National College of Ireland

Face Spoofing Detection using Ensemble Classifier

MSc Internship
Cybersecurity

School of Computing
National College of Ireland

Supervisor: Dr. Imran Khan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: AJOMALE GBEMISOLA AYODEJI……

Student ID: 20188641……

Programme; ..Cybersecurity…… **Year:** …2021……..

Module: MSc Research Project…….

Supervisor: ……Imran Khan…… ……

Submission Due Date: …… 16th Dec, 2021 ……

Project Title: …Face spoof detection using ensemble classifier ……

Word Count: ……4520……..**Page Count**……20…… ……..

I hereby certify that the information contained in this (my submission) is information pertaining to the 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 project's rear.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. Using other authors' written or electronic work is illegal (plagiarism) and may result in disciplinary action.
I agree to an electronic copy of my thesis being made publicly available on NORMA, the National College of Ireland's Institutional Repository, for a consultation.

Signature: …… ……

Date: …… ……

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 the 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):	

Face Spoofing Detection using Ensemble Classifier

Abstract

In modern technology, face recognition system has received great attention. Several desktop, web and mobile applications make use of face recognition for security purpose. A major point of concern is the ability of the face recognition system to prevent an authorised person from having access to the application. Face spoofing through pictures and videos often threatens the system module of a face recognition system by disguising as a real image. A detection technique for fase spoofing attack must be such which could be relied on against different mode of attacks. A novel approach to detect spoofed images needs to be developed to reduce and eradicate the effects of spoofing. Several researchers have proposed detection techniques. Some of these past attempts have been reviewed in this paper. I propose in this study, an ensemble machine learning approach for detecting face spoofing. Random forest algorithm an ensemble learning and neural network were used for face spoofing detection. Neural network gave a better classification result.

Keywords: Random forest, Ensemble learning, Neural networks

1 Introduction

1.1 Background

Internet has brought a lot of comfort in the way day-to-day activities and processes are easily accomplished through internet enabled technological inventions like mails, virtual meetings, online shopping, e-registration etc. These processes often times have restricted access to ensure that only designated users have access to either the shared information or receives the sent information. Cases of Cyber attack is on the increase daily due to the dependence on Internet for our day-to-day activities. While some Hackers launch attacks on their targets majorly for financial gains others do so in order to cause a breach in trust between technology companies and their customers. Several organizations are heavly investing in cyber security to prevent information loss as a result of attacks from hackers. However as new technologies emerge, so do corresponding threats to such innovations. One of the emerging technology is Biometrics. This is a means of access control through identity validation either via thumbprint, iris and facial recognition. This technology has gained more popularity and acceptability in Information technology security, medicine, finance, criminal detection and investigation. In facial recognition, one of the major threat is facial spoofing. Facial spoofing refers to a process where a user's image is deceptively used to gain biometric access [1]. Hackers frequently use a phony face in front of the camera to get around a facial biometric system. The majority of facial recognition technologies are vulnerable to spoofing [2]. Facial biometrics works by recording different facial characteristics of a human being and then matches it with the facial information already stord in the database previously[3]. Spoofing attack has been on a significant rise because of the increase in biometrics technology. Several

researches have been initiated to tackle this menace. An adaptive transfer for tackling the spoofing problem was proposed by . [5] proposed the use of ROC curve to evaluate large scale anti-spoofing evaluation by performing a feature selection. The National Vulnerability Database of the National Institute of Standards and Technology in the United States has been revised to include the face spoofing attack.[6].

1.2 Importance

Face spoofing has overtime discouraged the acceptability of facial biometrics. New facial spoofing techniques spring up everytime even as anti-spoofing techniques are been discovered. It is of great value to the research world as different people have lost valuable information as a result of spoofing activities.

1.3 Research Question and Objective

This research is motivated to give answers to the following

- Can a face spoofing detection be designed?
- Can Ensemble machine learning help improve face spoofing detection?

A novel approach to answer the above questions is proposed. This proposed methodology makes use of the Random Forest and neural network for detecting facial spoofing

1.4 Limitation

The information technology improves daily with different online applications being created. Biometrics technology is one of the most adopted approach for login validation. This proposed approach is tested with a dataset of face spoofing activities.

1.5 Assumption

The machine learning model suggested in this literature was applied to the dataset of face spoofing records. I acknowledge that the dataset used is a secondary data. It is also assumed that at the time of downloading the dataset and compiling the report the values are believed to be real and correct.

1.5 Report Structure

The remaining part of this document is arranged in the following mode. A state of the art detailing past researches carried out by some scholars with the demerits and merits of their approached clearly outlined in section numer two. The third section details the research methodology while the fourth section contains the design specification. In section five, the project implementation is explained. The sixth chapter contains the evaluation and conclusion.

2 Related Work

Face spoofing attack is a topic of common interest in Cybersecurity because it is a threat to biometric technology. The state of art relating to spoofing detection and prevention will be reviewed.

