# Face Spoof Detection using KNN classifier

Ramandeep Kaur, P.S.Mann
*D.A.V Institute of Engineering &Technology*

*Abstract*— The Face spoof detection is the technique which is applied which will classify the spoofed and non-spoofed. The DWT algorithm will be applied which will analyze the textual features of the test image. In the existing approach SVM classifier is applied which will classify the spoofed and non-spoofed features. In this work, KNN classifier is applied with the DWT algorithm for face spoof detection. The proposed improvement will also detect the spoofed faces which are approximately equal. The simulation of the proposed and existing technique is done, it is been analyzed that accuracy is increased and execution time is reduced.

**Keywords—**Face spoof detection; IDA;KNN Classifier

## I. INTRODUCTION

An algorithm utilized for performing some operations on an image for making some changes in it or for collecting some useful information from it is known as image processing. As an output various characters are provided that can further be helpful. There are various region-of-interests present within images, which are also referred to as objects that can be a basis for certain region [1]. Any regularity or patterns present within the data present within the images is identified by the process known as pattern recognition process. When the systems are trained by the labeled training data they are known to follow the supervised learning method within the pattern recognition process. However, the labeling of data through unknown previous patterns is known as unsupervised type of training. The most likely matching inputs are gathered for providing study related to the similar inputs that are present within the system. An instance which is also known as a vector of features is mainly given as an input for achieving certain output [2]. In case where it is difficult to identify the patterns through human visuals, the pattern recognition systems help in providing the facility. The patterns are elicited from the area that is to be analyzed and then are bifurcated into several classes. There are three important steps involved within the pattern recognition systems that are pre-processing, feature extraction as well as classification. For the purpose of selecting pattern, the application domain is to be considered by the pattern recognition system [3]. All the domains cannot utilize the similar pattern recognition system. There is a preprocessing of the original input variables for transforming them into some new space of variables within maximum of practical applications. This is done as per the requirement o the specific application [4]. In case of digit recognition issue for example, the translation and scaling of the digits of an image is done in such a manner that each digit is present within a box that is of fixed size. The variability within each of the digital class is minimized to great extent through this step as there are similar sizes of location and scales present for all digits. This further helps on differentiating the various classes within any pattern recognition algorithm.

Face recognition is a very important in many field of research these days. For the purpose of making enhancement in a raw image which might be achieved from a camera, satellite or any other source, the image processing techniques are utilized within face recognition methods [5]. Mainly the applications of face recognition are involved in automatically identifying or verifying the person from a certain digital image. Selected facial features of an image are compared with the database present within the systems for such identification and verification. Mainly in security systems and biometrics such as fingerprints, iris recognition and so on, these systems can be involved. This application has helped in providing more secure environments in numerous applications. There are various steps involved within this process which are face detection, feature extraction, and face recognition [6].

Face detection has the main objectives of identifying if there is any human face present within the provided image and the location of the present faces. The patches of the faces present within that image are given as output. The extraction of these patches that contain human-face, from the image is known as the feature extraction process [7]. Once the representation of each face is formulized, the recognition of their identities is the next step which is also known as face recognition step. There is a need to build the face database for attaining automatic recognition. There are numerous images gathered for each person and the features are extracted and stored within a database for matching them in future.

Within the biometric recognition systems, the greatest challenge is the chance of stealing the individual identity of an individual [8]. This is generally known as a spoofing attack which stoles the biometrics data and further exploits or mimics the original data. The unauthorized users can enter the biometric system and the original user can have no knowledge regarding this which thus will destroy the authenticity of the system. The process of showing fake sample to the acquisition sensor that contains facial information of certain user is known as face spoofing process. The fake sample that is presented can be in any form such as picture, video, and so on [9]. There can be image-based as well as video-based face spoofing attacks. For testing the originality of the biometric sample various methods have been proposed which help in detecting the spoofing attack. The proposed methods can be frequency-based, texture-based or motion-based as per their properties.

