Face Spoof Detection Using Tree Based Classifiers

Nisha sharma
nishasharma214@gmail.com
Research Scholar
Daviet Collage Jalandhar

Sahul goyal
Er.sahul.goyal@gmail.com
Assistant Professor
Daviet Collage Jalandhar

Abstract - The face recognition is the approach which is applied to recognize face of the input image. The face spoof detection is implemented for detecting the spoofed faces. The face spoof detection techniques have various steps which are pre-processing, feature extraction and classification. In this research work, the DWT technique is utilized for extracting the attributes. In the last, the techniques of decision tree and random forest are applied for the classification. It is analyzed that proposed technique improve precision and recall upto 10 percent as compared to existing techniques

Keywords - DWT, Random Forest, Decision Tree, Precision, Recall

I. INTRODUCTION

Providing security measures against any kinds of spoofing attacks is very important for general public. The fastest and most efficient security industry known for this is biometrics. The identity of an individual is stabled in biometrics on the basis of certain important attributes of an individual which differentiate him from other humans. Verifying the identity of individual is the most important task of a security system. The impostors are prevented from accessing the protected resources through such mechanism. Passwords or ID cards are some of the general security methods used in various systems [1]. However, it is easy to lose, hamper or steal such kinds of techniques of identity due to which the intended security can be affected. Higher level of security can be offered for a security system by a biometric system since it includes physical and biological properties of human beings. Iris scanner, handwriting verification, facial recognition, and facial recognition are few such techniques applied in various applications. The face recognition technology has been designed over the few years and in comparison to other techniques, this approach is user friendly, convenient and more direct.

In different get to regulate applications, particularly for mobile unlocking, the automatic face recognition technique has received huge attention [2]. For the mobile phones using IOS systems, the face recognition is known to be another biometric identification method that was previously commonly used in Android mobile operating system packages. There is no need of any other detector once the face recognition method is applied since there is a back and front end camera equipped in each of the single advanced mobile [3]. The concerns related to face parody assaults are an issue for the face recognition systems since they cause a reliability issue for the applications like police investigations. Imitating face recognition through artificial means has become exhausting due to the presence of commonalities among faces. Additionally, due to the presence of facial article of furniture, the illumination conditions, facial expressions and various image qualities, this mechanism is confusing. If the human faces are shown in the given image or not is the initial factor to be considered. Another factor to be considered is the location of these faces [4]. Few pictures are collected for every individual and the features are extracted and stored within the database to be used further. Performing face detection and performing extraction are the important steps. Further, for every face category that is stored within the database, the features are compared. For contending with the classification downside, various algorithms are explored here. Identification and verification are the two important applications of face recognition [5]. A system is designed for informing who the person is through the face identification process. When given a face image, the identification is guessed through face verification process. The guess is determined to be either true or false through this method. In order to build a recognition system, data sets are required for generating classes and comparing resemblance amid the test data and every class. In general, test data is referred as a "query" in image extraction written tasks. This term can be used all over the report. Generally, at first, size of the obtained data is reduced using data-driven and domain knowledge methods. All data in the datasets is translated into a feature set after the reduction of data size. Hence, the classification model is initially trained half on these feature images [6]. If a query generates, once again similar size reduction process is applied and the classifier becomes fully trained. Biometrics refers to the techniques that measures and examines the features of bodily features for face spoof detection. There are mainly two types of biometric features available. These features are mainly identified as physical and behavioral

attributes. Physical attributes are like fingerprints, face patterns. Conversely, behavioral attributes are voice, autograph or walking patterns (gait) [7]. Most of the biometric recognition frameworks go through a major challenge of ID (identity)stealing. This issue is generally referred as spoofing attack. The fraudsters can use and manipulate this stolen data readily to get illegal access of the biometric frameworkwithout the permission of the legal client [8]. Examples of spoofing attacks on biometrics systems are regarding the usage of artificial fingers, contact lens etc. Researchers have made a lot of efforts for the detection of face spoofing attacks over the time. This work presents a new face spoof detection approach. This approach makes use of facial features for face spoof detection. In general, forged faces are divided into two groups [9]. These groups are known as positive and negative. The positive group contains real faces that have limited variation. On the other hand, the negative group containsspoofed faces on images, dummy or recorded videos.