[8] suggested a compact learning model for detecting facial spoofing. The authors proposed a double channel neural architecture for the exploitation of both deep and wide features in the detection of face spoofing. Convolutional Neural Network was adopted as the deep learning model for discriminative pattern of spoofing extraction. In their experiment, they discovered that employing shallower architectures produced better result than the deep neural model. [9]

proposed the use of VGG-Face Architecture for face spoof detection. In their, approach, they removed noise from the detected face, changed the color model of the image to CIELUV and YCbCr. The image was then made to go through the VGG-Face Architecture where face embeddings of each of the colour space was extracted. In [10] the authors adopted a Deep Convolutional Neural Network (DCNN) with mixed feature for Face Spoofing Detection. They divided the research into training and testing phase. In the training phase, the videos are trained using CNN after cropping out the faces in the videos and extracting the image features. At the testing phase, the model is tested using another set of video to evaluate the performance. In [11], Enhanced Deep Learning Architecures was proposed for Face Liveness Detection. They used two approaches. The first approach was a nonlinear anisotropic diffusion which relied on a splitting scheme called additive operator. This was used for preserving the boundary locations of the image by enhancing the edges and surface texture. The second approach was the application of a specialized convolutional neural network to identify the complex features needed for the face classification. They tested this model using Replay-Mobile and Replay-Attack dataset. The best classification result gotten was 96.03%. [12] used Relativity Representation on Rieannian Manifold for detecting face spoofing. To improve spoofing detection, they made use of an SVM which is sensitive to attack in Euclidean space. In [13] Support Vector machine and K Near Neighbors were the machine learning classification algorithm used for spoofing detection. Qualitative and Quantitative basis were used for evaluation. In [14], the researchers proposed the use of machine learning with colour features for detecting face spoofing. In their approach, spoofed face detection was done by converting the input face image into colour spaces. The three adopted colour spaces were RGB, HSV and YCbCr. To extract local texture information from the images, several feature vetors were used. They made use of over 13,000 samples for training and applied Support Vector Machine for classification. [15] proposed the combination of Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN) for face image depth estimation and rPPG signal of face video estimation. They utilized the frontalized feature maps as the RNN inputs supervised by the loss function of rPPG. In [16], faster region-based convolutional neural network with optimized roi-pooling feature fusion added with crystal loss function was proposed for detecting face spoofing. Their proposed model makes use of crystal loss and fusion method. Improved Retinex based LBP made use of an iterative guided filter for estimation of illumination. [17] proposed PipeNet architecture for multi-modal face anti-spoofing. The PipeNet is designed usin Limited Frame Vote module and Selective Modal Pipeline module. In [18], a multimodal multi-scale fusion method, that performs modality dependent feature re-weighting to select the more informative channel features while suppressing the less informative ones for each modality across different scales was proposed. In the research by [19], fully convolutional network(FCN) was proposed. FCN adopts the total use of face spoofing distortion properties such as repetetitive and ubiquitous. [20] proposed a two-stream convolutional network (TCNN) for detecting face spoofing for differentiating between legitimate and illegitimate pictures. The TCNN was applied to RGB space and multi-scale retinex space. They proposed an attention based fusion method to fuse the features from the two selected features. In [21] Convolutional Neural Network was used to properly countermeasure spoofing attacks. [23] applied deep transfer and neural network to detect attacks by face spoofing. They trained their model on the NUAA dataset using

VGG16. However, their model could only work on printed photographs and mobile photos.

The summary of existing literature is presented in detail in Table 1.

Table1. Existing Literature

Ref	Approach	Algorithm	Dataset	Limitations
8	Deep Learning for Face Spoofing Detection	CNN	ROSE-Youtu, SiW and NUAA	Low Detection accuracy, precision, and recall.
9	VGG-Face Architecture	SVC	NUAA photography imposter	Result was affected by inadequate illumination
10	Mixed Feature with Deep Convolutional Neural Networks	Deep CNN	Replay Attack Database	Accuracy achieved is 92%
11	Enhanced Deep Learning	Specialized CNN	Replay-Mobile and Replay-Attack	Achieved 96.03%
12	Machine Learning	SVM-classifier	CASIA-FASD, Replay-Attack, ULUNPU, SiW	low performance under the unseen-attack testing
13	Machine Learning	SVM and KNN	Extracted image datasets	The SVM, KNN algorithm shows 77.41% and 97.69% accuracy
14	Machine Learning	SVM	Extracted image samples	Improved SVM classification
15	Deep Learning	CNN-RNN	SiW	proposed method reduces the cross-testing errors on the Replay-Attack and CASIA-MFSD databases by 8.9% and 24.6% respectively
16	Deep Learning	R-CNN	CASIA-FASD, REPLAY-ATTACK and OULU-NPU	experiments of loss function show that Crystal Loss can improve the training effect
17	Deep Learning	CNN	CeFA	achieves the Average Classification Error Rate (ACER) of 2:21 1:26 on the test set.
18	Heuristic	Multi-modal	CASIA-SURF	the performance of ACER is reduced by 0:25%, 0:14% and 1:38% in Protocol 1, 2, and 3 respectively when using the proposed CASIA-SURF dataset as pre-training

19	Deep Learning	FCN	CASIA-FASD, Replay-Attack	With the help of small-sample external training data in the target domain, the FCN-DA-LSA further improves the performance and outperforms the existing methods.
20	Deep Learning	TCNN	CASIA-FASD, REPLAY-ATTACK and OULU	The experiments of fusion methods show that the attention model can achieve promising results on feature fusion.
21	Deep Learning	CNN	NUAA spoofing database	This technique outperformed the results of other state-of-the-art methods on NUAA dataset
23	Deep Learning	Deep Transfer Learning	NUAA	Performed well but could not detect mask and video attack

In conclusion, the reviews of these literatures shows that an improved classification algorithm needs to be applied to this field of research.