## II. LITERATURE REVIEW

Reshma Rajan et.al, (2017) proposed in this paper [10], the involvement of color texture along with the IDA features for

enhancing the spoof detection rate. The feature ranking as well as selection process is applied for selecting the set of feature which is best suitable. There are various domain face spoof databases such as MSU MFSD and Idiap Replay-attack on which the proposed method is applied. It is seen through the simulation results achieved that on the basis of Image Distortion Analysis, the performance of proposed method is better than the existing method.

Saptarshi Chakraborty et.al, (2014) proposed in this paper [11] a study of the numerous approaches involved for detecting liveness. In case of liveness detection, there are numerous problems such as the illumination change, amplified noise on images and so on. The texture information present on the image is destroyed due to the impact of such factors. There are various solutions presented here which can avoid the changes occurring due to various factors. For example, eye glasses can be utilized for causing reflection which can be seen as a solution to the problem. There are various non-interactive video sequences that can help in performing certain tasks and involve non-interactive sequences in it.

Ye Tian, et.al, (2016) proposed in this paper [12] a novel technique for avoiding video-based face spoofing attacks. On the basis of local binary patterns (LBP) as well as multiscale discrete cosine transform (DCT), the new technique is proposed that is simple, time-saving and effective. Within the selected frame, the spatial information is chosen with the help of LBP features. There are two benchmarking datasets that are replay-attack and CASIA-FASD on which the experiments are made. Comparisons of the simulation results achieved are made and it is seen that the novel approach is more effective as compared to the existing methods.

Azeddine Benlamoudi, et.al, (2015) proposed in this paper [13] an approach for differentiating the 'live' and 'fake' faces. This method basically is an anti-spoofing method as it will help in avoiding the unauthorized users to enter the system and make any changes. The features within each region of an image are extracted with the help of overlapping block LBP operator. Fisherscore method is utilized for minimizing the features. To check if the input image is related to any live face or not, a nonlinear Support Vector Machine (SVM) classifier is utilized along with the kernel function. As per the results achieved, it is seen that the proposed technique performs better than the other similar methods applied earlier.

Roberto Tronci, et.al, (2011) proposed in this paper [14] a study on both video and static analysis for attaining necessary information related to the motion, texture and liveness of the data. This study helps in providing a more robust classification of the data. As per the static analysis the outcomes achieved show that the detection of photo spoofing attacks can be done very easily through this type of analysis. A single frame can be utilized for implementing this static analysis. There are various methods apart from this method that can be utilized for visual degradation clues. However, a portion of video is required for their processing. So, the proposed method in this paper provides better classification results as it gathers various static and video analysis tools for analysis.

William Robson, et.al, (2011) proposed in this paper [15] an anti-spoofing solution on the basis of set of low-level feature descriptors. This method differentiates amongst the live and spoof images or videos present within a system. For the purpose of learning various properties amongst two different classes, the spatial and temporal information is analyzed. As per the simulation results achieved, the proposed method provides better results in comparison to the existing approaches. The experiments are conducted on the datasets that include both images as well as videos.

