iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** II **Month of publication:** February 2022

DOI: https://doi.org/10.22214/ijraset.2022.40452

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue II Feb 2022- Available at www.ijraset.com

Hybrid Algorithm for Face Spoof Detection

Abhishek Mittal[1], Pravneet Kaur[2], Dr. Ashish Oberoi[3]
[1]*(Research Scholar M.Tech, Department of CSE, RIMT University, Mandi Gobindgarh, Punjab, India)*
[2]*(Assistant Professor, Department of CSE, RIMT University, Mandi Gobindgarh, Punjab, India)*
[3]*(Professor, Department of CSE, RIMT University, Mandi Gobindgarh, Punjab, India)*

Abstract: ***The face spoof detection is the approach which can detect spoofed face. The face spoof detection methods has various phases which include pre-processing, feature extraction and classification. The classification algorithm can classify into two classes which are spoofed or not spoofed. The KNN approach is used previously with the GLCM algorithm for the face spoof detection which give low accuracy. In this research work, the hybrid classification method is proposed which is the combination of random forest, k nearest neighbour and SVM Classifiers. The simulation outcomes depict that the introduced method performs more efficiently in comparison with the conventional techniques with regard to accuracy.***
Keywords: Face Spoof, KNN, Hybrid Classifier, GLCM

I. INTRODUCTION

With the maturation of computer vision technology and the advancement of GPU-based computing platforms, the development of person recognition methodologies gradually moves its target towards practice-oriented applications. The popularity of the application of biometric identification methods for example fingerprint, iris, finger vein, etc., has touched new heights in the last few decades. Notably, face biometrics takes advantage of its security and convenience to be comprehensively used in diverse fields and is integrated at various stages [1], e.g., login, authentication and payment, which are closely associated with individual strategic interests. However, with the development of social networks it becomes easier to get pictures or videos of any person making it possible to spoof the face authentication system. These behaviours are equally termed as face spoofing attacks. And they include three modes: face photo attack, replay attack, and 3D mask attack. Face spoofing attacks limit the application of face recognition system as well as increase its susceptibility with respect to security concerns. This brings about one of the daunting issues: given an image or video captured with a camera that contains human faces, how to extract different features and how to differentiate live faces and spoofing face effectively in a fruitful manner [2].

A. General Process of Face Recognition or Classification

Face liveliness detection, also termed as face spoofing detection, is designed to protect against a variety of spoofing attacks. Before the face recognition process begins, face liveness detection determines whether the image is taken of a real or simulated subject. Suspicious images are filtered and will not be sent to the recognition system. Figure 1presents a generic face recognition/classification system [3].

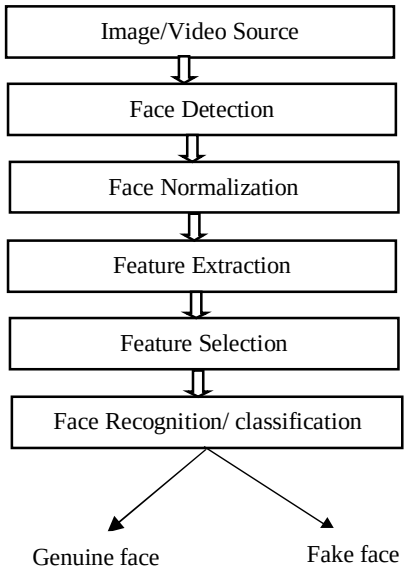


Figure 1: General Face Recognition Model

The face recognition model consists of following steps:

1) *Image/video Source:* In the initial stage, face detection is performed in the received image independent of scale and space [4]. An advanced filtering process is applied using precision classifiers to isolate the locations where faces are exposed and filtered. All translation, scaling and rotational transitions occur in the face detection phase. For example, changes in facial expressions and hairstyle or faces with smiling and frowns are considered significant changes in the pattern recognition stage.
2) *Face Detection:* Under this process certain patterns are detected within the image for face detection. It is a scheme in which the locations and sizes of human faces in arbitrary images are verified. Facial recognition may or may not include face detection [5].
3) *Face Normalization:* In the detected face, different images of the same person may vary in terms of rotation, brightness, and size. Those properties do not depend on facial features and have a substantial effect on detection rates. Normalization of detected faces is the only technique to deal with this problem. Its main objective is to reduce the impact of insufficient and unnecessary information to improve the recognition process. The centre points of the eyes are positioned to select the basic feature points to normalize the face.
4) *Feature Extraction:* This stage involves extracting thecrucial information from the image of a face. During this operation, dimensions are reduced, relevant features are extracted and the most optimum features are chosen [6]. The output of feature extraction is the low dimensionality, transformation of the data, and the selection of the appropriate subspace in the original feature space.
5) *Feature Selection:* This stage aims at selecting the subsets of extracted features to reduce classification error. There are many existing feature extraction methods like Principal Component Analysis, Kernel PCA etc.
6) *Face Recognition/ Classification:* The extracted properties are used to recognize the face. It depends on the user application. The photograph provided for the subject is compared with all the biometric templates that are stored on the database to be recognized [7]. In case of its implementation for verification purpose, the biometric template of the claimed identity is recovered and compared with the given image.

B. Face Spoof Detection Techniques

Based on the different types of cues used in face spoof detection, the taxonomy of published methods includes four main types: (i) motion-based methods, (iii) texture-based methods, (iii) methods based on image quality analysis, and (iv) depth-based methods.