3 Research Methodology

Methodology refers to the pattern of methods applied in a specific are of research or study.

In the previous sections, the background of face spoofing prevention was discussed. Previous literatures on preventive and detective measures were also reviewed. In this section, the methodological approach adopted in this research will be explained.

3.1 Data Processing

Sourcing for a reliable dataset is vital in machine learning. The quality of data used for learning and testing contributes a lot to the reliability of the result. Several open source websites were browsed for face spoofing datasets. The adopted website for data gathering was Kaggle. Kaggle is an open source data repository with datasets freely available for data analysis. The dataset used was then preprocessed.

3.1.1 Data Preprocessing

After the source of data for machine learning has been decided, the nxt step is the preprocessing steps to follow. The data for this research was downloaded from Kaggle.

Python programming language was adopted for this research. There are predefined libraies in python used for data preprocesing. The python libraries used are:

-**Numpy:** Numpy is used for performing scientific calculcations, large multidimensional arrays and matrices.

-Pandas: Pandas is used for manipulating and analyzing data. To import the dataset into the program, pandas is needed.

-Matplotlib: To create visual representation of data in 2D, the matplotlib library was used.

The next step is to indentify missing values and delete them. Data splitting is also done to divide the data into training and testing.

Data preprocessing

3.1.2 Training and Testing Data

In machine learning, training data refers to the dataset used to train a machine learning algorithm so as to produce the proposed outcome. Training data helps the program to have a clear understanding on how the technology will be applied.

3.2 Ensemble Learning

In machine learning, ensemble learning is the combination of different predictions gotten from several learning models to deduce a better model with a much more reliable prediction. Ensemble learning is used for learning based generalization of training data such that predicitons wll be carried out on unkown data. Ono of the advantages of ensemble is the ability to accurately combine models that are weak to produce a robust and accurate model thereby achieving a better performance. Ensemble learning model could be classified into three;

- **Stacking** – Stacking in ensemble learning is a process whereby the predictions gottten from each model are all combined together and supplied as an input to the last estimator. The estimator then computes the final prediction

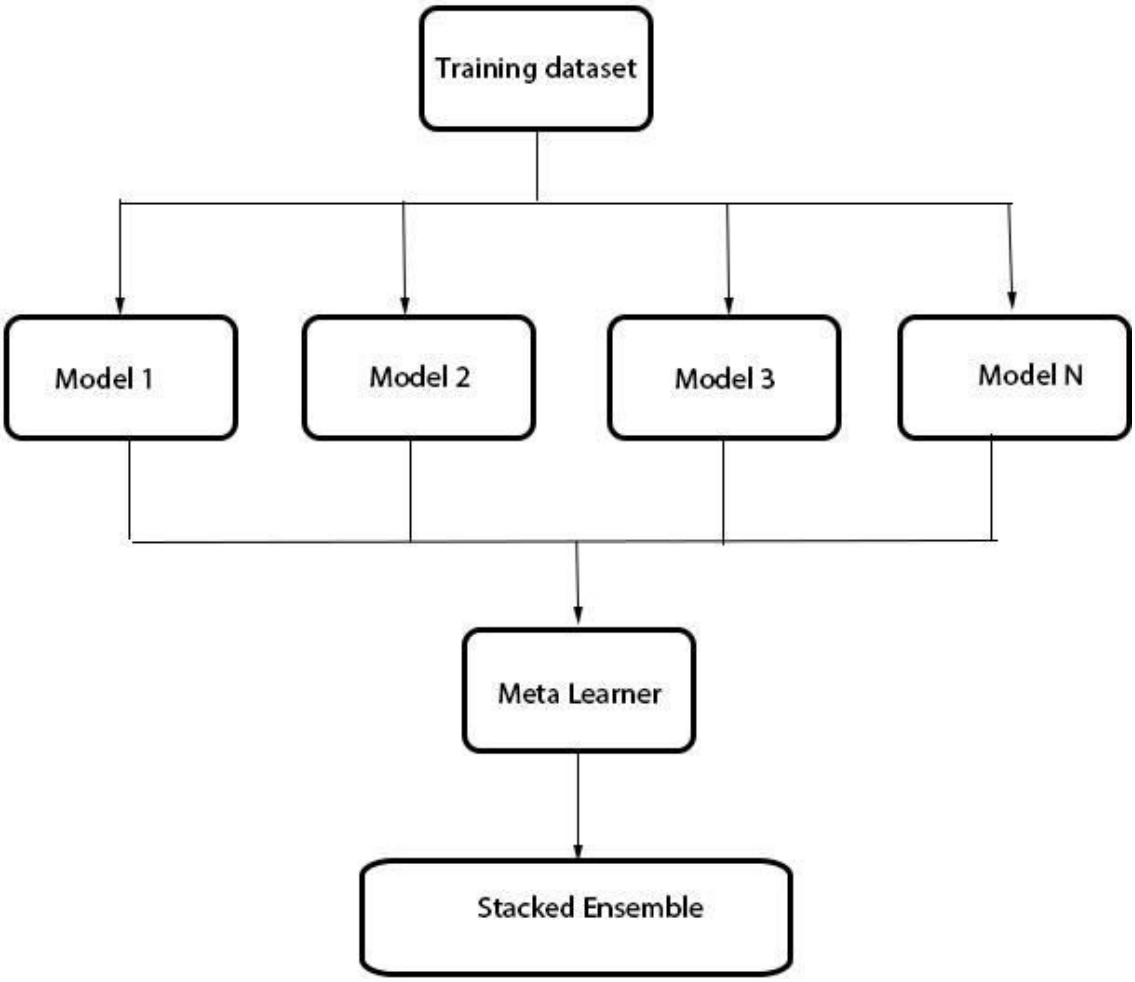

Fig 1 Stacking in ensemble classifier

- **Boosting**- Boosting produces a stronger classifier from weak ones by first making use of the training data to build a model and then creating another model which aims at correcting errors gotten from the first model built.