## III. PROPOSED METHODOLOGY

The face spoof Detection is the technique which detects the spoofed information of the faces which wants to take un-authorized of the bio-matrix system. The SVM classification technique is been used in the previous systems for the face spoof detection. In the existing system for the face spoof detection textual features of the test image is analyzed using the DWT algorithm. The textural features will be act like the training set for the classification. The result of the SVM classification will classify the test image into spoofed or non-spoofed face. The textual features of the spoofed image is approximate equal to the original image due to which SVM classification accuracy is reduced in some cases of detection. In this work, KNN classifier is used for the face spoof classification. In KNN classifier The training samples are depicted by n dimensional numeric attributes. Every sample represents a point in an n-dimensional space. Along these lines, the greater part of the training samples is stored in an n-dimensional pattern space. At the point when given an unknown sample, a k-nearest neighbor classifier looks the pattern space for the k training samples that are closest to the unknown sample. "Closeness" is defined in terms of Euclidean distance. Not at all like decision have tree induction and back propagation, nearest neighbor classifiers assigned break even with weight to every attribute. This may bring about confusion when there are numerous irrelevant attributes in the data. Nearest neighbor classifiers can likewise be utilized for prediction, that is, to give back a genuine valued prediction for a given unknown sample. For this situation, the classifier gives back the average value of the genuine valued associated with the k nearest neighbors of the unknown sample. The k-nearest neighbors' algorithm is among the simplest of all machine learning algorithms. The features of the test image will be analyzed with the DWT algorithm and on the detected features KNN classifier will be applied which will classify the face into spoofed or non-spoofed.

### A.Pseudo code of SVM classifier for face spoof Detection

1. Input: Tanning, trained datasets
2. Output : Classified Data
3. Apply DCT ()
    1. For k = 0 To DCTsize – 1
    2. DCT(k) = 0
    3. For n = 0 To DCTsize - 1
    4. DCT(k) = DCT(k) + WaveForm(n) * Cos(Pi * k / DCTsize * (n + 0.5))

5. Next n
6. Next k

4. Apply SVM classifier ()
   1. Set the S be an empty set
   2. For (each item is the K)
   3. Compute d=[$k_{1,\ldots\ldots}K_n$] according to equation given in step 4

$$\frac{1}{2} w^T w + C\sum_{i=1}^{N} \xi_i$$

   4. .
   5. Compute the kernel function $a^k$ for the data classification
   6. repeat the step 2 to 4 until whole data get classified
   7. return classified data

**B.Pseudo Code of KNN classifier for face spoof Detection**

1. Input: Tanning, trained datasets
2. Output : Classified Data
3. Apply DCT ()
   1. For k = 0 To DCTsize – 1
   2. DCT(k) = 0
   3. For n = 0 To DCTsize - 1
   4. DCT(k) = DCT(k) + WaveForm(n) * Cos(Pi * k / DCTsize * (n + 0.5))
   5. Next n
   6. Next k
4. Apply Knn classifier
   1. Classify (K, n , X ) training data is K, n is the trained data, X is the number of samples
   2. for i=1 to size of the input data do
   3. compute distance d($X_i$,x)
      End for
   4. Compute set I containing indices for the k smallest distance d($X_i$x)

Return majority lable for ($Y_i$ where i belongs to I}

## IV. RESULTS AND DISCUSSION

The proposed KNN based face spoof detection algorithm is tested in the 10 test images and also compared with the existing SVM based face spoof detection algorithm. The MATLAB is the tool which is used for the simulation. In the results it is shown that proposed algorithm performs well in terms of Execution time, accuracy, false positive rate and false negative rate.

1) **Execution Time:** It is the time during which a program is running

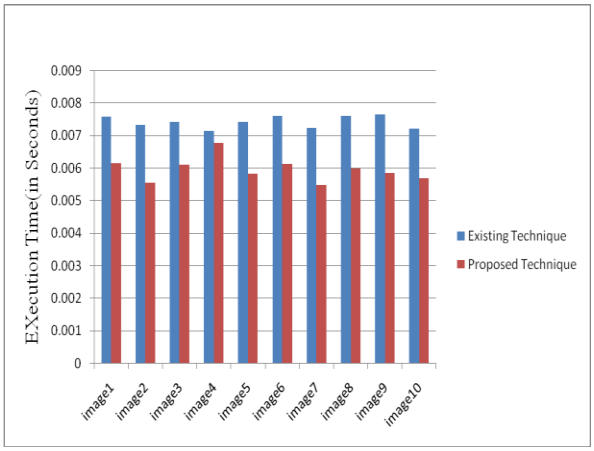
Execution Time= End of Algorithm Time - Start of Algorithm Time …..(1)