The detailed description of all these methods is given below:

1) *Motion-Based Methods:* The operation of these methods is inspired by the notion that images of authentic and fraudulent faces have specific motion patterns. Different from genuine human faces (3D objects), 2D faces showvarious motion patterns like blinking of eyes, moment of lips, rotation of head. Optical flow can be adopted to derive the information of liveliness. In such methods, the researchers try to take advantage of frames instead of still photographs to analyze face spoofing detection.For example, eye-blink detection has been used to detect the liveliness of a face. However, the motion-based methods have certain limitations [8]. Human physical rhythm that ranges from 0.2 to 0.5 Hz sets a limit on the frequency of facial movements. As a result, the time (typically >3s) to assemble continuous vitality features is relatively long for face liveliness detection. Apart from this, other movements (such as background movement) that are irrelevant to facial liveliness or replayed motion in video attacks can easily interrupt or confuse motion-basedtechniques.
2) *Image Quality Analysis-Based Methods:* Image quality-based methods primarily use the difference between image distortion and reflection features to differentiate between genuine and fake faces. These methos apply Color space analysis to detect the degradation of image quality due to spoofing means. This degradation can be found in spoofing facial photographs, printed photographs and replayed videos displayed on a monitor. Therefore, the extraction of chromatic moment features is performed using the analysis of image quality-based schemes to separate the live face photograph from the spoofed photograph of the face. In these methods, the whole image is deployed to evaluate the image quality due to their good generalization ability. But image quality can be more discriminatory in smaller and localized areas of facial images [9].

3) *Texture-Based Methods:* These methods assume that the use of multiple spoofing mediums results in different surface reflectance and shape distortion, leading to a difference in texture between live and spoofed facial images. Texture-based methods extract image artifacts in spoof face images to counter both the printed photo and replayed video attacks. Comparted to motion-based methods, texture-based methods require only one image to detect the spoof. Nevertheless, a good generalization ability for a range of facial expressions, posture and spoofing methods is required when collecting training data from a few subjects under constrained circumstances [10]. Thus, the texture features are combined with the image quality features. Consequently, the performance of face spoof detection goes better. The two popular techniques in this category are described as follow:

a) *LBP:* Various texture descriptors are applied to detect face spoofing; However, first preference is given to LBP. It is a grayscale illumination-invariant texture coding method in which each pixel is assigned a label after comparing it with its neighbours and the result is rendered in a binary number. All parameters of a local binary pattern exist in terms of number of neighbours, neighbourhood scope, and coding strategy. After that, the final computed label is organized in the histogram to determine the texture of the entire image or even image path.

b) *Histograms of oriented gradients (HOG):* This is another texture descriptor in which variations in gradient orientation are depicted in different parts of the image in an illumination-invariant style [11]. The magnitude of gradients in different orientations is expressed in cells that are subsequently integrated into blocks. Finally, bins, cells, and blocks are normalized to compile the final feature vector.

4) *Depth-Based Methods:* In these techniques detailed information about the face is estimated for the discrimination of a live three-dimensional face from a spoofing face that is presented on 2D planar media. These technologies include defocusing technology, NIR sensors and light field cameras. The depth attribute is used to effectively detect printed photo and video replay attacks. In contrast, 3D depth analysis procedures have been designed to estimate facial 3D depth information in some studies [12]. An approach based on optical flow field has been suggested for the analysis of the difference in optical flow field between a planar object and a 3D face. Another study deployed geometric invariants based on a set of facial landmarks to detect replay attacks. But, depth-based techniques require multiple frames or depth measuring equipment to estimate depth information, which can result in increased system costs.

II. LITERATURE REVIEW

A. *Face Spoof Detection using Deep Learning*

Polash Kumar Das, et.al (2019) suggested an approach in which the handcrafted attributes were integrated with DNN (deep neural network) attributes for constructing the discriminant face spoofing detection [13]. LBP (Local Binary Patterns) descriptor was implemented to analyze the information related to attributes from the brightness and the chrominance channels. A technique planned on the basis of pre-trained CNN (convolutional neural network) called VGG-16 was put forward via static features for recognizing the video and printed 2D photo attacks. The suggested approach was effective for recognizing the real and spoofed images feature.

Xun Zhu, et.al (2021) focused on developing and training a CEM-RCNN (Contour Enhanced Mask- Region-based Convolution Neural Network) algorithm in order to detect the face spoofing [14]. This algorithm employed the contour objectness for detecting the SMCs (spoofing medium contours). The experimental outcomes indicted that the developed algorithm was suitable to recognize the face images having SMCs and more efficient in contrast to the existing techniques.

Abdulkadir Şengür, et.al (2018) introduced a mechanism on the basis of TL (transfer learning) for which pre-trained CNN (convolutional neural network) model was deployed [15]. This mechanism emphasized on investigating diverse deep attributes and comparing them on a common ground while detecting face liveness in videos. NUAA and CASIA-FASD datasets were applied in the experimentation. The results of experiments demonstrated that the introduced mechanism had generated optimal outcomes as compared to other schemes. Shilpa Garg, et.al (2020) formulated a robust and effectual method named DeBNet with the objective of detecting face liveness [16]. The multilayer deep network was exploited to attain effective outcomes for diverse percentage of training set of images. The deep attributes were extracted and the face images were classified as real and spoofed using this method. An analysis was conducted on NUAA data set of images. The experimental results exhibited that the formulated method offered the accuracy of 99% for detecting the face liveness and HTER value of 0.31 on the utilized dataset.