II. LITERATURE REVIEW

Theja J. Jayan, et.al (2018)proposed a fast and robust algorithm through which the fake faces could be detected from the photographs posted on different social platforms [10]. Within the various color spaces, the face segments were extracted and the illuminate map of region was estimated through the proposed algorithm. Additionally, the image quality parameters of segment were measured by this algorithm and the background region was compared. The feature vectors were generated using the image quality metrics based on reference and without reference. The fake face was recognized using the QDA classifier. The different datasets were used for testing the proposed algorithm. The achieved outcomes showed that for detecting the fake faces, the proposed method achieved around 96% of accuracy.

Graham Desmon Simanjuntak, et.al (2019) suggested a new approach for detecting the face spoofing using the color distortion analysis [11]. Here, the chromatic aberration was captured from the face image using this method. The color moment and ranked histogram features were extracted using the color distortion analysis such that the feature vector could be generated. For performing the dimensionality reduction, the feature vector was forwarded to PCA. The Naïve Bayes classifier was applied on the principal components collected from PCA such that the live or spoof face image could be classified. Based on the conducted experiments and achieved outcomes it was seen that with the TPR value of 97.4%, the proposed approach provided highly competitive performance as compared to other approaches.

Tanvi Dhawanpatil, et.al (2017) proposed a new method in which the Moire pattern detection was applied for making a robust face authentication system [12]. One of the effective texture based descriptor as compared to others that was applied for spoof detection was the Local Binary Pattern. The SIFT descriptor was applied along with MLBP in this research. Therefore, it was easy to detect the spoof attacks. The MLBP and SIFT descriptor were applied for plotting the histograms. The spoof face was detected through the bin count. Thus, the Moire pattern could detect the spoof faces easily as per this research.

Aziz Alotaibi, et.al(2016) presented a research which aimed to detect the face spoof attacks by designing a non-intrusive approach [13]. Here, the single frame was used among the sequenced frames. The complex and high attributes of input diffused frame were extracted here by designing a specialized deep-CNN based method. The data that includes videos with real access and spoofing attacks was included in a dataset and this dataset was applied for testing the proposed method. Experiments were conducted and results were achieved which showed that the proposed research provided better outcomes as compared to existing approaches.

Mayank Yadav, et.al(2018) proposed the face spoof detection mechanism through which the spoofed and non-spoofed faces from the images could be classified [14]. The DWT algorithm was used here for analyzing the textual features existing in the test image. The previously proposed approach used SVM was classifying the spoofed and non-spoofed features. However, for identifying the spoofed faces, the results need to be improved in terms of their accuracy. The proposed and existing techniques were compared based on the execution time and accuracy for evaluating the efficiency of presented approach. The outcomes showed that the presented approach outperformed previous approaches.

Di Wen, et.al(2015) proposed a new approach in which image distortion analysis was applied for designing a face spoof detection algorithmthat had robustness and efficiency [15]. For designing the IDA feature vector, four various features were extracted in this research. For differentiating among the genuine and spoof faces, the ensemble classifier which included multiple SVM classifiers was applied. A voting based mechanism was applied by the proposed approach was extending it to a multi-frame face spoof detection process in videos. The experiments were performed on two public-domain databases for computing the performance of intendedtechnique. The outcomes showed that the intended approach provided better outcomes than existing researches.

III. PRIOR WORK

The face recognition is generallyused in biometricsystem to reduce the chances of unauthorized access. The machine learning is a common approach for face recognition. In the process of face recognition, has the two steps which are face extraction and classification. In the prior system, the face spoofing is detected using the Support Vector Machine classifier. The state-of-art system of detecting the face spoof has deployed the Discrete Wavelet Transform for analyzing the textual attributes of test image.These attributes play a role of training set in order to carry out the classification. SVM is a supervised ML algorithm. Each data item is plotted as a point in n-Dimensional space in which the value of every figure is the value of a particular coordinate. After that, the hyperplane that is capable of differentiating two classes has discovered for the classification. In this work, the technique has suggested in order to detect the face spoof on the basis of the extraction of attribute and classification. The features which are extracted are reflection, blurriness, chromatic movement and color diversity. The SVM classifier will work on the training and test datasets for the data classification. The SVM algorithm based Neural Network is trained using the selected attributes whose extraction is done from various training images having diverse categories under the training phase. The outcomes obtained from the Support Vector Machine algorithm determine the test image as spoofed or normal. The textual attributes of spoofed image and of original images are approximately equal that leads to mitigate the precision of SVM classification in some cases of detection.