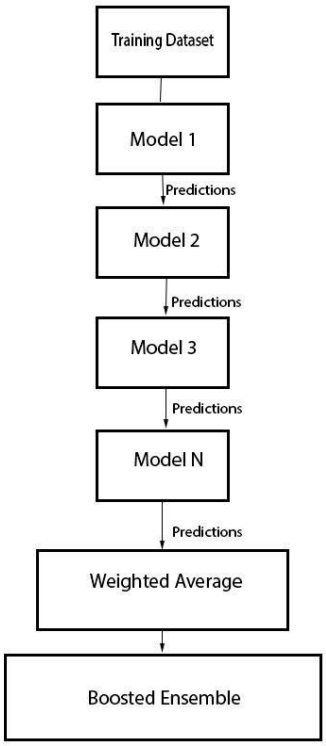

Fig 2 Boosting in Ensemble classifier

- **Bagging –** Bagging decreases the prediction variance through the additional generation of training data from the given datasets using repetitive combinations to produce several sets of the original dataset.

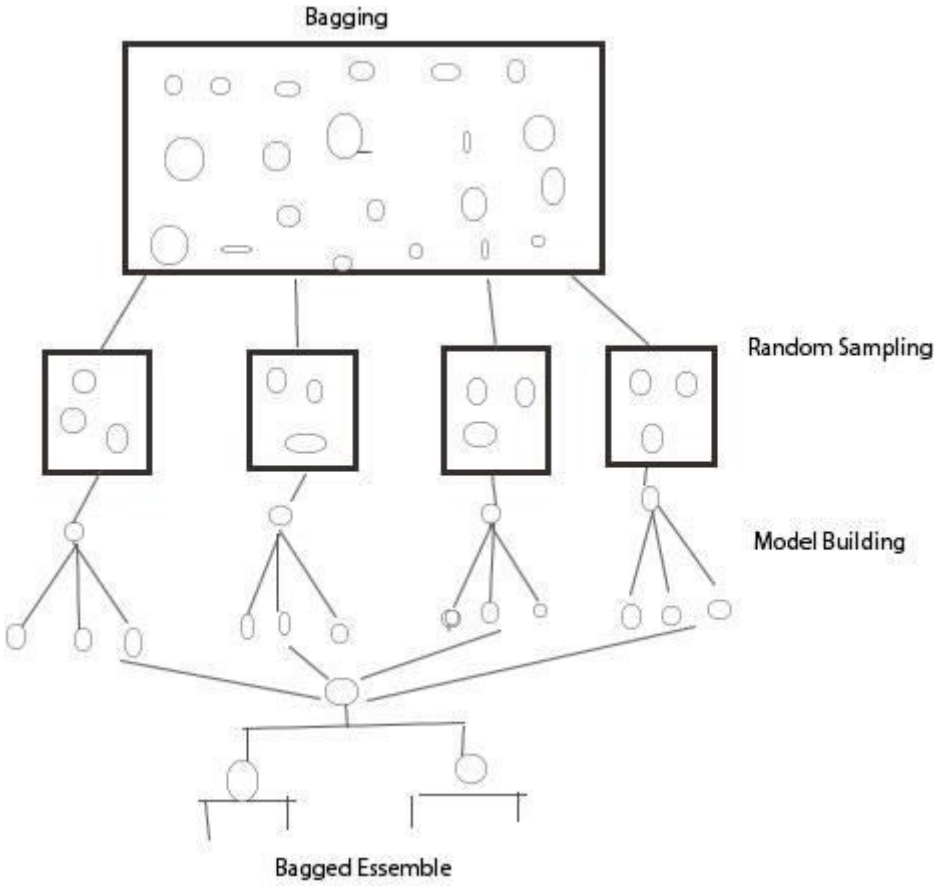

Fig 3 Bagging in ensemble classifier

3.3 Random Forest Algorithm

Random forest algorithm is a model in artificial intelligence used for solving classification and regression problems. It is an ensemble learning algorithm which defines its operation by constructing several decision trees duing training. During classification in random forest, the class selected by majority of the trees is the output produced.

3.4 Neural Network

Neural network is a deep learning algorithm that seeks to recognize relationship that exist in a datset by mimicking the pattern in which the human brain works. This is done by creating neurons which serve as channels for moving information from input state to an output.