Abdelrahamn Ashraf Mohamed, et.al (2021) investigated a DL (deep learning) method known as sequential CNN (convolution Neural Network) which had two phases such to extract the features and to classify the images [17]. The CelebA-Spoof 2020 dataset was executed to perform the experiments for identifying the faces as real and spoofed. The accuracy was considered to determine the investigated method. The investigated method was capable of attaining the accuracy up to87% and area under ROC curve around 0.535.

Comparison Table

Author	Year	Technique Used	Findings	Limitations
Polash Kumar Das, et.al	2019	An approach based on pre-trained convolutional neural network VGG-16 model	The suggested approach was effective for recognizing the real and spoofed images feature.	This approach attained lower efficiency on diverse datasets of large size.
Xun Zhu, et.al	2021	CEM-RCNN (Contour Enhanced Mask-Region-based Convolution Neural Network) model	The experimental outcomes indicted that the developed algorithm was suitable to recognize the face images having SMCs and more efficient in contrast to the existing techniques.	The developed algorithm was ineffective for detecting the SMCs of some fine-grained presentation attacks.
Abdulkadir Şengür, et.al	2018	Transfer learning and CNN (convolutional neural network)	The results of experiments demonstrated that the introduced mechanism had generated optimal outcomes as compared to other schemes.	The face presentation attack was not detected accurately using this mechanism.
Shilpa Garg, et.al	2020	A robust and efficient technique named DeBNet	The formulated method offered the accuracy of 99% for detecting the face liveness.	The DL algorithm was utilized to extract the attributes which consumed much time.
Abdelrahamn Ashraf Mohamed, et.al	2021	Sequential CNN (convolution Neural Network)	The investigated method was capable of attaining the accuracy up to87% and area under ROC curve around 0.535.	The face spoofing was not detected from videos using the investigated method.

B. Face Spoof Detection using Hybrid Technique

Wenyun Sun, et.al (2020) established an FCN-DA-LSA (Fully Convolutional Network with Domain Adaptation and Lossless Size Adaptation) technique for detecting the face spoofing [18]. A LSA pre-processor and FCN based pixel-level classification algorithm, whose embedding was done with a DA layer, were comprised in this technique. The FCN (Fully Convolutional Network) algorithm aimed to deploy the basic properties of face spoof distortion. The generalization was enhanced across diverse domains via DA (domain adaptation). LSA was applied for preserving high-frequent spoof clues occurred due to the face recapturing procedure. The results depicted the supremacy of the established technique over the traditional methods for detecting the face spoofing.

Raden Budiarto Hadiprakoso, et.al (2020) projected a combined technique detecting face liveness and CNN (Convolutional Neural Network) classification algorithm [19]. Two modules namely blinking eye module to compute eye openness and lip movement, and the CCN classification module were involved in this technique. A public dataset was exploited to train the projected technique. A simple facial recognition application made the deployment of this integrated technique on Android platform. According to results, the projected technique was adaptable for recognizing several facial spoof attacks.

Junqin He, et.al (2019) intended a methodology on the basis of integrating distinct color space models [20]. This methodology concentrated on converting the colored image into YCbCr and Luv color space model so that attributes of LBP (Local Binary Patterns) were extracted and transforming the RGB image into HSV color space model with the objective of extracting CM (Color Moment) features later on.

At last, the extracted features were cascaded into SVM (Support Vector Machine) in order to classify the decision. Replay-Attack and CASIA-FASD datasets were utilized to compare the intended methodology against the traditional techniques. The experimental outcomes revealed the superiority of the intended methodology and its discrimination ability was found greater.

Xiaofeng Qu, et.al (2019) designed a shallow CNN-LE (shallow convolutional neural network with laplacian embedding) to detect the face spoofing [22]. The face liveness was detected through diverse attributes in accurate way. Initially, four layers were comprised in the shallow CNN that led to enhance its speed. The DT-CWT (dual tree-complex wavelet transform) was assisted in extracting the dynamic texture features. Subsequently, the designed model employed these features which were integrated with the depth features. Eventually, LE was adopted for maintaining the inter-class discrimination and penalizing the distance of intra-class. The designed model attained more discriminative attributes when it was embedded with laplacian loss with the softmax loss. These attributes were useful for detect face anti-spoofing. The CASIA FASD, Replay attack and MSU USSA databases were applied to carry out the experiments. The experimental results confirmed that the designed model performed more successfully in contrast to others while detecting face anti-spoofing.

Comparison Table

Author	Year	Technique Used	Findings	Limitations
Wenyun Sun, et.al	2020	Fully Convolutional Network with Domain Adaptation and Lossless Size Adaptation (FCN-DA-LSA)	The results depicted the supremacy of the established technique over the traditional methods for detecting the face spoofing.	This technique had an issue related to the external data.
Raden BudiartoHadiprakoso, et.al	2020	a combined method of face liveness detection and CNN (Convolutional Neural Network) classifier	According to results, the projected technique was adaptable for recognizing several facial spoof attacks.	This technique consumed much time to recognize the face.
Junqin He, et.al	2019	A method based on the combination of different color space models	The experimental outcomes revealed the superiority of the intended methodology and its discrimination ability was found greater.	This technique provided lower accuracy in case of actual scene having more influencing factors such as dramatic changes in illumination, occlusion, etc.
Xiaofeng Qu, et.al	2019	A shallow convolutional neural network with laplacian embedding (shallowCNN-LE)	The experimental results confirmed that the designed model performed more successfully in contrast to others while detecting face anti-spoofing.	The designed model was more prone to some specific face spoof attacks.