IV. PROPOSED WORK

The method to detect the face spoof is suggested to classify the image as spoofed or without spoofed. The initial stage makes the implementation of method of Eigen face detection which later given as the input value to perform the classification. Samples are employed in order to represent the n-dimensional numeric features in the DT algorithm. A sample reveals the point in n-dimensional space. The possible consequences are represented using a tree-like graph in the DT algorithm. Some set of rules can be generated in case a training data set is utilized as input along with the targets and attributes in DT. The predictions are executed through these rules. This point is demonstrated with one instance. Assume to predict that whether a child likes an animated movie or not. Firstly, all the past animated movies that the child liked must be collected. Some attributes are considered as the input. After that, the DT classifier can be utilized for producing the rules. The attributes of this movie can be employed as input for determine that the child will like this movie or not. The information gain and Gini index calculations are deployed to compute these nodes and generate the rules in this procedure.

V. RESEARCH METHODOLOGY

The face spoof detection method is suggested to classify the spoofed and non spoofed image. TheEigen face detection scheme is carried out at the initial stage. Later on it is utilized as input to perform the classification. Then-dimensional numeric attributes are represented in the K-Nearest Neighbor algorithm using samples. A sample represents thepoint includes in n-dimensional space.The k-training samples are matched andthe pattern space that is close to the unknown sample is chosen with K-NN algorithm in the presence of anyunknown sample.The Euclidean distance is employed to describe thecloseness. Contrasting to other ML method, the weight is broken to each attribute using KNN. Themassive amount of confusion is occurred due to these situations in the availability of unlimited amount of unnecessary data in the network.

A flowchart is presented here to describe research methodology.

There are several stages of the flowchart which are defined as:

Step 1: Input the number of images fororganizing the training set for the spoof and non spoofed faces

Step 2: Eigen Feature Calculation of input training image

2.1. Calculate the Eigen feature of each image

2.2. Store the calculated feature in the database with image label

Step 3: Input the test image that is the unknown image

3.1. Compute the Eigen feature of the unknown image

Step 4: Implement K-Nearest Neighbor algorithm to detect the spoofed and non spoofed unknown image

