objective and aim of the performed researched was to provide the comparison of the different machine learning models and choose the best model for the spoofing attack detection.

3.2 Spoofing Attack detection (Real or Fake images) Methodology approach

The machine learning and knowledge discovery database are responsible for the technique for spoofing attack detection (KDD). The KDD is mostly used machine learning approach in the detection research. There are two methodology knowledge discovery database (KDD) and the Cross-Industry standard data mining method (CRISP-DM). Chapelle et al. (1999) For the spoofing attack detection research used KDD approach for the implementation because the (CRISP-DM) is business application oriented approach and it always need project deployment compared to KDD. It provides more accurate and complete results. The below Figure 2. explains the structure of spoofing attack detection.

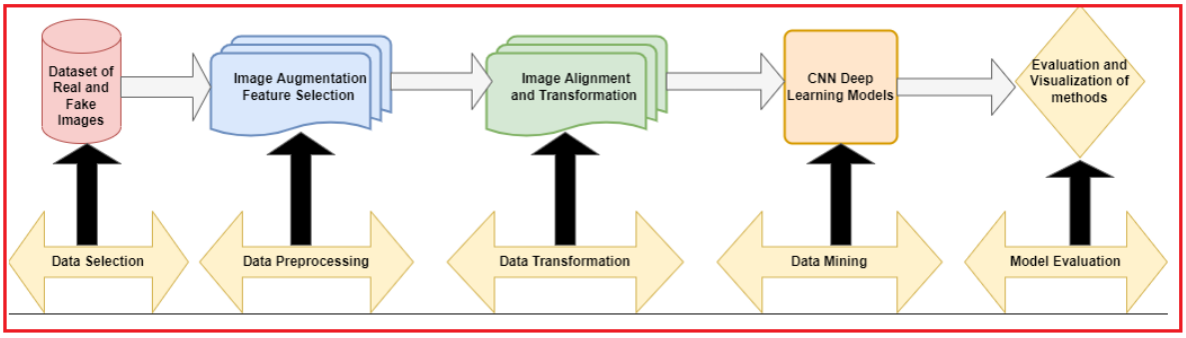

Figure 1: Structure of Spoofing Attack Detection Methodology

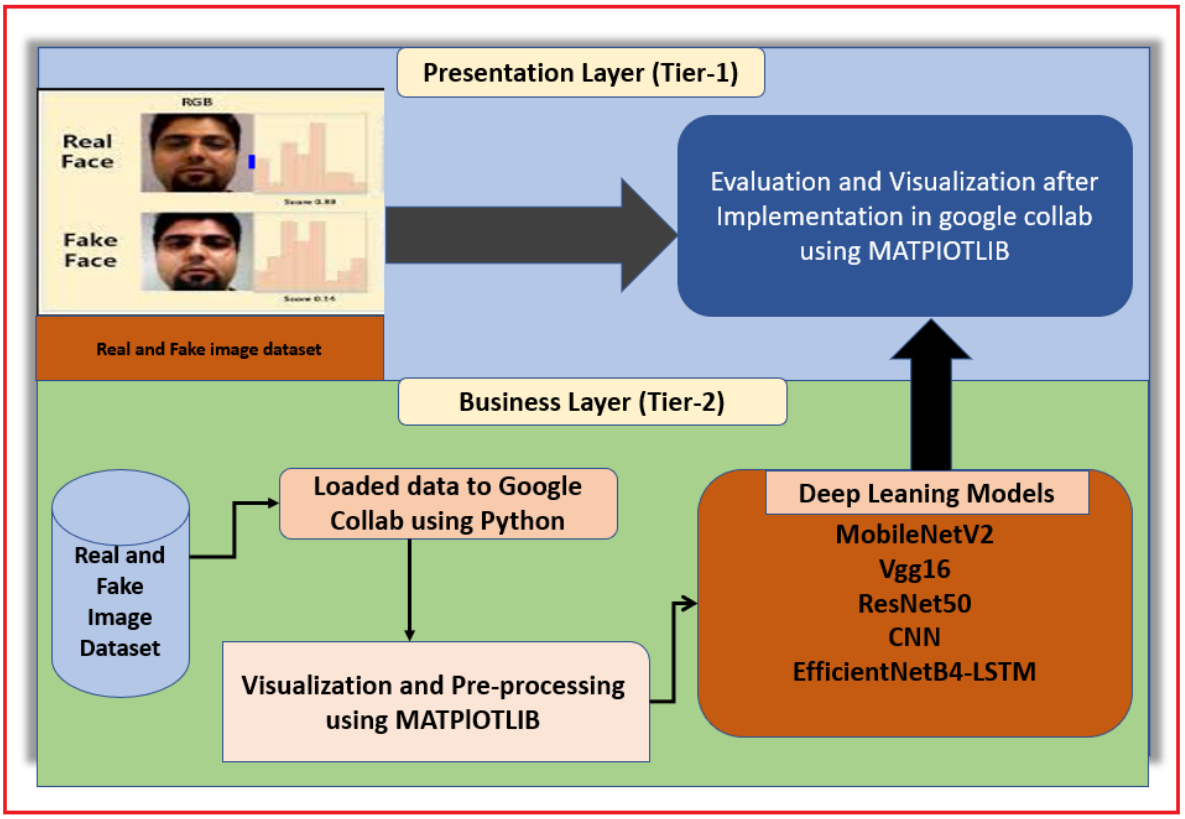

Figure 2: Design Specification

3.3 Data Selection for the spoofing attack detection

The images dataset which are used to performed research is of very low quality pixels or some of them are small in size. While working on the research at the time of choosing dataset always make sure that the data is in good quality and it has the sufficient amount of images. As the spoofing attack are increasing and the fake face are used for cyber attacks so the research is also increasing. The open source dataset of the images and videos are available on the so many websites like kaggle, FacbookAI, images datasets and so on. For this spoofing attack detection research used publicly available dataset which

is on kaggle of real and fake images. The dataset consist of real and fake images of the random peoples in very high resolution faces. It comprises of total 20,000 images in a good quality PNG images and pixels. The fake photos in the dataset are from Photoshop experts. The fake images are edited using the Photoshop tools.