C. Face Spoof Detection using Image Processing

Graham Desmon Simanjuntak, et.al (2019) presented a method to detect a face spoofing on the basis of color distortion analysis for capturing the chromatic aberration from a face image [23]. The color distortion was analyzed for extracting the color moment and ranked histogram attributes that resulted in creating 116 feature vector. Thereafter, PCA (Principal Component Analysis) employed these feature vectors for mitigating the dimensionality. The face images were classified as spoof or real using NB (Naïve Bayes) on the principal components. The experimental outcomes validated that the presented method offered the TPR (True Positive Rate) up to 97.4% in comparison with the existing methods.

Shan Jia, et.al (2021) suggested a new anti-spoofing technique on the basis of MC_FBC (factorized bilinear coding of multiple color channels) in order to learn the way for differentiating the real images from the spoofed ones [24]. The discriminative and fusing complementary information was extracted from RGB and YCbCr spaces to build a principled solution for detecting the 3D (three dimensional) face spoofing. According to the experimental outcomes, the suggested technique was more effective as compared to the existing technique achieves under different scenarios.

Mayank Yadav, et.al (2018) constructed a method of detect face spoofing so that the faces were classified as real and spoofed [25]. The KNN (K-Nearest Neighbor) algorithm was implemented to classify the faces using the approximate equal classification methods. The results of the constructed methods were analyzed with regard to accuracy and execution time. The experimental results revealed that the constructed method was assisted in maximizing the accuracy and mitigating the execution time.

Patrick P. K. Chan, et.al (2018) developed a technique to detect the face liveness with flash against 2D (two dimensional) spoofing attack [26]. The flash was helpful for enhancing the process to different the authentic users from the malicious ones as well as alleviating the impact of the environmental factors. The information related to the images was captured using 4 texture and 2D structure descriptors. The cost to install this flash was lower and there was not any necessity of user cooperation. The experiments were conducted on the dataset in which 50 subjects were included. The experimental results indicated that the developed technique was more applicable in comparison with others in different environmental scenarios and proved more accurate and robust while detecting the face spoofing.

Vanitha A., et.al (2018) recommended an efficient CCMF (Color based Chromatic Moment Features) algorithm to detect the face spoof [27]. This algorithm was consisted of two modules. At first, Viola Jones technique was implemented to detect the face. After that, the recommended algorithm was deployed to detect the face liveliness. NUAA, MSU MFSD datasets were applied to test this algorithm with regard to reliability. The experimental results revealed that the recommended algorithm yielded superior accuracy around 91.75% as compared to the conventional methods.

Comparison Table

Author	Year	Technique Used	Findings	Limitations
Graham Desmon Simanjuntak, et.al	2019	A face spoofing detection based on color distortion analysis	The experimental outcomes validated that the presented method offered the TPR (True Positive Rate) up to 97.4% in comparison with the existing methods.	The presented method was not captured more generalized attributes, which were useful for detecting other kind of face spoofing attacks.
Shan Jia, et.al	2021	MC_FBC (factorized bilinear coding of multiple color channels)	According to the experimental outcomes, the suggested technique was more effective as compared to the existing technique achieves under different scenarios.	The error rate obtained from the suggested technique was still found 10% under inter-database.
Mayank Yadav, et.al	2018	Face spoof detection method	The experimental results revealed that the constructed method was assisted in maximizing the accuracy and mitigating the execution time.	The constructed method was not suitable to detect all kinds of face spoofing attacks.
Patrick P. K. Chan, et.al	2018	Face liveness detection method	The developed technique was more applicable in comparison with others in different environmental scenarios and proved more accurate and robust while detecting the face spoofing.	The illuminance of flash had not any impact on human eyes still this was the major concern related to user comfort.
Vanitha A., et.al	2018	Color based Chromatic Moment Features (CCMF) scheme	The experimental results revealed that the recommended algorithm yielded superior accuracy around 91.75% as compared to the conventional methods.	This algorithm was not detected the spoofing attack in real time.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue II Feb 2022- Available at www.ijraset.com

III. RESEARCH METHODOLOGY

The methods of detecting face spoof detection are applicable to detect the input as spoofed or normal. This work projected a system to detect the face spoof in diverse stages which are defined as:

1) *Pre-processing Phase:* It is the initial stage to detect the face spoof. An image dataset generated from a reliable data source is utilized for input in the system. Kaggle was implemented to gather the images. The noise is eliminated from the images by processing the input images to accomplish the effective execution.
2) *Segmentation:* The fundamental objective of this stage is to partition a digital image into numerous segments. This technique is utilized to recognize the objects or acquire the information from the photos of face. This procedure assists in mitigating the complexity when the image is analyzed. The bounding line of pictures and objects is investigated. Every pixel is labeled in an image by sharing diverse attributes via pixels available under the similar label. KMC (K-Means Clustering) is implemented for classifying the objects on the basis of a set of attributes. This leads to alleviate the sum of the squares of the distance amid the object and the equivalence cluster to classify the object. 3 is the highest value of k which is taken for input. The segments of images are created in accordance with the value of K.
3) *Feature Extraction:* The outcomes obtained are considered as a ROI (region of interest). Thus, this stage aims to extract the attributes from this selected area. It is a process in which a group of attributes are extracted from an image. The significant information related to picture is obtained from these attributes so that the following processing becomes easy. Various attributes such as colour, texture, morphology and color coherence vector are utilized to recognize the face. At present, several methods are present to extract the attributes. These methods are capable of developing a system. GLCM (Gray-scale co-occurrence matrix), color co-occurrence technique, spatial gray-level dependency matrix and HOG (histogram of oriented gradients) are various methods utilized to extract the attributes. GLCM is a statistical technique utilizes to extract the texture attributes. The extraction of a number of attributes such as Entropy, Correlation and Variance etc. is done to detect the symptom at initial phase.