4.1. Computing the distance between the features of the unknown image and all the images stored in the database

4.2. When distance between the images is above zero, it is non-spoofed

4.3 Otherwise it is spoofed

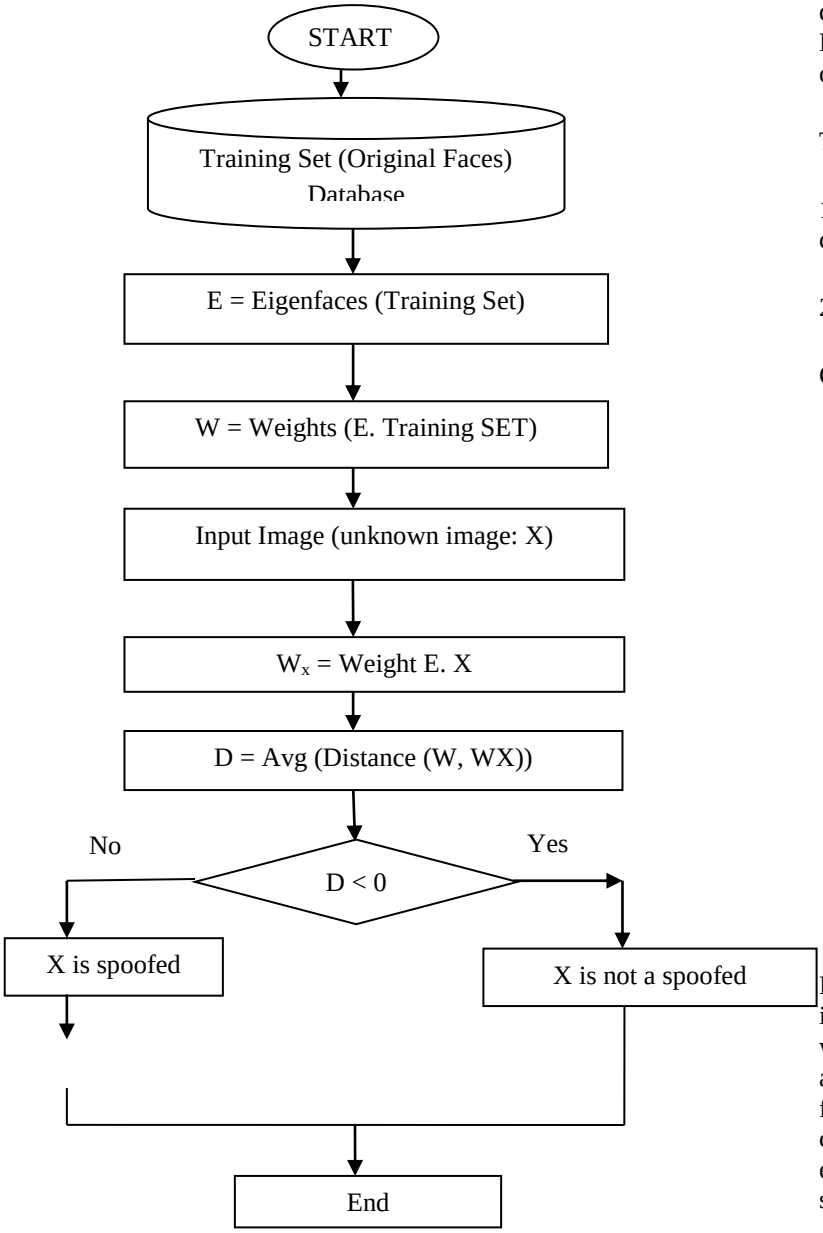

Figure 1: Proposed Flowchart

The algorithm used for the implementation of the proposed work is given below: -

Algorithm

The proposed algorithm detects the spoofed and non-spoofed image. The proposed algorithm is divided into three phases. In the phase 1, the images are taken as input which needs to classify. In the second phase, the feature extraction process is done which the Eigen Vector technique. In the last phase, the Random Forest classification algorithm is applied in order to classify the faces as spoofed or not.

The algorithm is given below: -

1. Input the images of training set and test set for the classification.

2. Store the input image into the variable A

Calculate Features of the input image with following steps:

- $Ax = \lambda X$ denotes that the same direction is kept by x when multiplied by A.
- $Ay = \lambda Y$ represents that the $\det(A - \lambda I) = 0$. N Eigen values are determined by it
- The eigen values of A^2 and A^{-1} are $\lambda^2 and\ \lambda^{-1}$ with the same Eigen vector
- The sum of $\lambda's$ is equal to the sum down the main diagonal of A that is a trace. The product of $\lambda's$ is equal to the determinant.
- Projections denote with P, Reflection denotes with R, 90 rotations reveals with Q have special Eigen values 1, 0, -1:I, -i.
- For the Singular metrics $\lambda = 0$. Triangular metrics have $\lambda's$ on their diagonals.

VI. RESULT AND DISCUSSION

MATLAB is called matrix-laboratory. It is a software package implemented for generating various numerical computations which are complex in nature. The C language is executed in it as theprogramming language. There are various inbuilt functions that can be updated from version to version comprised in the MATLAB. The image processing, NNs, GUI etc. are involved in this in-built function. Thenetworks are stimulated using it in MATLAB that have very high graphics.

There are 10 diverse images of fortyunique subjects are extracted in this data set. Each and every image is taken atdiverse period of time underdissimilar lighting; facial expressions and all the images consist of the facial details. The capturing of images is done indark homogeneous background with the subject at the upright position, front position. This AT&T database is the most common database recognized as The Oral Database of Faces was initially suggested at AT&T laboratory

Table 1: Precision Analysis

Image Number	Existing Algorithm	Proposed Algorithm
1	82	93
2	84.5	92.46
3	81	90.67
4	80	93.45
5	83	92.56
6	81.56	93.45
7	86.78	94.78
8	84.67	93.67
9	82.70	91.56
10	85.78	93.78

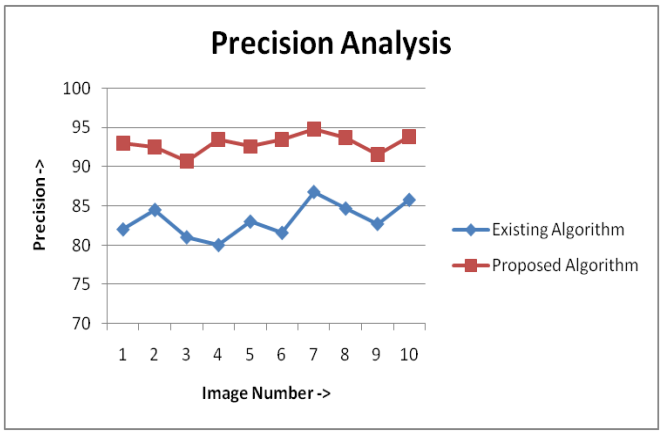

Figure 2: Precision Analysis

The figure 2 represents that the precision value of suggested algorithm is compared with the existing one to analyze the performance. This demonstrated that precision value of the suggested algorithm is higher than the existing algorithm.