3.4 Data Pre-processing of Real and Fake Images Data

To improve the model performance and result of the spoofing attack detection project the images should be pre-processed. The datasets consist of the so many errors, noises in the data and in the images dataset the size of the images are not proper. If the dataset are not clean and in proper format so the output of our research is not undesirable and it will not provide accurate value. For the desired output and correct result the data should be clean and any false information should be deleted from the dataset. Kamiran & Calders (2012) The real and fake datasets all the images were scaled and resized and data augmentation techniques are applied to the image dataset for generating new training dataset. In image data augmentation the images data are augmented into the updated changes and duplicated into the training set data. The data augmentation involves the horizontal flip, vertical flip, zoom in and zoom out of images, change the shear range value, rescale the images and many other approaches. The data augmentation is always applied on the training set of the dataset not on the validation set. The data pre-processing like image resizing of the images and the scaling of the pixels are different it can be done while processing the or training the models. For this fake or real mage dataset the batch size of the dataset taken as the 32 and resizing the images in the 241 * 241 the reason of resizing the images are the goggle colab GPU issue. When we process a large image dataset the colab did not work properly. So we have to resize the images in specific pixels. In python the tensorflow gives the built-in function for the data augmentation techniques. The below are the some images from the dataset which are real and fake images.

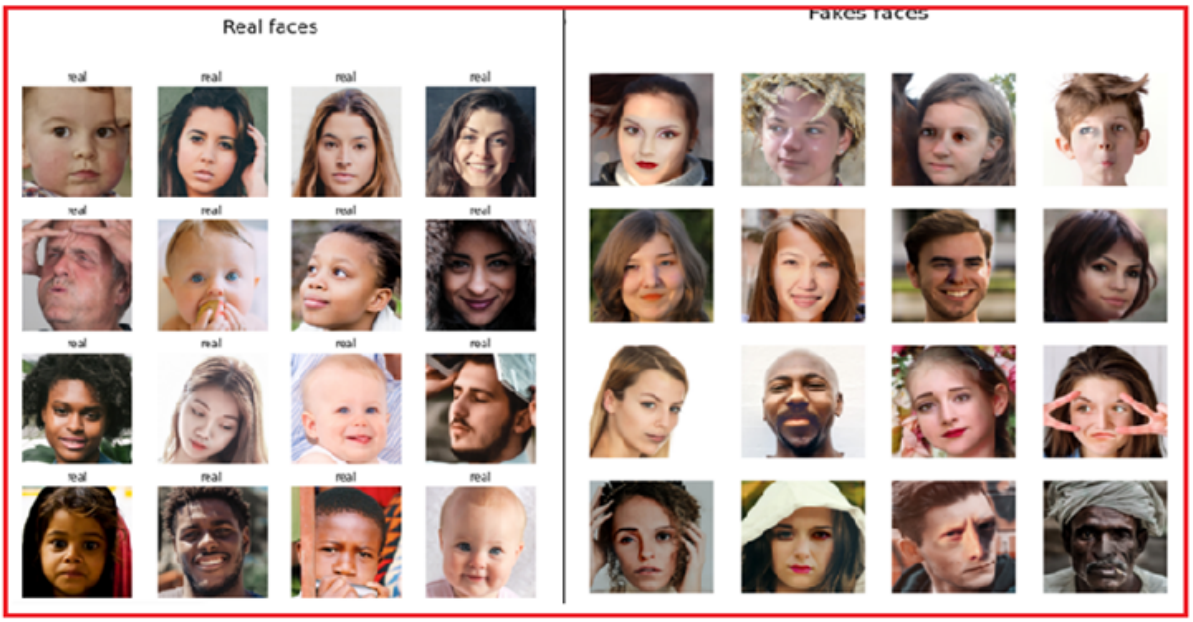

Figure 3: Real and Fake Images after pre-processing

3.5 Data Transformation

The data transformation is the process of converting the raw data into the formatted or structured data which is more suitable for the training the data modelling. The data transformation is the process in the images of the dataset removes the unnecessary white space from the images to provide the more accurate result for our classification models. After that the dataset is divided into the training and the validation set. The dataset divided is in between 70% and 30%. To provide the better accuracy and good result the validation data consist of the 30% images of the dataset and both the training and the validation set consist of the real and fake images.

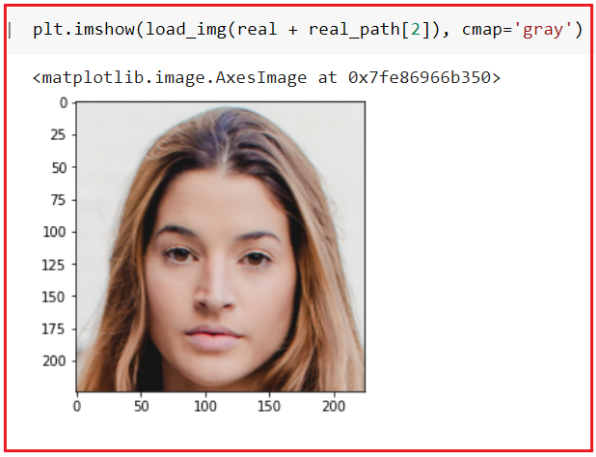

Figure 4: After data Transformation

3.6 Model Selection

After the data pre-processing and the data transformation the deep learning model selection is carried out in which in our research project this presents the convolution neural network architecture. The models presents are MobileNetV2, Vgg16, ResNet50 and basic CNN model all these models are used for the feature extraction and the all the images are classified into the real and fake images. Rokhana et al. (2021). All the deep learning CNN models consist of the different layers and classes. Among all the models the some of the models are pre-trained models. Some python libraries tensorflow and keras are used for the training all the convolution neural network models.