These attributes are discussed as:-

a) *Contrast:* It is a measure of the local variations available in an image.

$$Contrast = \sum_{n=0}^{G-1} n^2 \left\{ \sum_{i=1}^{G} \sum_{j=1}^{G} P(i,j) \right\}, |i-j| = n \ldots . (4)$$

This measure of contrast will support contributions from $P(i,j)$away from the diagonal, i.e. $i \neq j$

b) *Homogeneity:* It is a measure of the closeness of the distribution of elements in the GLCM (Gray-scale co-occurrence matrix) to the GLCM diagonal

$$\sum_{i} \sum_{j} \frac{P_d[i,j]}{1 + |i-j|} \ldots . (5)$$

c) *Local Homogeneity, Inverse Difference Moment (IDM)*

$$IDM = \sum_{i=0}^{G-1} \sum_{j=0}^{G-1} \frac{1}{1 + (i-j)^2} P(i,j) \ldots . (6)$$

It has influence of the homogeneity of the image as the weighting factor $(1 + (i-j)^2)^{-1}$IDM can attain small contributions from inhomogeneous regions $(i \neq j)$. The result shows a lower Inverse Difference Moment value for inhomogeneous images and a relatively higher value for homogeneous images.

d) *Entropy:* It is a measure of information content. This component is employed to quantify the randomness of intensity distribution. Lower 1st order entropy is included in inhomogeneous scenes, whereas a homogeneous scene attains a higher entropy.

$$-\sum_{i=0}^{G-1} \sum_{j=0}^{G-1} P(i,j) \times \log\big(P(i,j)\big) \ldots . (7)$$

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue II Feb 2022- Available at www.ijraset.com

e) Correlation: It is a measure of gray level linear dependence among the pixels at the particular positions relative to each other.

$$\sum_{i=0}^{G-1}\sum_{j=0}^{G-1} P\frac{\{i \times j\} \times P(i,j) - \{\mu_x \times \mu_y\}}{\sigma_x \times \sigma_y} \ldots . (8)$$

f) Sum of Squares, Variance:

$$\sum_{i=0}^{G-1}\sum_{j=0}^{G-1} (i-\mu)^2 P(i,j) \ldots . (9)$$

This attribute is responsible for placing relatively high weights on the elements which are different from the average value of $P(i,j)$.

4) Classification of Data: The final stage is to develop a model for detecting the face spoof. The dataset is divided in two sets. The training set is large as it deploys 60% of the data and rest of the data is utilized in the testing set to perform the classification. KNN (K-Nearest Neighbour) is a classification algorithm planed on the basis of instance. The similar or similarity functions are utilized at individual level for relating the unknown samples to the unknowns in this algorithm. The learning process of this algorithm is slow. Moreover, the formulation and analysis of this algorithm is done at the same time. The k-nearest centers are required for assigning the larger part of class to the unspecified case. Simplicity is the major factor of this algorithm. The majority vote and its k neighbours play a significant role in this algorithm. This algorithm is a suitable for performing classification and regression. RF (Random Forest) is a ML (Machine Learning) algorithm which provides flexibility. The algorithmic tree predictors are integrated in this algorithm. RF generates optimal outcomes in all of the scenarios. Diverse kind of data can be handled using this algorithm. This algorithm allows the development of numerous trees. The promising outcomes are obtained with the integration of these trees in terms of precision. The major task of ML is to perform the classification. This work presents hyperparameters which are similar to DTs (decision trees) or bagging algorithms. The random trees are overlapped in this algorithm and their analysis can be conducted easily. To illustrate, seven random trees provide information related to some variables. 4 trees are agreed and rest are not. The SVM (Support Vector Machine) is integrated in voting procedure so that the classification can be executed. This ML algorithm is planned according to the majority of voting. In Random Forest, a random subset of attributes, available on the dataset, provides outcomes with higher accuracy. The output acquired from the RF, K-Nearest Neighbour and SVM is utilized in voting for input to vote amid the two classification algorithms and for generating optimal results.