Table 2: Recall Analysis

Image Number	Existing Algorithm	Proposed Algorithm
1	82 .4	93
2	84.89	92.46
3	81	90.67
4	80	93.45
5	83	92.56
6	81.56	93.45
7	86.78	94.78
8	84.67	93.67
9	82.70	91.56
10	85.78	93.78

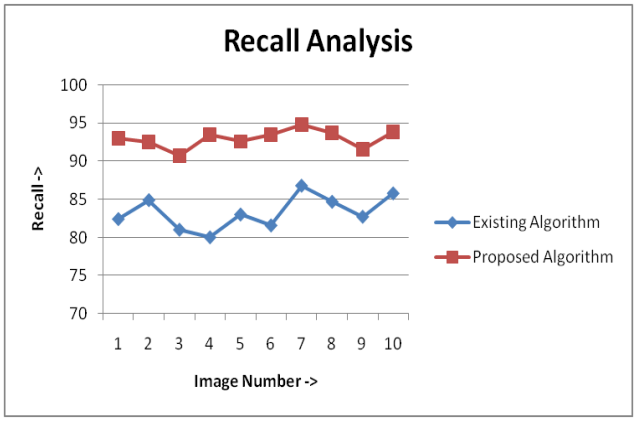

Figure 3: Recall Analysis

The figure 3 denoted that the recall value of existing algorithm is compared with the suggested one while analyzing the performance. This revealed that suggested algorithm has provided the higher recall value than the existing algorithm.

VII. CONCLUSION

In this work, it is observed that the methods of face spoof detection include several phases such as pre-processing, extraction of attribute and classification process. The computation of wavelet features involve in the input images is done to perform the classification. Finally, the DT and RF methods are implemented to complete the classification. The results obtained from the suggested and existing algorithms are contrasted with respect to accuracy and recall. This reveals that accuracy, recall values of suggested algorithm is greater in compared to the existing algorithms.

VIII. REFERENCES

[1] Nidhi Sharma, Mrs. Shivani Chauhan, "Analysis of Face Spoof Detection Technique", 2019, International Journal of Computer Science and Mobile Computing, Vol.8 Issue.3, pg. 166-171

[2] Chin-Lun Lai, Jun-Horng Chen, Jing-Ying Hsu, Chih-Hong Chu, "Spoofing face detection based on spatial and temporal features analysis", 2013, IEEE 2nd Global Conference on Consumer Electronics (GCCE)

[3] Diogo C. Garcia, Ricardo L. de Queiroz, "Evaluating the effects of image compression in Moiré-pattern-based face-spoofing detection", 2015, IEEE International Conference on Image Processing (ICIP)

[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, Volume: 24, Issue: 12

[5] Y. BinnyReeba, R. Shanmugalakshmi, "Spoofing face recognition", 2015, International Conference on Advanced Computing and Communication Systems

[6] 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)

[7] M. Parisa Beham, S. Md. Mansoor Roomi, H. Jebina, M. Kavitha, "Face Spoofing Detection using Binary Gradient Orientation Pattern with Deep Neural Network", 2017, Ninth International Conference on Advances in Pattern Recognition (ICAPR)

[8] Neha D. Patil, Sujata V. Kadam, "Face spoof detection techniques: IDA and PCA", 2016, Online International Conference on Green Engineering and Technologies (IC-GET)

[9] 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)

[10]Theja J. Jayan, R.P. Aneesh, "Image Quality Measures Based Face Spoofing Detection Algorithm for Online Social Media", 2018, International CET Conference on Control, Communication, and Computing (IC4)

[11] Graham Desmon Simanjuntak, Kurniawan Nur Ramadhani,AndityaArifianto, "Face Spoofing Detection using Color Distortion Features and Principal Component Analysis", 2019, 7th International Conference on Information and Communication Technology (ICoICT)

[12] Tanvi Dhawanpatil, Bela Joglekar, "Face Spoofing Detection using Multiscale Local Binary Pattern Approach", 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA)

[13] Aziz Alotaibi, Ausif Mahmood, "Enhancing computer vision to detect face spoofing attack utilizing a single frame from a replay video attack using deep learning", 2016 International Conference on Optoelectronics and Image Processing (ICOIP)

[14] Mayank Yadav, Kunal Gupta, "Novel Technique for Face Spoof Detection in Image Processing", 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)

[15] Di Wen, Hu Han, Anil K. Jain, "Face Spoof Detection with Image Distortion Analysis", IEEE Transactions on Information Forensics and Security, 2015, Volume: 10, Issue: 4