3.7 Model Evaluation

The spoofing attack detection is the classification of the fake or real images. While performing the classification and prediction in the deep machine learning there are four different measures need to be consider for the comparison of the result of all the models. Vujović (2021)In the spoofing attack detection for the model evaluation considered the confusion matrix and the classification report of the trained model. In the classification report the conditions which are needs to be checked are (1.True positive) which means that the if the image is fake and it is classified as fake then it is true positive. (2.True Negative) is that whenever the model predict that the image is real and it is real. (3.

False Negative) whenever the model predict the image is fake and it is real. All the cases of the true positive and false negative is depend on our system. The model evaluation is also done based on the accuracy of the model. The percentage of the model accuracy define the right classification of the fake or real images.

4 Implementation Evaluation and Results of Biometric Spoofing Attack Models

4.1 Introduction

This research are performed to find the solution of the Research question in the Ref. of chapter 1 section 1.2. The chapter has been divided into the sections based on the objectives set in 1.3. So, here the introduction of the models and the implementation, evaluation and results obtained are presented for the classification models.

The result obtained from the above formula values are compared for all CNN models.

4.2 Implementation, Evaluation and Results of MobileNetV2

The MobileNetV2 is the convolution neural network model. For the spoofing attack detection in model building the first model which is considered is mobileNetV2 which is proposed by the network of Google. For the feature extraction this model performed well. There are two version of the MobileNet convolution neural network which are MobileNetV1 and MobileNetV2. Basically this model is designed for the devices which has the low capacity to make sure the execution speed of the model and calculate the accuracy of the model while performing the classification of spoofing attack detection.

```
Model: "sequential"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 mobilenetv2_1.00_96 (Functi  (None, 3, 3, 1280)       2257984
 onal)

 global_average_pooling2d (G  (None, 1280)             0
 lobalAveragePooling2D)

 dense (Dense)               (None, 512)               655872

 batch_normalization (BatchN  (None, 512)              2048
 ormalization)

 dropout (Dropout)           (None, 512)               0

 dense_1 (Dense)             (None, 128)               65664

 dropout_1 (Dropout)         (None, 128)               0

 dense_2 (Dense)             (None, 2)                 258

=================================================================
Total params: 2,981,826
Trainable params: 722,818
Non-trainable params: 2,259,008
_________________________________________________________________
```

Figure 5: Implementation of MobileNetV2

The data given in the first step of the CNN model (MobileNetV2) contains 2257984 parameters in total. The second tier is an average global pooling layer with units of 1289,

the third layer is a dense layer with the activation function "relu," the fourth layer is batch normalization, which controls the advances to a layer for every mini-batch, and the fifth layer is a dropout layer with units of 0.5, which lessens the likelihood of model overfitting. In the layer beneath, we used a dense layer of 128 units in an effort to find more hidden feature trends. The model is put together utilizing the loss function of binary cross entropy and Adam's optimizer because the project's purpose is to identify real or false images. Durability is one.

4.2.1 Evaluation and Result of MobileNetV2

The spoofing attack detection is the classification research which helps to identify the images is real or fake. For the Evaluation of the classification model MobileNetV2we are considering the confusion matrix and the classification report to predict the model accuracy, precision and recall. In the below Figure 6 the accuracy is 94% and loss is 17% which is best among all the classification models.

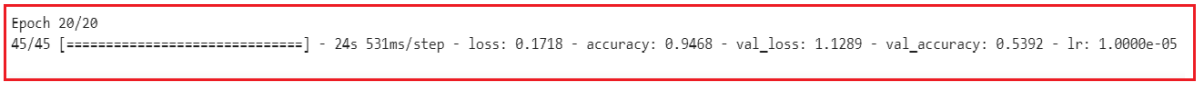

Figure 6: Accuracy and Loss percentatge of Model 1

In Figure 7 shows the classification report of the model MobileNetV2 shows that the accuracy and f1 score for the real and fake images which is 49% and 50%. This model not performed well for the classification of the real and fake images.