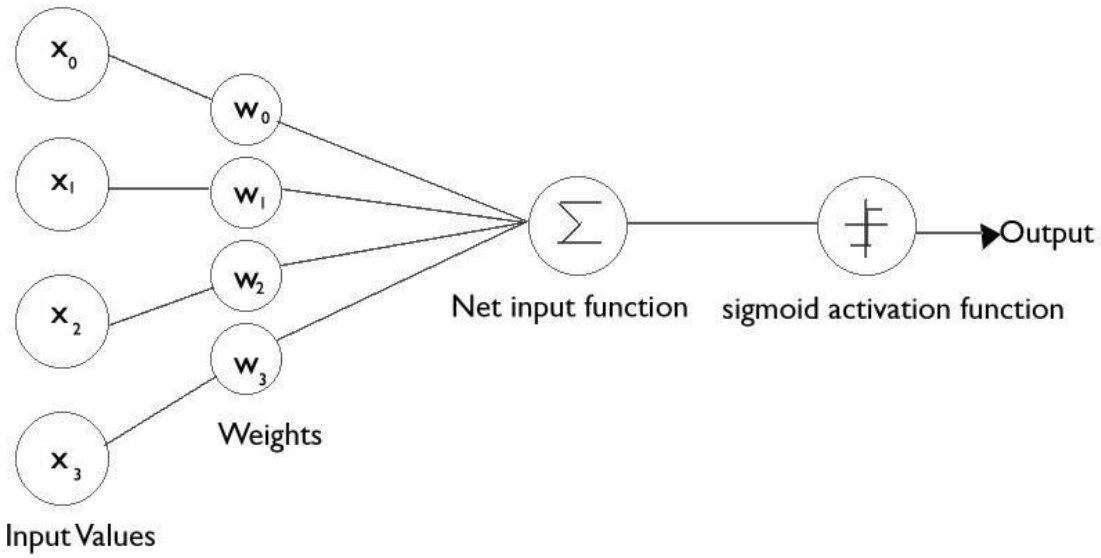

Fig 4 Neural network forward propagation

3.5 Evaluation Methodology

Model evaluation refers to the assessment of the performance of a machine learning model. This helps to determine to what degree, the model can be adopted. The evaluation starts with the output of the accuracy level, Precision, recall and F1-score. F1-score measures the test's accuracy by considering the precision and recall score.

3.5.1 Precision

The formula for calculating precision is given as :
Precision = tp / (tp + fp)
where:
tp is True Positive
fp is false positive

3.5.2 Recall

The formula for Recall is given as
tp / (tp + fn)
where:
tp is the number of true positives and
fn is the number of false negatives

3.5.3 F1 Score

Formula for calculating F1 Score is given as .
F1= 2 * (precision * recall) / (precision + recall).

4 Design Specification

In this section, the model design specification will be described. The steps and process flow are described using the flowchart below.

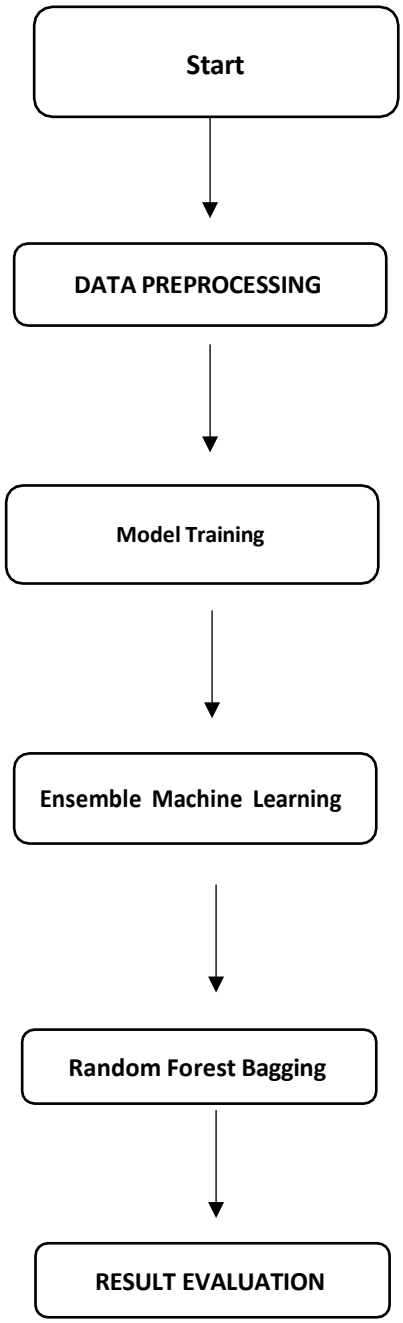

Fig 5 Design specification flowchart

The dataset is imported into the program using the pandas library. The shutil library is used for performing operation on the files. For computer vision algorithms, keras models such as sequential, Dense, Dropout, maxpooling2D, Conv2D and Flatten is imported. The dataset is then split into training and testing in ratio 8:2. The epoch is then set for the training dataset. The output is then evaluated using the F1, Recall and precision metrics

5 Implementation

In this section, the adopted approach for the implementation of this research method is explained.

5.1 Python

Python programming language is a high-level language built with non-static semantics. It is used in different range of fields such as data science, software prototyping and development, web development and so on. It offers powerful capability such as readable and concise code. While machine learning is backed up with versatile workflows and complex algorithms, python makes it easy for developers to produce models that are reliable without focusing on the technicality behind the language. Python is also reach in frameworks and libraries which reduces development time. Another advantage of python is that it is that it is platform independent.

5.2 Pycharm

PyCharm is an Integrated Development Environment dedicated for writing python code. It is specifically built to create an easy environment for python developers. It is available in community, professional and education editions. It has a friendly user interface with features for easy navigation, running, debugging and upgrading code constructs. Pycharm community edition was used in this project.