Table 1: Difference between Execution Time of existing and proposed technique

| Image Number | Execution Time of Existing Technique (in Seconds) | Execution Time of Proposed Technique(in Seconds) |
|---|---|---|
| 1 | 0.007593 | 0.006158 |
| 2 | 0.007343 | 0.005548 |
| 3 | 0.007438 | 0.006100 |
| 4 | 0.007154 | 0.006771 |
| 5 | 0.007422 | 0.005836 |
| 6 | 0.007623 | 0.006136 |
| 7 | 0.007245 | 0.005485 |
| 8 | 0.007613 | 0.005992 |
| 9 | 0.00765 | 0.005857 |

To compare the proposed technique with existing technique, first Execution time parameter has use. We are measuring Execution time in seconds.
To Calculate the Execution time **tic and toc** functions are used .Tic defines start of execution and toc defines end of execution.

Graph 1: Difference between Execution Time of existing and proposed technique




From above given graph, we can easily compare the execution time difference between the existing and proposed technique. From the graph, it is clear that proposed technique takes less execution time as compare to the existing technique.

**2) Accuracy**

To compare the proposed technique with existing technique, secondly Accuracy parameter has use.
**Accuracy** defines how precise is the calculation at taking in an arrangement of appearances from preparing pictures and afterward accurately recognizing similar individuals from a test set of various pictures, where both picture sets contain similar individuals.

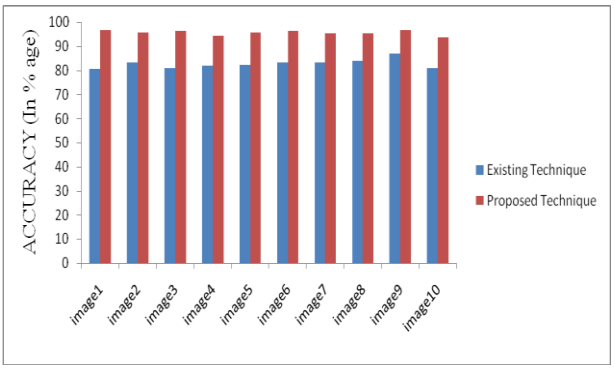
Accuracy=No. of points classified *100
Total No. of Points

Table 2: Comparison of Accuracy

| Image Number | Accuracy of Existing Technique (in % age) | Accuracy of Proposed Technique (in %age) |
|---|---|---|
| 1 | 80.81739 | 96.88250 |
| 2 | 82.36294 | 95.84333 |
| 3 | 84.39600 | 96.37958 |
| 4 | 83.96592 | 94.47167 |
| 5 | 82.07947 | 95.60750 |
| 6 | 82.55758 | 96.46833 |
| 7 | 8613078 | 95.49500 |
| 8 | 86.67281 | 95.44792 |
| 9 | 83.92367 | 96.60083 |
| 10 | 81.52806 | 93.59333 |

From the given graph, we can easily compare the Accuracy difference between the existing and proposed technique. From the graph, it is clear that proposed technique is more accurate as compare to the existing technique.

Graph 2: Comparison of Accuracy




**3) False Positive Rate:**

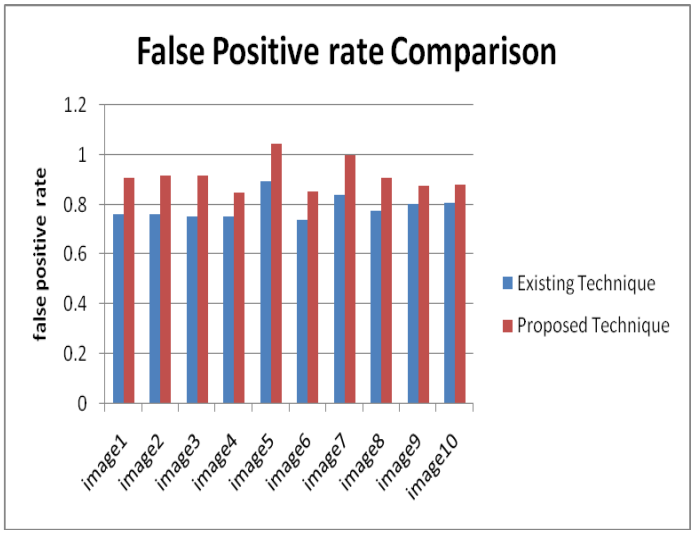
It is the value of prediction which classifier correctly predicted.