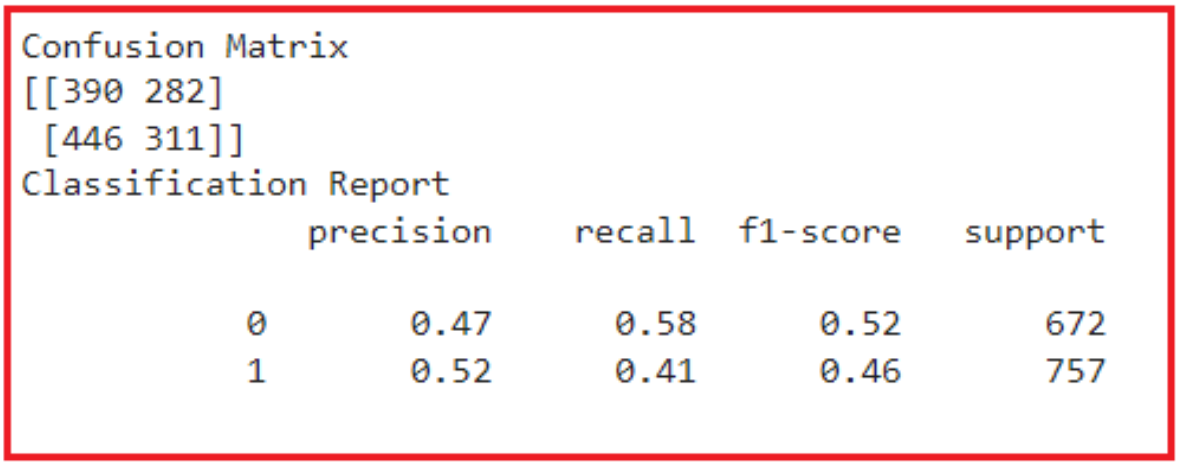

Figure 7: Classification Report of the MobileNetV2

In Figure 8 it shows the graphical representation of the validation accuracy and loss of each epoch. To present the graph the matplotlib python library is used. As per the graph the model accuracy is increasing and the loss is decreasing.

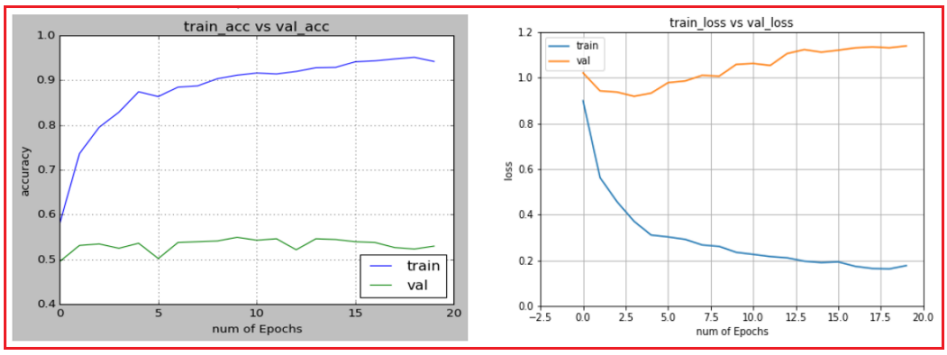

Figure 8: Plot of the Accuracy and Loss

4.3 Implementation, Evaluation and Results of VGG16

The deep learning network, which takes advantage of the architecture suggested by Google's VGG16 network, is used in the model building process to build the dataset, which is composed of an acceptable amount of data. The VGG16 model is built to be largely executed on portable and low-capability devices to ensure portability and execution speed while maintaining general accuracy in the phase of detection..

4.3.1 Implementation of VGG16

```
Model: "sequential"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 vgg16 (Functional)          (None, 7, 7, 512)         14714688

 flatten (Flatten)           (None, 25088)             0

 dense (Dense)               (None, 2)                 50178

=================================================================
Total params: 14,764,866
Trainable params: 50,178
Non-trainable params: 14,714,688
_________________________________________________________________
```

Figure 9: Implementation of VGG16

In VGG16 the convolution neural network model the first step is the vgg16 functional layer which has total 14714688 parameters. After that the second layer is flatten with the output shape of 25088 and at last the dense layer is there which helps to find out the hidden feature trend in the our dataset. The main objective of this project is to classify

the human images into real and fake images. For vgg16 we employed a simple model with less layer to find out the accuracy of the model and the performance. The loss function used in the vgg16 model while compiling is sparse categorical entropy and the sigmoid activation function. The Batch size is 16 for total 20 Epoch. The evaluation is done based on the accuracy and loss value of the training outcome.

4.3.2 Evaluation and Result of VGG16

The spoofing attack detection is the classification research which help to identify the images is real or fake. For the Evaluation of the classification model VGG16 are considering the train data accuracy and validation data accuracy and same for loss. The Confusion matrix and the classification report to predict the model precision, recall and F1-score. In the Figure 18 the accuracy of the model is 85% and loss is 38% which is quite good to accept the model.

```
Epoch 20/20
15/15 [==============================] - 31s 2s/step - loss: 0.3861 - accuracy: 0.8516 - val_loss: 0.7763 - val_accuracy: 0.5539 - lr: 1.0000e-05
```

Figure 10: Accuracy and Loss percentage of VGG16

```
Confusion Matrix
[[472 200]
 [539 218]]
Classification Report
              precision    recall  f1-score   support

           0       0.47      0.70      0.56       672
           1       0.52      0.29      0.37       757
```

Figure 11: Classification Report of VGG16

In Figure 11 it shows the classification report of the Vgg16 model with the confusion matrix. In the classification report the value of precision is 47%, recall is 70% and F-1 score is 56%. The graphical representation of the validation accuracy and loss of each epoch. To present the graph the matplotlib python library is used. As per the graph the model accuracy is increasing and the loss is decreasing.