5.3 Libraries

Libraries refer to related built-in modules which could be repeatedly used in different programs.

- **Tensorflow:** Tensorflow is a library used for data flow graph computation in python.
- **Scikit-learn:** Scikit-learn is a python library for performing statistical modeling such as clustering, regression, classification and reduction of dimensions.
- **Keras:** This is the library sued for optimizing, normalization and application of activation functions.

6.0 Evaluation

In this section, the efficiency and effectiveness of this model is evaluated using Accuracy, F1-Score and Precision. I carried out this research using dataset of Face Anti-spoofing containing real and fake face detection. The dataset was gotten from Kaggle. In this research, our aim is to compare the performance of more than one machine learning hence the reason for ensemble learning approach. I have used Random Forest and Neural Network for the implementation of this research. I evaluated the result gotten from these two machine learning algorithms.

6.1 Accuracy

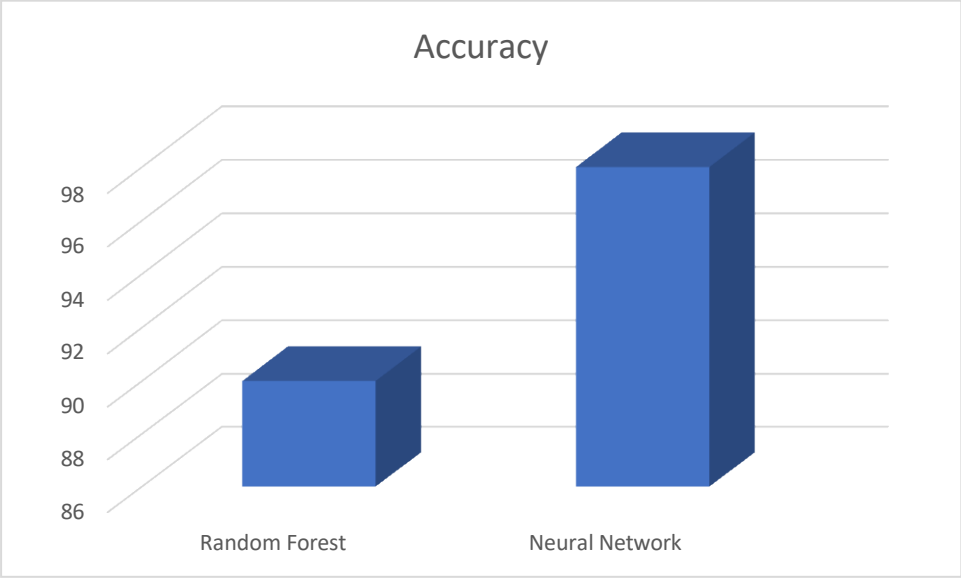

Fig 6 Accuracy of the two machine learning Model

In machine learning, accuracy measurement metrics is used to determine of all models applied, which one gave the best identification relationship. After training and testing 98% was recorded for neural network while 90% was recorded for random forest.

6.2 F1-score

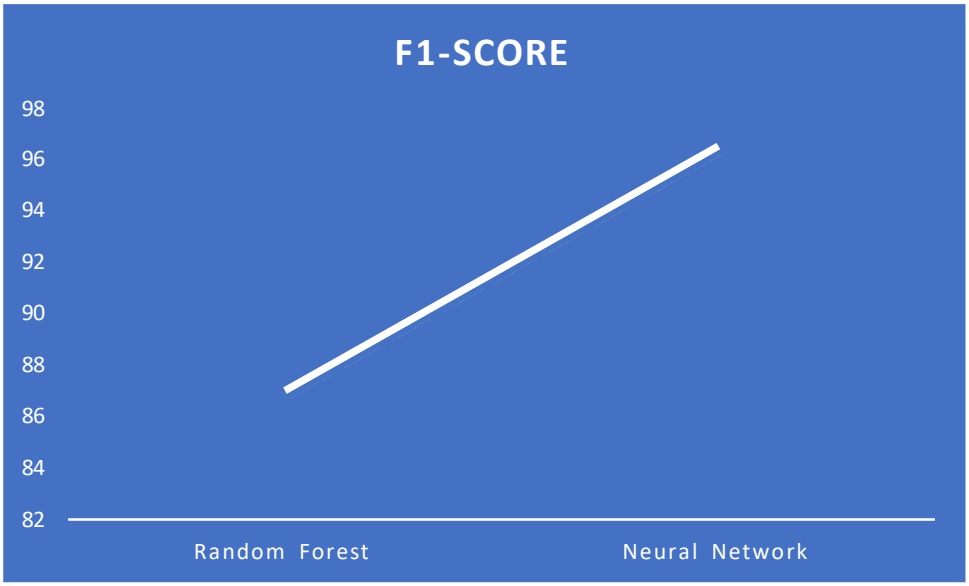

Fig 7 F1-Score of the two machine learning model

In machine learning, F1-Score is mainly calculated when there is a need to compare the result of two different classifiers. 96.5% was recorded for neural network while 87% was recorded for random forest.