Table 3: difference between False Positive Rate of existing and proposed technique

| Image Number | False Positive Rate of Existing Technique | False Positive Rate of Proposed Technique |
|---|---|---|
| 1 | 0.76337 | 0.90932 |
| 2 | 0.76397 | 0.91858 |
| 3 | 0.75379 | 0.91632 |
| 4 | 0.75100 | 0.84895 |
| 5 | 0.89260 | 1.04603 |
| 6 | 0.73881 | 0.85374 |
| 7 | 0.83913 | 0.99709 |
| 8 | 0.77515 | 0.90944 |
| 9 | 0.80079 | 0.87788 |
| 10 | 0.80742 | 0.87869 |

As shown in graph 3, the proposed and existing algorithms are compared with false positive rate. In existing technique the SVM classifier was applied to classify the features. The SVM classifier has less false positive rate because it use only two classes to classify the features. In the proposed algorithm KNN classifier is used which can classify the features more than two classes due to which it has more false positive rate as compared to SVM classifier.

Graph 3: Variation in False positive Rate




**4) False Negative Rate:**

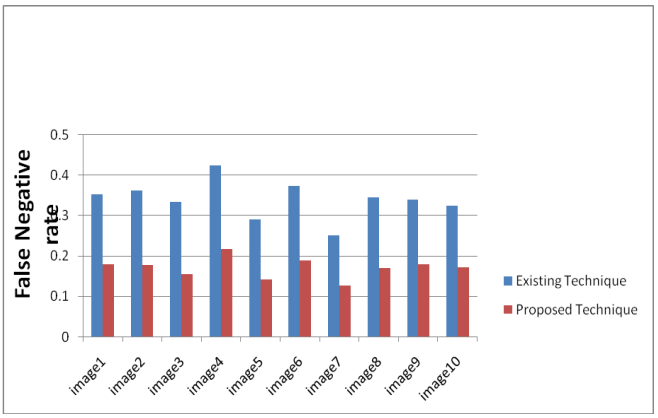
It is the parameter which gave the values wrongly predicted.

Table 4: Difference between False Negative Rate of existing and proposed Technique

| Image Number | False Negative Rate of Existing Technique | False Negative Rate of Proposed Technique |
|---|---|---|
| 1 | 0.35230 | 0.1788 |
| 2 | 0.36243 | 0.17736 |
| 3 | 0.33355 | 0.15524 |
| 4 | 0.40288 | 0.21636 |
| 5 | 0.29014 | 0.14075 |
| 6 | 0.37396 | 0.18841 |
| 7 | 0.25041 | 0.12682 |
| 8 | 0.34575 | 0.17001 |
| 9 | 0.33949 | 0.17841 |
| 10 | 0.32414 | 0.17184 |

As shown in table 4, the difference between false negative rate is done between proposed & existing algorithm. False negative rate is the parameter which gave the values wrongly predicted. In the proposed algorithm, the KNN classifier is applied which classify features more than two classes due to which false negative rate is less as compared to proposed algorithm in which SVM classifier is applied.

Graph 4: Comparison of False Negative Rate




As shown in graph 4, the difference between false negative rate is done between proposed & existing algorithm. The false negative rate is the parameter which gave the values wrongly predicted. In the proposed algorithm, the KNN classifier is applied which classify features more than two classes due to which false negative rate is less as compared to proposed algorithm in which SVM classifier is applied.