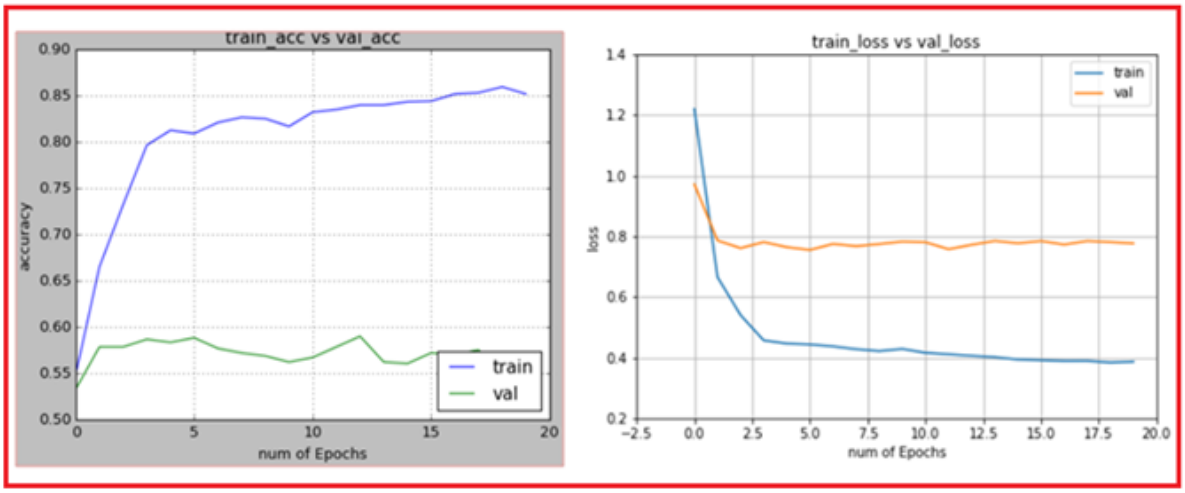

Figure 12: Plot of the Accuracy and Loss

4.4 Implementation, Evaluation and Results of ResNet50

ResNet stands for A residual neural network. The CNN model ResNet50 is the 50 layer deep machine leaning model. The ResNet50 can work with the 50 neural network layers. In the ResNet model it has various model. The ResNet50 has 48 convolution layer and one Maxpoolinga and average pooling layer. The accuracy in the ResNet model we get is 80% in 30 epoch.

4.4.1 Implementation of ResNet50

```
Model: "model"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 input_5 (InputLayer)        [(None, 224, 224, 3)]     0

 resnet50 (Functional)       (None, 7, 7, 2048)        23587712

 global_average_pooling2d (G  (None, 2048)             0
 lobalAveragePooling2D)

 flatten_1 (Flatten)         (None, 2048)              0

 dense_2 (Dense)             (None, 1024)              2098176

 dense_3 (Dense)             (None, 512)               524800

 classification (Dense)      (None, 20)                10260

=================================================================
Total params: 26,220,948
Trainable params: 26,167,828
Non-trainable params: 53,120
```

Figure 13: Implementation model of ResNet50

In the modle implementation of the ResNet50 in the first step the input size for the input is decalred after thata in second layer the resnet50 which is functional layer with the

23587712 parameter. The third layer is global average pooling layer 2d layer which helps to reduce the fully connected layer into the classical CNN layers and the it also block the size of the input width, input height and input channel of the block. The forth layer is flatten layer which helps to convert the 1D aaray into the input of the next convolution layer. After that the fifth layer is dense layer with 1024 output shape and parameter size is 2098176 which is deeply connected with the previous convolution layer. The last layer is classification dense layer which classify the classes into the real or fake images.

4.4.2 Evaluation and Result of ResNet50

The Evaluation of the ResNet50 model is done based on the accuracy percentage of the training and validiation data. The classification report is also used for the evaluating the results of the 3rd Modle. In the Figure 14 the accuracy of the model is 66% and loss is 60% and same the validation accuracy and validation loss of the model is 52% and 74%. The classification research that helps to determine whether an image is real or fraudulent is the spoofing attack detection. The confusion matrix and the classification report are taken into account when evaluating the classification model VGG16 in order to forecast its accuracy, precision, and recall.

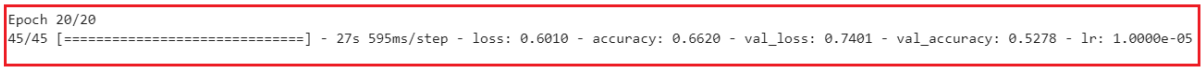

Figure 14: Accuracy and Loss percentage of ResNet50

In the Figure 23 the classification of the ResNet50 is generated in which the value of precision is 46%, recall is 83% and F1-score is 60% which is not good among all the models used for the comaprison of the spoofing atatck detection.

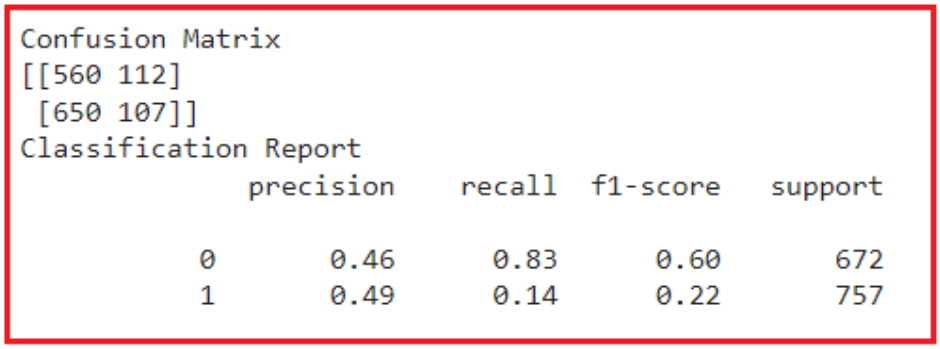

Figure 15: Classification report of ResNet50

The Figure 25it shows the graphical representation of the validation accuracy and loss of each epoch. To present the graph the matplotlib python library is used. As per the graph the model accuracy is increasing and the loss is decreasing.