6.3 Recall

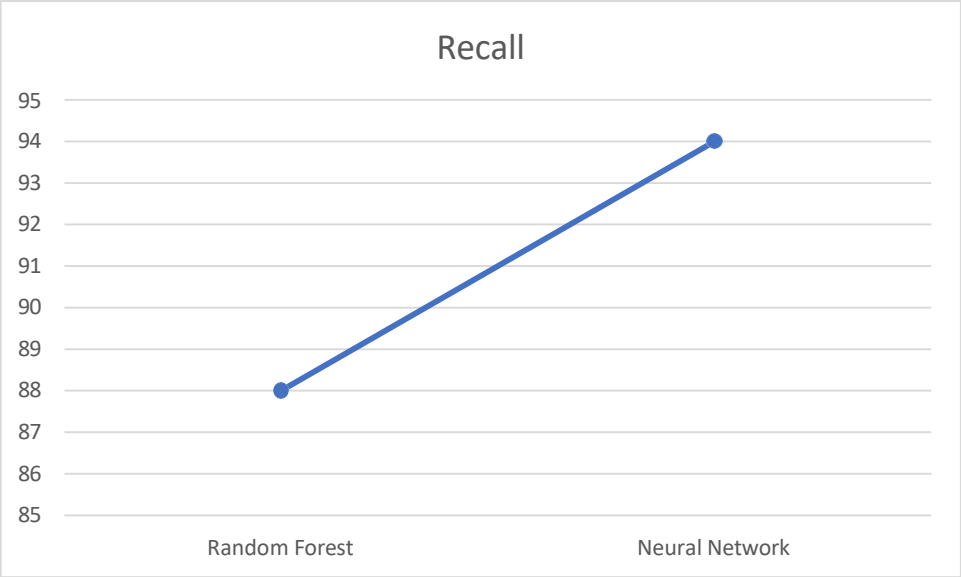

Fig 8 Recall of the two machine learning model

Recall in machine learning refers to the number of true positives found. 94% was recorded for neural network against 88% for random forest.

7 Discussion

Ensemble is a machine learning approach targeted towards improved and effective predictive and identification performance through the utilization of more than one machine learning model. It gives a high probability of accuracy improvement when compared to the use of a single model. The three ensemble classes are bagging, boosting and stacking. The bagging enables the incorporation of all possible outcomes while also randomizing them. Boosting also improves on the prediction of the bagging. Stacking completes the steps by enabling the ensemble to measure error rate. I have identified that face spoofing requires a reliable predictive model hence the proposed approach of combining more than one model. In this research, we selected random forest due to its bagging and boosting properties. We also trained the dataset using neural network. The result gotten with the two machine learning algorithms were compared. Neural network gave a classification accuracy of 98% while Random Forest gave a classification accuracy of 90%. Neural network gave an F1-Score of 96.5% while Random Forest gave F1-score of 87%. For Recall, Neural network gave 94% while Random Forest gave 88%. The novelty approach of this research is in the approach adopted which helps to reduce variance. This was achieved by ensuring that the epoch of the entire training the dataset was maintained at 100 to prevent overfitting and underfitting. This approach is an improvement to the reviewed literatures because it ensured that the training process does not overfit and our classification result also improved.

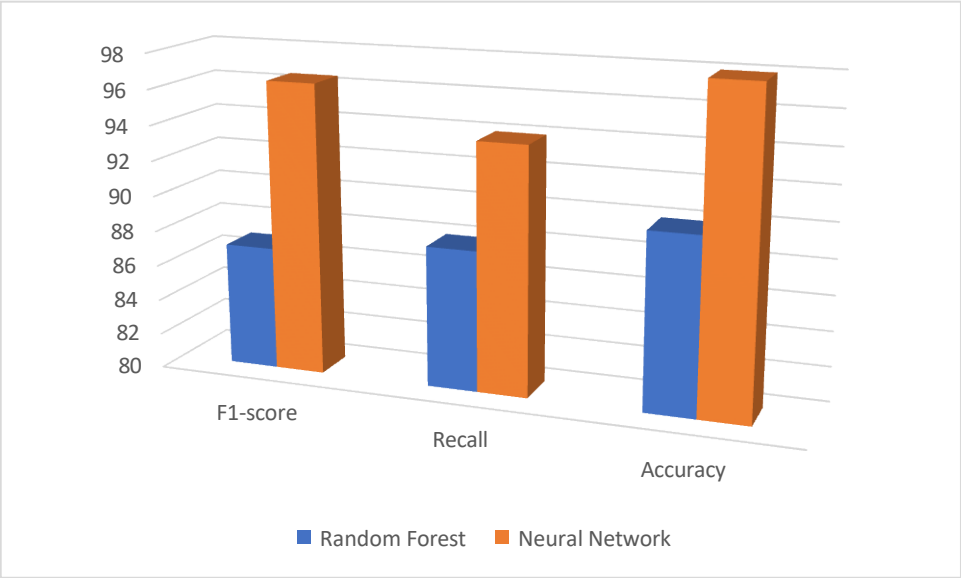

Fig 9. Comparison of Random forest with Neural network

8 Conclusion and Future work

The rate of discovery of new technological strides cannot be underestimated. This discovery also leads to new cyber-attack modes. As more applications adopt biometrics for user access control, so do fraudsters develop more strategies to defeat this security systems. Different methods have been proposed to reduce and mitigate this menace. However, these approaches have not been sufficient to reduce spoofing attacks. I have introduced ensemble machine learning as a method of detecting face spoofing attacks because of its combination of different machine learning models. The algorithms used is random forest and neural network. Neural network gave a better classification and shows to be a better fit for image classification. In this paper, emphasis have been laid on images, future research should focus more on approaches that can auto detect live videos.