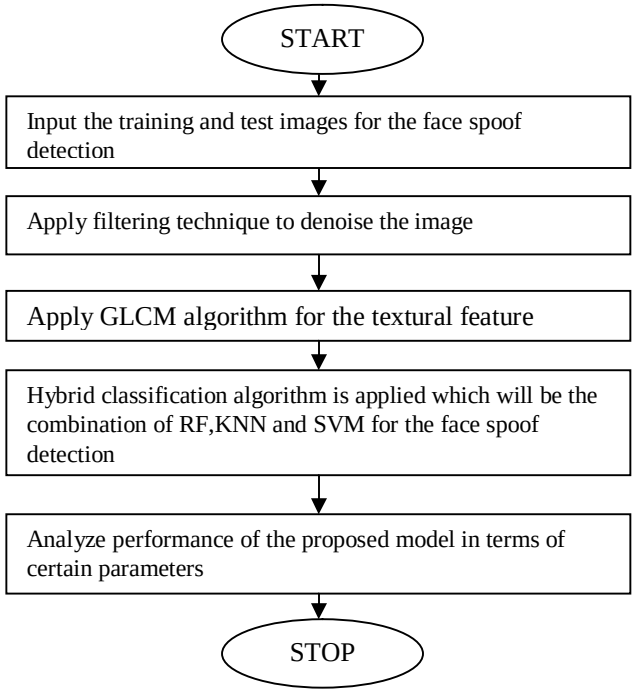


Figure 2: Proposed Flowchart

IV. RESULT AND DISCUSSION

MATLAB tool assists in carrying out the mathematical complex computations. This tool makes the utilization of simplified C as the programming language. There are a number of inbuilt toolboxes such as mathematical toolbox, drag and drop based Graphical User Interface, Image processing, NNs etc. are comprised in this tool. The algorithms are exploited, graphs are plotted and user interfaces are designed using MATLAB. The results of the proposed model is analyzed in terms of accuracy, precision and recall.

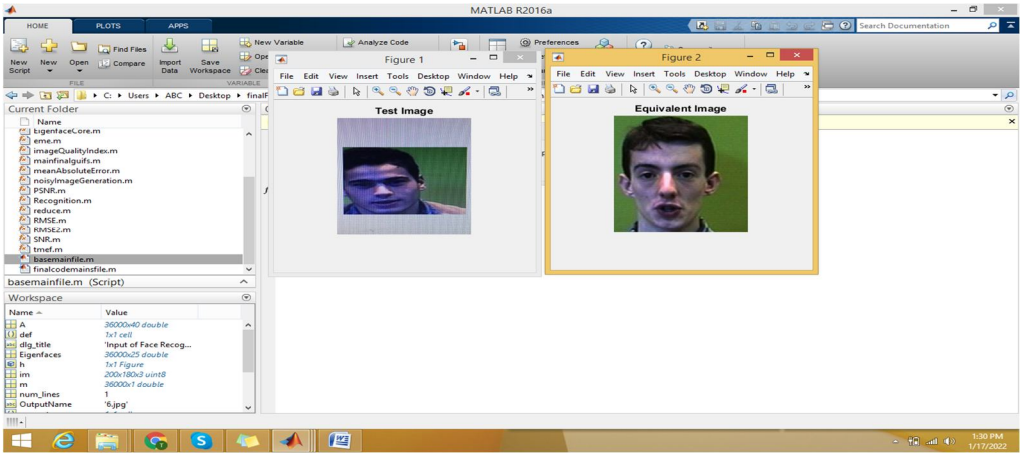


Figure 3 Matched Image

As shown in figure 3, the attributes of the test and training images are analyzed with the help of textual feature analysis algorithm. The Voting classifier is applied which can classify the best match which is shown in the form of matched image.

Table 2.4. Performance Analysis

Parameter	KNN Classifier	GLCM +Hybrid Classifier
Accuracy	84.56 percent	94.12 percent
Precision	83.45 percent	94.00 percent
Recall	81.90 percent	95.90 percent