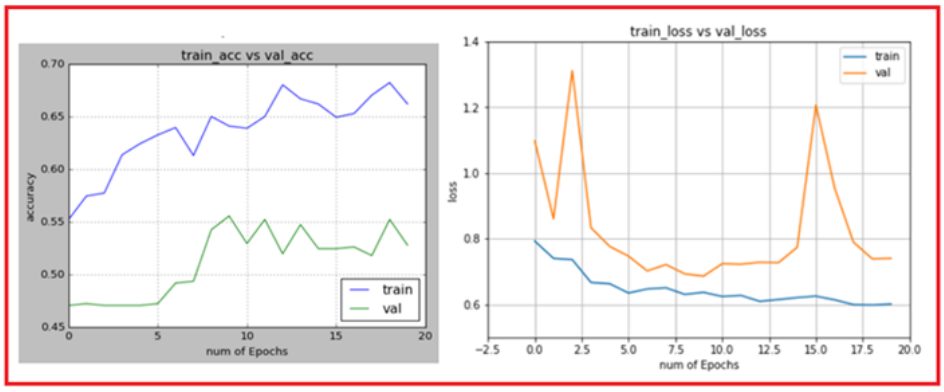

Figure 16: Classification report of ResNet50

4.5 Implementation, Evaluation and Results of CNN

The Basic CNN model is applied to fake or real image dataset. The convolution neural network model has several layers like convolution2D layer, maxpolling layer, Dense and flatten layer.

4.5.1 Implementation of CNN Model

```
Model: "sequential_1"
_________________________________________________________________
 Layer (type)                 Output Shape              Param #
=================================================================
 conv2d_3 (Conv2D)            (None, 94, 94, 16)        448

 max_pooling2d_3 (MaxPooling  (None, 47, 47, 16)       0
 2D)

 conv2d_4 (Conv2D)            (None, 45, 45, 32)        4640

 max_pooling2d_4 (MaxPooling  (None, 22, 22, 32)       0
 2D)

 conv2d_5 (Conv2D)            (None, 20, 20, 16)        4624

 max_pooling2d_5 (MaxPooling  (None, 10, 10, 16)       0
 2D)

 flatten_1 (Flatten)          (None, 1600)              0

 dense_2 (Dense)              (None, 256)               409856

 dense_3 (Dense)              (None, 1)                 257

=================================================================
Total params: 419,825
Trainable params: 419,825
Non-trainable params: 0
_________________________________________________________________
```

Figure 17: Implementation of CNN

In convolution neural network model the first layer is convolution2d layer with 448 parameter. After that the second layer is Maxpooling2d layer and several two or three max-pooling and convolution2d layer are added to the basic CNN model. The main aim of this project is to classify the human face images into real and fake images.

4.5.2 Evaluation and Result of CNN

The evaluation of the CNN model is done based on the accuracy and loss percentage value of the training and validation data. The CNN model classify the images into the real and fake image and with the help of classification report and accuracy percentage we can identify the model performance. In the Figure 18 the accuracy of the model is 81% and loss is 42% which is very less compared to other Models.

```
Epoch 20/20
45/45 [==============================] - 24s 544ms/step - loss: 0.4241 - accuracy: 0.8125 - val_loss: 0.9666 - val_accuracy: 0.5310
```

Figure 18: Accuracy and Loss percentage of CNN

```
Classification Report
              precision    recall  f1-score   support

           0       0.47      1.00      0.64       672
           1       0.00      0.00      0.00       757
```

Figure 19: Classification Report of CNN

In Figure 19 the classification report of the CNN model generated which shows the value of precision, recall and F-1 scor. The precision value is 47%, recall is 1 and F1-score is 64%.

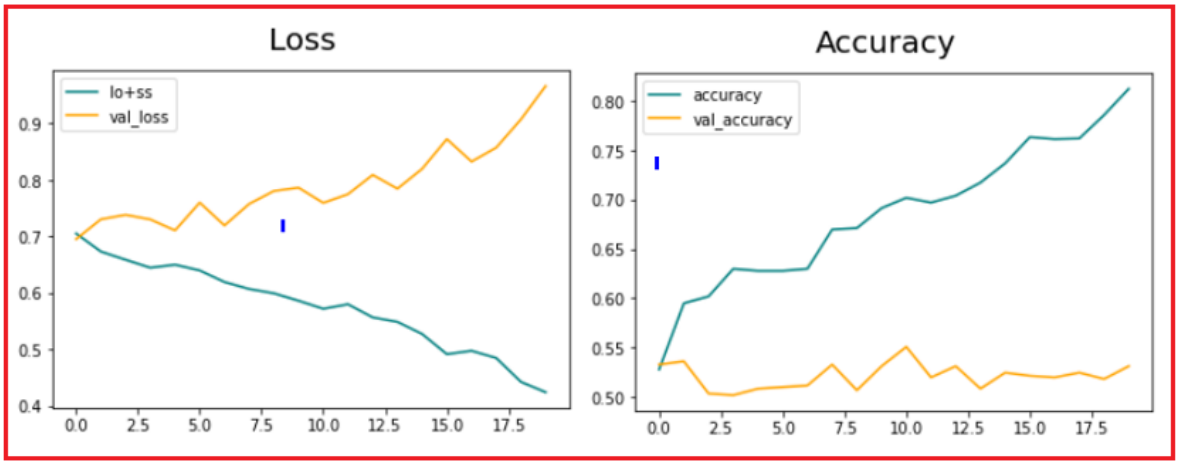

Figure 20: Plot of the Accuracy and Loss

4.6 Implementation, Evaluation and Results of EfficientNetB4-LSTM

This convolution neural network model has various versions from EfficientNet- B0 to EfficientNet-B7 which provide the better efficiency and accuracy in the classification models. The EfficientNet models performs very well compared to the convolution neural network models. As per the performance of the CNN models in terms of the accuracy of the model. The Efficient provide good results. The EfficientNet-B4 combined with the

LSTM model for the classification of the real or fake images. The combination of this models is known as the hybrid model.