References

1. Zhang, M., Zeng, K. and Wang, J., 2020. A Survey on Face Anti-Spoofing Algorithms. Journal of Information Hiding and Privacy Protection, 2(1), pp.21-34.
2. Boulkenafet, Z., Komulainen, J. and Hadid, A., 2016. Face Spoofing Detection Using Colour Texture Analysis. IEEE Transactions on Information Forensics and Security, 11(8), pp.1818-1830.https://www.researchgate.net/publication/301571761.
3. Pujol, F., Pujol, M., Rizo-Maestre, C. and Pujol, M., 2019. Entropy-Based Face Recognition and Spoof Detection for Security Applications. Sustainability, 12(1), p.85.

4. Quan, R., Wu, Y., Yu, X. and Yang, Y., 2021. Progressive Transfer Learning for Face Anti-Spoofing. IEEE Transactions on Image Processing, 30, pp.3946-3955.
5. Zhang, S., Liu, A., Wan, J., Liang, Y., Guo, G., Escalera, S., Escalante, H. and Li, S., 2020. CASIA-SURF: A Large-Scale Multi-Modal Benchmark for Face Anti-Spoofing. IEEE Transactions on Biometrics, Behavior, and Identity Science, 2(2), pp.182-193.
6. Määttä, J., Hadid, A. and Pietikäinen, M., 2012. Face spoofing detection from single images using texture and local shape analysis. IET Biometrics, 1(1), p.3.
7. Qin, Y., Zhao, C., Zhu, X., Wang, Z., Yu, Z., Fu, T., Zhou, F., Shi, J. and Lei, Z., 2020. Learning Meta Model for Zero- and Few-Shot Face Anti-Spoofing. Proceedings of the AAAI Conference on Artificial Intelligence, 34(07), pp.11916-11923.
8. Hashemifard, S. and Akbari, M. 2021. A Compact Deep Learning Model for Face Spoofing Detection. arXiv preprint arXiv:2101.04756.
9. Balamurali, K., Chandru, S., Razvi, M. and Sathiesh Kumar, V., 2021. Face Spoof Detection Using VGG-Face Architecture. Journal of Physics: Conference Series, 1917(1), p.012010.
10. Jesslin Melba N V, P. U., Blessy J 2020.Face Spoofing Detection using Mixed Feature with Deep Convolutional Neural Networks. International Journal of Recent Technology and Engineering (IJRTE), 8.
11. Koshy, R. and Mahmood, A., 2020. Enhanced Deep Learning Architectures for Face Liveness Detection for Static and Video Sequences. Entropy, 22(10), p.1186.
12. Yao, C., Jia, Y., Di, H. and Wu, Y., 2020. Face Spoofing Detection Using Relativity Representation on Riemannian Manifold. IEEE Transactions on Information Forensics and Security, 15, pp.3683-3693.
13. Sanjay Ganorkar S. R., Gaurav R., 2019. Face Liveness Detection Using Machine Learning INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, 8, ISSUE 09, SEPTEMBER 2019
14. Mahitha. M.H 2018. Face Spoof Detection Using Machine Learning with Colour Features. International Research Journal of Engineering and Technology (IRJET), 5.
15. Liu, Y., Jourabloo, A. and Liu, X., 2021. "Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision.
16. Chen, H., Chen, Y., Tian, X. and Jiang, R., 2019. A Cascade Face Spoofing Detector Based on Face Anti-Spoofing R-CNN and Improved Retinex LBP. IEEE Access, 7, pp.170116-170133.
17. Yang, Q., Zhu, X., Kae Fwu, J., Ye, Y., You1and, G. and Zhu, Y., 2020. "PipeNet: Selective Modal Pipeline of Fusion Network for Multi-Modal Face Anti-Spoofing"arXiv:2004.11744v1 [cs.CV].
18. Zhang, S., Liu, A., Wan, J., Liang, Y., Guo, G., Escalera, S., Escalante, H. and Li, S., 2020. CASIA-SURF: A Large-Scale Multi-Modal Benchmark for Face Anti-Spoofing. IEEE Transactions on Biometrics, Behavior, and Identity Science, 2(2), pp.182-193.
19. Sun, W., Song, Y., Zhao, H. and Jin, Z., 2020. A Face Spoofing Detection Method Based on Domain Adaptation and Lossless Size Adaptation. IEEE Access, 8, pp.66553-66563.
20. Chen, H., Hu, G., Lei, Z., Chen, Y., Robertson, N. and Li, S., 2021. Attention-Based Two-Stream Convolutional Networks for Face Spoofing Detection. IEEE

Transactions on Information Forensics and Security. https://doi.org/10.1109/TIFS.2019.2922241

21. Grover, K. and Mehra, D., 2019. Face Spoofing Detection using Enhanced Local Binary Pattern. International Journal of Engineering and Advanced Technology, 9(2), pp.3365-3371.
22. Vishnu, K., Raut, R. and Thakar, V., 2017. Effective Methodology for Detecting and Preventing face Spoofing Attacks". International Journal of Advance Research in Science and Engineering, 06(06).
23. Dr. Yogesh Kumar Sharma, Ms. Sujata Pandurang Patil, Dr Ranjit D, Patil "Deep Transfer Learning for Face Spoofing Detection" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 22, Issue 5, Ser. III (Sep. – Oct. 2020), PP 16-20 www.iosrjournals.org