## V.CONCLUSION

Face spoof technique is technique which will detect the faces which are spoofed to take un-authorized access. I have taken two databases trained database and testing database.Trained database contain the images of genuine faces and the test database contain the spoofed images. The DCT technique is been which will detect the textual features from the input. In the existing algorithm SVM classifier is applied which classify spoofed and non-spoofed faces.In this work, it is been concluded that to classify approximate equal classifiers the KNN classifier will be applied for the classification.The results are analyzed by accuracy, execution time, false negative rate and false positive rate.It is been analyzed that accuracy is increased and execution time is reduced and FPR increased and FNR is reduced in proposed technique.

## VI. FUTURE WORK

Some new directions of research in the field of face spoof detection are not yet fully explored.

1. The proposed algorithm is based on the KNN classifier for the face spoof detection. In future to analyze reliability of the algorithm it can be compared with other classifiers
2. The proposed algorithm can be replaced with the decision tree classifier for the deep feature analysis.

## VII. REFERENCES

[1]. Rubeena Mirza, Vinti Nanda, "Paper Currency Verification System Based on Characteristic Extraction Using Image Processing", 2012, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 –8958, Volume-1, Issue-3

[2]. Vipin Kumar Jain, Dr. Ritu Vijay, "Indian Currency Denomination Identification Using Image Processing Technique", 2013, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (1), 126 – 12

[3]. Priyanka Sharma Manavjeet Kaur, "Classification in Pattern Recognition: A Review", 2013, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4

[4]. Jie Liu, Jigui Sun, Shengsheng Wang, "Pattern Recognition: An overview", 2006, IJCSNS International Journal of Computer Science and Network Security, vol. 6, no. 6

[5]. W. Bao, H. Li, N. Li, and W. Jiang, "A liveness detection method for face recognition based on optical flow field", 2009, IEEE IASP, pages 233–236

[6]. M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, D. Muntoni, G. Fadda, M. Pili, N. Sirena, G. Murgia, M. Ristori, F. Roli, J. Yan, D. Yi, Z. Lei, Z. Zhang, S. Li, W. R. Schwartz, A. Rocha, H. Pedrini, J. Lorenzo-Navarro, M. CastrillonSantana, and J. Maatta, "Competition on Counter Measures to 2D Facial Spoofing Attacks", 2011, IJCB

[7]. C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines", 2011, ACM TIST, 2

[8]. N. Dalal and B. Triggs, "Histograms of Oriented Gradients for Human Detection", 2005, IEEE CVPR, pages 886–893

[9]. T. Fladsrud, "Face recognition in a border control environment: Non-zero effort attacks 'effect on false acceptance rate'", 2005, Msc. thesis, Gjovik Univ. College, Norway

[10]. Reshma Rajan and Ani Sunny, "Detecting Face Spoof Using IDA Features and Colour Texture Analysis", 2017, International Science Press Volume 10

[11]. Saptarshi Chakraborty and Dhrubajyoti Das, "An overview of face liveliness detection", 2014, International Journal on Information Theory (IJIT), Vol.3, No.2

[12]. Ye Tian and Shijun Xiang, "Detection of Video-Based Face Spoofing Using LBP and Multiscale DCT", 2016, Springer International Publishing AG, IWDW LNCS 10082, pp. 16–28

[13]. Azeddine Benlamoudi, Djamel Samai, Abdelkrim Ouafi, Salah Eddine Bekhouche, Abdelmalik Taleb-Ahmed, "Face spoofing detection using Local binary patterns and Fisher Score", 2015, Research gate publications .

[14]. Roberto Tronci, Daniele Muntoni, Gianluca Fadda, Maurizio Pili, Nicola Sirena, Gabriele Murgia, Marco Ristori, "Fusion of multiple clues for photo-attack detection in face recognition systems", 2011, Research gate publications