4.6.1 Implementation of EfficientNetB0-LSTM

```
Model: "sequential"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 efficientnetb4 (Functional)  (None, 3, 3, 1792)       17673823

 dense (Dense)               (None, 3, 3, 512)         918016

 dropout (Dropout)           (None, 3, 3, 512)         0

 dense_1 (Dense)             (None, 3, 3, 128)         65664

 time_distributed (TimeDistr  (None, 3, 384)           0
 ibuted)

 lstm (LSTM)                 (None, 128)               262656

 dropout_1 (Dropout)         (None, 128)               0

 dense_2 (Dense)             (None, 100)               12900

 dense_3 (Dense)             (None, 1)                 101

=================================================================
```

Figure 21: Implementation model of EfficientNetB4

In this EfficientNetB4-LSTM hybrid model the first functional layer is EfficientNetB4 with parameter 17673823. The second layer is dense layer with 512 units and third and forth layer id dropout and dense layer. The Fifth layer is time distributed layer it helps to work with the photos and the video frame for the CNN model. For the classification of the Long short term memory classification layer to classify into the binary formate.

4.6.2 Evaluation and Result of EfficientNetB4-LSTM

In the hybrid CNN-LSTM (EfficientNetB4-LSTM) model the evaluation of this model is done based on the accuracy and the loss value percentage of the trained model in the last epoch. The accuracy of the hybird is not good compared to other models and the graphs of the accuracy and loss are not increasing compared to other models for the spoofing attack detction.

```
Epoch 20/20
64/64 [==============================] - 111s 2s/step - loss: 0.6938 - accuracy: 0.5091 - val_loss: 0.6915 - val_accuracy: 0.5294 - lr: 1.0000e-05
```

Figure 22: Accuracy and Loss percentage of EfficientNetB4-LSTM

In the Figure 23 the classification of the EfficientNetB4-LSTM is generated in which the value of precision is 47%, recall is 1% and F1-score is 64% which is not good among all the models used for the comaprison of the spoofing atatck detection.

Classification Report

	precision	recall	f1-score	support
0	0.47	1.00	0.64	960
1	0.00	0.00	0.00	1081

Figure 23: Classification report of EfficientNetB0-LSTM

The Figure 25it shows the graphical representation of the validation accuracy and loss of each epoch. To present the graph the matplotlib python library is used. As per the graph the model accuracy is increasing and the loss is decreasing.

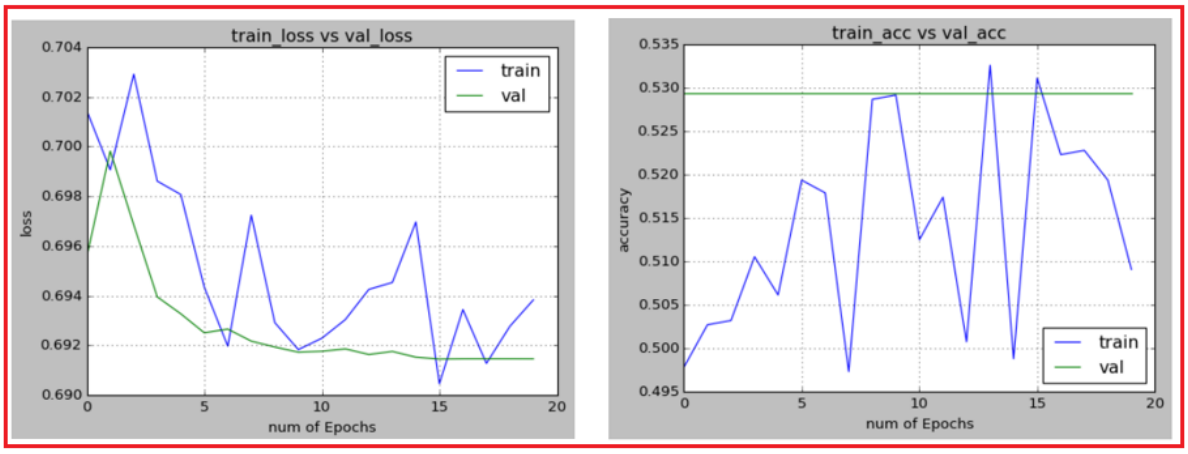

Figure 24: Classification report of EfficientNetB0-LSTM

5 Comparisons of All Models and Discussion

This section includes the comparison of all the developed models based on the validation loss and training loss of all the developed models based on the results declared in the section 4 which is implementation and evaluation of all the developed models.

5.1 Comparison of the Developed Models

Once the model implementation and evaluation is done the results of all the developed models are compared based on their train validation accuracy of the models. The convolution neural network models performed good for the spoofing attack detection and the

evaluation is done based on the 20 epochs in each model. In 20th epoch the accuracy of the MobileNetV2 is 96% which is well good to accept the model for the spoofing attack detection. After that Vgg16 also performed better the accuracy of the training and validation data is increasing as per the epoch increases and loss of both the data is decreasing the accuracy of the vgg16 model is 85%. After that the ResNet50 also performed well the accuracy for the ResNet50 model is 55% which is less among all the convolution neural network models. For the classification of the real and fake images the all the CNN models performed well the best accuracy got from the MobileNetV2 which is highest among the entire model. In the performance of the deep learning models the training time is very important for this the batch size of all the models are 32 and for all the models the epoch taken is 20 epochs. In the below table the training and validation accuracy is compared.