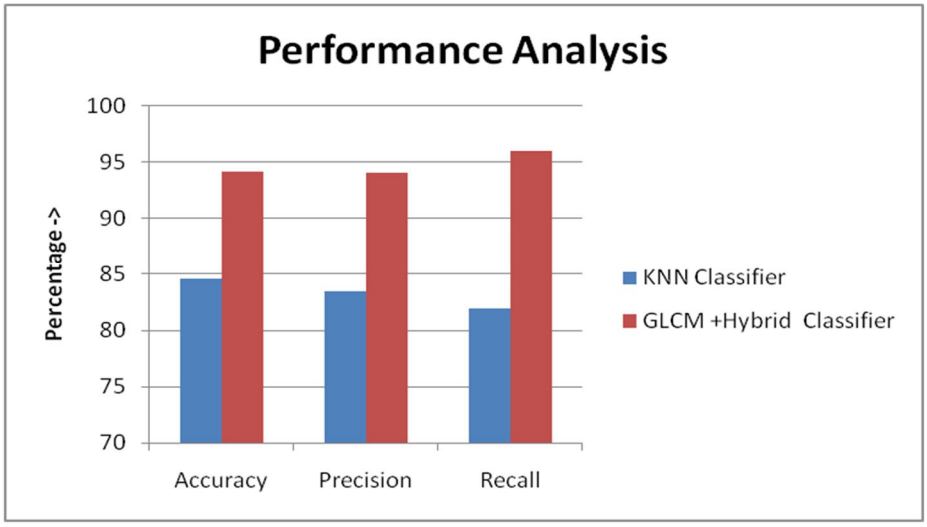


Figure 4 Accuracy Comparison

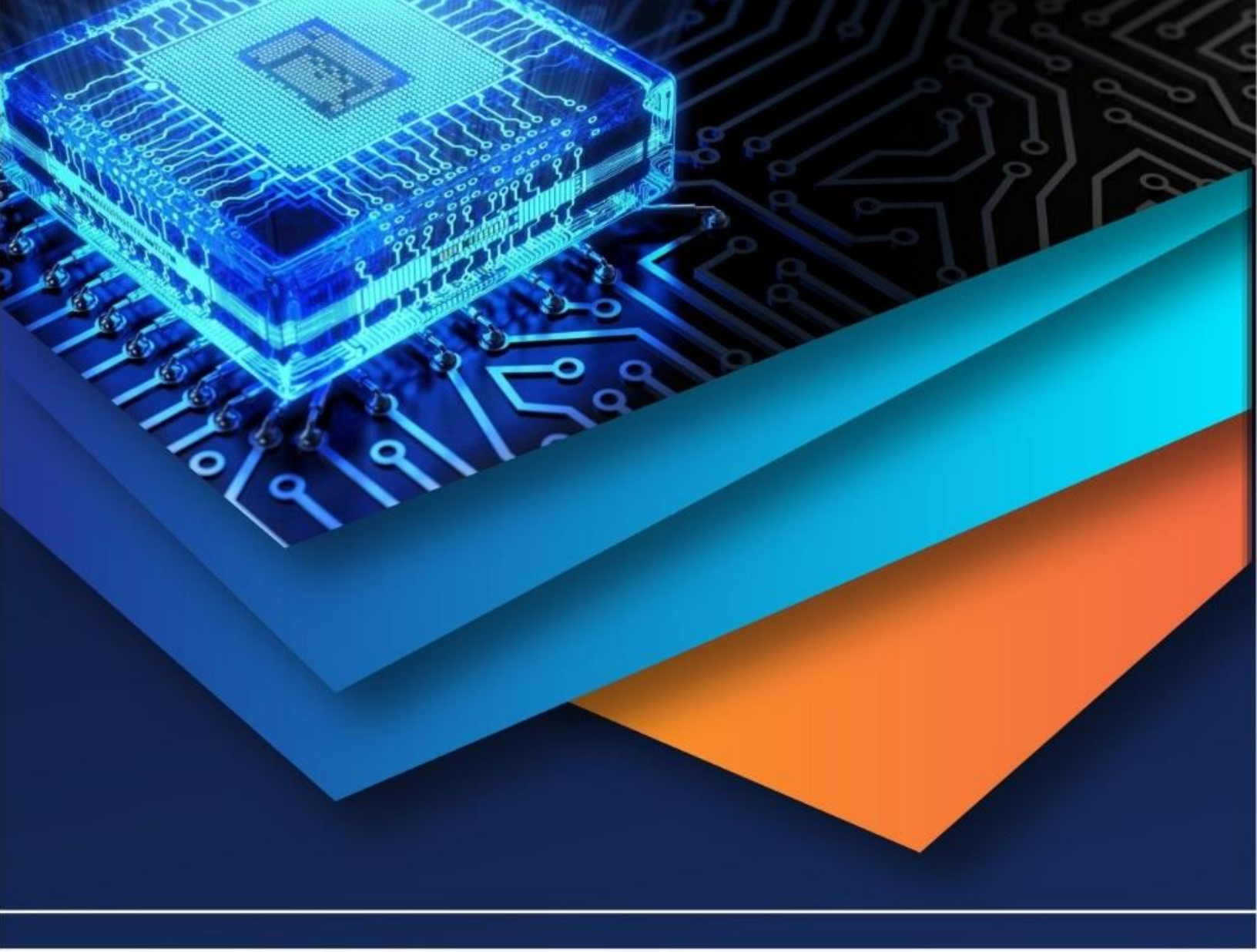
Figure 4 illustrates the analysis of the performance of KNN (K-Nearest Neighbor) classification and hybrid classifier concerning precision, recall and accuracy. This demonstrates that the hybrid classifier provides higher values of all three metrics in comparison with KNN.

V. CONCLUSION

The Machine learning algorithm focuses on extracting the novel values from the earlier experiences. The training set is executed to carry out the segmentation, analyze the attributes and performs the classification. The test set is available in the form of an image whose identification is required for the attendance system. This research work utilizes the hybrid classifier for classifying the faces. The GLCM (grey level co-occurrence matrix) is implemented to analyze the texture attributes so that the faces can be classified. The simulation outcomes indicate that the introduced technique enhances the results up to 10%.