5.2 Comparison of the Existing Model with the Developed Model

Table 1 Model Comparison

Models	Train Accuracy	Training Loss
MobileNetV2 (Model 1)	94%	17%
VGG16 (Model 2)	85%	38%
ResNet50 (Model 3)	66%	60%
CNN (Model 4)	81%	42%
EfficientNetB4-LSTM	50%	69%

Figure 25: Comparison Table of Developed Model

In the above Table of the comparison of model done based on the Training accuracy of the model and training loss. For the spoofing attack detection the model which performed well for the classification of the real and fake image in the spoofing attack is MobileNetV2 the reason of that while training the model the model accuracy is highest among all the existing and the developed model which is 94% and the loss is 17%. After that the Vgg16 model also performed well compared to ResNet50, CNN and EfficientNetB4-LSTM model. In the discussion the model which performed well for the spoofing attack detection is MobileNetV2 and among all the highest accuracy achieved from this model. The hybrid model which is EffiecientNetB4-LSTM did not performed well because the accuracy of the hybrid model is very less.

6 Conclusion and Future Work

The main reason of the research project is to find out the solution of the research question " To what extend can the detection of biometric spoofing attack detection be improved using deep machine learning algorithms (MobileNetV2, Vgg16, ResNet50, CNN, InceptionNet-LSTM, EfficientNet-LSTM?" To detect the spoofing attack detection from the publicly available dataset that classify into the real and fake images. To detect the best spoofing attack models for the evaluation for the spoofing attack detection the Accuracy, F1-score and classification report. In this research the best model for the spoofing

attack detection is MobileNetV2 with the accuracy of 94%. The training accuracy and loss percentage of the model is very good compared to other models. In other different models the vgg16 performs well compared to the hybrid model, ResNet and CNN. In the conclusion to detect the spoofing attack for the real and fake images the MobileNetV2 is the best model for spoofing attack detection. In future the research performed on the large dataset and the work on the hybrid model to detect the spoofing attacks for live videos and images.

7 Acknowledgement

I would like to thank my supervisor, Dr. Catherine Mulwa, for his leadership throughout the project's execution. I'd want to thank him for his consistent oversight and help, which made the project's execution move more smoothly.

References

Abdullakutty, F., Elyan, E. & Johnston, P. (2021), 'A review of state-of-the-art in face presentation attack detection: From early development to advanced deep learning and multi-modal fusion methods', *Information fusion* **75**, 55–69.

Biggio, B., Russu, P., Didaci, L., Roli, F. et al. (2015), 'Adversarial biometric recognition: A review on biometric system security from the adversarial machine-learning perspective', *IEEE Signal Processing Magazine* **32**(5), 31–41.

Chapelle, O., Haffner, P. & Vapnik, V. N. (1999), 'Support vector machines for histogram-based image classification', *IEEE transactions on Neural Networks* **10**(5), 1055–1064.

Daniel, N. & Anitha, A. (2021), 'Texture and quality analysis for face spoofing detection', *Computers & Electrical Engineering* **94**, 107293.

de Souza, G. B., da Silva Santos, D. F., Pires, R. G., Marana, A. N. & Papa, J. P. (2019), 'Deep features extraction for robust fingerprint spoofing attack detection', *Journal of Artificial Intelligence and Soft Computing Research* **9**(1), 41–49.

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.

Hadid, A. (2014), Face biometrics under spoofing attacks: Vulnerabilities, countermeasures, open issues, and research directions, *in* 'Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops', pp. 113–118.

Kamiran, F. & Calders, T. (2012), 'Data preprocessing techniques for classification without discrimination', *Knowledge and information systems* **33**(1), 1–33.

Kumar, S., Singh, S. & Kumar, J. (2017), A comparative study on face spoofing attacks, *in* '2017 International Conference on Computing, Communication and Automation (ICCCA)', IEEE, pp. 1104–1108.

Li, L., Correia, P. L. & Hadid, A. (2018), 'Face recognition under spoofing attacks: countermeasures and research directions', *Iet Biometrics* **7**(1), 3–14.

Mansour, A. I. & Abu-Naser, S. S. (2022), 'Age and gender classification using deep learning-vgg16', *International Journal of Academic Information Systems Research (IJAISR)* **6**(7).

Nasir, J. A., Khan, O. S. & Varlamis, I. (2021), 'Fake news detection: A hybrid cnn-rnn based deep learning approach', *International Journal of Information Management Data Insights* **1**(1), 100007.

Nasiri, A., Yoder, J., Zhao, Y., Hawkins, S., Prado, M. & Gan, H. (2022), 'Pose estimation-based lameness recognition in broiler using cnn-lstm network', *Computers and Electronics in Agriculture* **197**, 106931.

Rokhana, R., Herulambang, W. & Indraswari, R. (2021), Multi-class image classification based on mobilenetv2 for detecting the proper use of face mask, *in* '2021 International Electronics Symposium (IES)', IEEE, pp. 636–641.

Rupapara, V., Rustam, F., Amaar, A., Washington, P. B., Lee, E. & Ashraf, I. (2021), 'Deepfake tweets classification using stacked bi-lstm and words embedding', *PeerJ Computer Science* **7**, e745.

Shibel, A. M., Ahmad, S. M. S., Musa, L. H. & Yahya, M. N. (2022), 'Deep learning detection of facial biometric presentation attack', *Life-Sciences* **8**(2), 01–18.

Toprak, I. & Toygar, Ö. (2021), 'Detection of spoofing attacks for ear biometrics through image quality assessment and deep learning', *Expert Systems with Applications* **172**, 114600.

Vujović, Ž. Đ. (2021), 'Classification model evaluation metrics', *International Journal of Advanced Computer Science and Applications* **12**(6), 599–606.