REFERENCES

[1] Zinelabidine Boulkenafet, Jukka Komulainen and Abdenour Hadid, “Face Spoofing Detection Using Colour Texture Analysis”, 2018, IEEE Transactions on Information Forensics and Security, Vol. 45, No. 21, PP. 489-495
[2] Di Wen, Hu Han, Anil K. Jain, “Face Spoof Detection with Image Distortion Analysis”, 2015, IEEE Transactions on Information Forensics and Security, Vol. 10, No. 4, PP.746 - 761
[3] Shervin RahimzadehArashloo, Josef Kittler, William Christmas, “Face Spoofing Detection Based on Multiple Descriptor Fusion Using Multiscale Dynamic Binarized Statistical Image Features”, 2015, IEEE Transactions on Information Forensics and Security, Vol. 10, No. 11, PP. 2396 – 2407
[4] Allan Pinto, HelioPedrini, William Robson Schwartz, Anderson Rocha, “Face Spoofing Detection Through Visual Codebooks of Spectral Temporal Cubes”, 2015, IEEE Transactions on Image Processing, Vol. 24, No. 12, PP. 4726 – 4740
[5] Keyurkumar Patel, Hu Han, Anil K. Jain, “Secure Face Unlock: Spoof Detection on Smartphones”, 2016, IEEE Transactions on Information Forensics and Security, Vol. 11, No. 10, PP. 2268 – 2283
[6] Abdulkadir Şengür, Zahid Akhtar, YamanAkbulut, Sami Ekici, Ümit Budak, “Deep Feature Extraction for Face Liveness Detection”, 2018, International Conference on Artificial Intelligence and Data Processing (IDAP), Vol. 35, No. 11, PP. 6373-6381
[7] R. Raghavendra, Kiran B. Raja, Christoph Busch, “Presentation Attack Detection for Face Recognition Using Light Field Camera”, 2015, IEEE Transactions on Image Processing, Vol. 24, No. 3, PP. 1060 – 1075
[8] Xiao Song, Xu Zhao, Tianwei Lin, “Face spoofing detection by fusing binocular depth and spatial pyramid coding micro-texture features”, 2017, IEEE International Conference on Image Processing (ICIP), Vol. 55, No. 13, PP. 4648-4654
[9] Hoai Phuong Nguyen, Florent Retraint, Frédéric Morain-Nicolier, Agnès Delahaies, “Face spoofing attack detection based on the behavior of noises”, 2016, IEEE Global Conference on Signal and Information Processing (GlobalSIP), Vol. 32, No. 9, PP.7582-7589
[10] HeniEndahUtami, Hertog Nugroho, “Face Spoof Detection by Motion Analysis on the Whole Video Frames”, 2017, 5th International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME), Vol. 21, No. 7, PP. 8993-9001
[11] Wonjun Kim, Sungjoo Suh, Jae-Joon Han, “Face Liveness Detection from a Single Image via Diffusion Speed Model”, 2015, IEEE Transactions on Image Processing, Volume: 24, Issue: 8
[12] A. Fernández, J.L. Carús, R. Usamentiaga, R. Casado, “Face Recognition and Spoofing Detection System Adapted to Visually-Impaired People”, 2016, IEEE Latin America Transactions, Volume: 14, Issue: 2
[13] Polash Kumar Das, Bin Hu, Chang Liu, Kaixin Cui, Prabhat Ranjan, Gang Xiong, “A New Approach for Face Anti-Spoofing Using Handcrafted and Deep Network Features”, 2019, IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)
[14] Xun Zhu, Sheng Li, Xinpeng Zhang, Haoliang Li, Alex C. Kot, “Detection of Spoofing Medium Contours for Face Anti-Spoofing”, 2021, IEEE Transactions on Circuits and Systems for Video Technology
[15] Abdulkadir Şengür, Zahid Akhtar, YamanAkbulut, Sami Ekici, Ümit Budak, “Deep Feature Extraction for Face Liveness Detection”, 2018, International Conference on Artificial Intelligence and Data Processing (IDAP)
[16] Shilpa Garg, Sumit Mittal, Pardeep Kumar, Vijay Anant Athavale, “DeBNet: Multilayer Deep Network for Liveness Detection in Face Recognition System”, 2020, 7th International Conference on Signal Processing and Integrated Networks (SPIN)
[17] Abdelrahamn Ashraf Mohamed, Marwan Mohamed Nagah, Mohamed Gamal Abdelmonem, Mohamed Yasser Ahmed, Mahmoud El-Sahhar, Fatma Helmy Ismail, “Face Liveness Detection Using a sequential CNN technique”, 2021, IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)
[18] Wenyun Sun, Yu Song, Haitao Zhao, Zhong Jin, “A Face Spoofing Detection Method Based on Domain Adaptation and Lossless Size Adaptation”, 2020, IEEE Access
[19] Raden BudiartoHadiprakoso, Hermawan Setiawan, Girinoto, “Face Anti-Spoofing Using CNN Classifier & Face liveness Detection”, 2020, 3rd International Conference on Information and Communications Technology (ICOIACT)
[20] Junqin He, Jun Luo, “Face Spoofing Detection Based on Combining Different Color Space Models”, 2019, IEEE 4th International Conference on Image, Vision and Computing (ICIVC)
[21] Xiaofeng Qu, Jiwen Dong, SijieNiu, “shallowCNN-LE: A shallow CNN with Laplacian Embedding for face anti-spoofing”, 2019, 14th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2019)
[22] Graham Desmon Simanjuntak, Kurniawan Nur Ramadhani, Anditya Arifianto, “Face Spoofing Detection using Color Distortion Features and Principal Component Analysis”, 2019, 7th International Conference on Information and Communication Technology (ICoICT)
[23] Shan Jia, Xin Li, Chuanbo Hu, Guodong Guo, Zhengquan Xu, “3D Face Anti-Spoofing With Factorized Bilinear Coding”, 2021, IEEE Transactions on Circuits and Systems for Video Technology
[24] Mayank Yadav, Kunal Gupta, “Novel Technique for Face Spoof Detection in Image Processing”, 2018, Second International Conference on Intelligent Computing and Control Systems (ICICCS)
[25] Patrick P. K. Chan, Weiwen Liu, Danni Chen, Daniel S. Yeung, Fei Zhang, Xizhao Wang, Chien-Chang Hsu, “Face Liveness Detection Using a Flash Against 2D Spoofing Attack”, 2018, IEEE Transactions on Information Forensics and Security
[26] Vanitha A., Vaidehi V., Vasuhi S., “Liveliness Detection in Real Time Videos using Color based Chromatic Moment Feature”, 2018, International Conference on Recent Trends in Advance Computing (ICRTAC)



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY