Approach for Face Spoof Detection Using KNN classifier

Sakshi Jha[1], Dr. Neetu Sharma[2]

[1]M.Tech. Scholar, [2]Associate Professor
Computer Science & Engineering,
Ganga Institute of Technology and Management Kablana,
Jhajjar, Haryana, India

***Abstract*: In order to classify the spoofed as well as non-spoofed faces from images, the face spoof detection technique has been proposed. In order to analyze the textual features present within a test image, the DWT algorithm is applied. In order to classify the spoofed and non-spoofed features, the already existing approach used SVM classifier. However, the accuracy of results needs to be enhanced in the proposed work in order to identify the spoofed daces. In order to analyze the proposed approach, comparisons are made amongst the proposed and existing mechanisms in terms of accuracy and execution time.**

Index Terms - Face spoof detection, SVM, KNN, DWT

I. INTRODUCTION

Within several mobile technologies, the major issue that arises while accessing information is the security of private data. In order to provide authentication to users, passwords have been used since many years so that no external user can access the data. However, the effectiveness of the passwords can be compromised due to several usability and security concerns. The passwords generated by users are used sometimes on other accounts and services as well. Due to this reason it is easy to crack or get access to the passwords. The proper utilization and maintenance of systems becomes difficult due to the higher numbers of accounts and passwords involved [1]. Thus, the stolen accounts and passwords are often found in news and reports. As the mobile devices are easy to be lost or stolen, this problem mainly arises within them. However, there are many new authentication options provided within these mobile devices which are now helping in increasing the levels of security for users. The technologies that measure and analyze the characteristic properties of human body are known as biometrics. The physical characteristics as well as the activity characteristics are the two broader classifications of biometrics traits. Fingerprints, iris or facial patterns etc. are known to the physical characteristics and voice signature or the strolling patterns are known as activity characteristics [2]. The chances of fraud which is also known as a spoofing attack is the major challenge that is found within these systems. In order to realize the unauthorized access to the biometric system without any consent of real user, the exploitation and copying of stolen data by the attackers is done. Completely different views are generated during the examination of features when spoofing attack occurs in the system. There is a need to make choice related to limited number of frames when the real-time response of face spoof detection is to be applied within the mobile applications [3]. In order to differentiate amongst genuine and spoof faces on the basis of solitary casing, discriminative features that are appropriate are to be designed here. For instance, a scenario is presented in which a genuine or a spoof face is presented to a camera in order to generate scenario for comparing images. The shape as well as the properties of facial surface present before the camera are the two major differences found amongst genuine and spoof face images. Within the face spoof images, there is a possibility that some exceptional distortions are available such as the geometric distortion and the artificial texture patterns. Thus, the camera and illumination subordinates are major reasons for these distortions. A perfect camera for instance must be utilized in order to notice the difference amongst geometric distortion and the illumination as well as depiction of artificial texture [4]. Thus, lately the face spoof images concentrate on more than the four common sources and the relevant features are then further designed. The full-reference methods such as Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR) and Signal-to-Noise Ratio (SNR) are the commonly known assessment algorithms that are utilized in order to measure the quality of an image. The extraction of parameters is done and then the Neural Network Classifier is provided with these parameters. Whether an image is spoofed or genuine, it can be identified through this classifier. In order to recognize the quality of test input, the accessibility of a clean distortion free image is needed within full-reference IQA [5]. However, there is no need of a reference image is order to decide the quality of an image in case of non-reference IQA. Amongst several problems arising within image processing, image distortion is a major issue. As per the illumination and quality of camera, there is difference in distortion. The four features which are specular reflection, blurriness, chromaticity, and shading diversity are considered in order to identify the image distortion within the face spoof images. Several classifiers are utilized within this research work. K-Nearest Neighbors is the classifier in which on the basis of distance or similarity function for pairs of observations the case-based learning algorithm generated. A module classified generated within the priori probability as well as the class conditional probability is known as Naïve bias classier. The probability that a document D belongs to class C is calculated in this method. In order to perform text classification, a decision tree is used in which the terms are labeled through the internal nodes of the tree, the test on weight is labeled through the branches that are being generated from the

tree and the relevant class labels are denoted by the leaf node [6]. In order to classify the documents as per their annotated categories, the rule-based inference is utilized by decision rules classification mechanism. In order to perform text classification, another approach proposed is known as Support vector machine (SVM) method. Both positive as well as negative training sets that are uncommon for other classification techniques are required within SVM.

II. LITERATURE REVIEW

Alireza Sepas-Moghaddam, et.al (2018) presented a mechanism for spoofing attacks detection. A novel approach is proposed here which is known as the IST Lenslet Light Field Face Spoofing Database (IST LLFFSD) in order to detect face spoofing attacks [7]. On the basis of compact however effective descriptor that exploits the color and texture variations that are related to several directions of light that is capture within light field images, a novel spoofing attack detection solution is proposed by this study. In order to evaluate the performance of proposed mechanism, several experimental simulations have been performed and it is seen that the face spoofing attack types can be identified successfully through this proposed mechanism.

Shervin Rahimzadeh Arashloo, et.al (2017) proposed a novel and more realistic spoof detection mechanism on the basis of anomaly detection concept [8]. In order to handle the unseen attack types, a new evaluation protocol has also been proposed here. Towards the end, using common spatio-temporal and image quality features, a detailed evaluation as well as comparison of 20 several types of one-class and two-class systems was performed. The anomaly-based formulation performed better in comparison to the conventional two-class approach as per the results achieved through simulations.

Muhammad Asim, et.al (2017) proposed in this paper a novel anti-spoofing technique on the basis of spatio-temporal information [9]. Here, the legitimate access and the impostor videos also known as video sequences for the image attacks were differentiate through this method. In order to extract the spatio-features from the video sequences as well as to capture the most discriminative clues amongst the genuine access and the impostor attacks, the LBP-TOP mechanism is cascaded with CNN. Upon two very challenging datasets that are CASIA and REPLAY-ATTACK, extensive experiments are performed. As per the simulation results, very high competitive results have been achieved and it is seen that the proposed scheme outperforms existing approaches.

Xudong Sun, et.al (2016) proposed near-infrared differential (NIRD) images using the controllable active near-infrared (NIR) lights [10]. There is huge lighting difference amongst the images that include active NIR lights and images that do not include active NIR lights within the NIRD image that is based on reflection model. The pixel consistency amongst the face as well as non-face regions is analyzed and in order to identify the spoofing images, the context clues are employed. Further, in order to identify the spoofing attacks of the medium that is cropped on purpose the lighting feature that is extracted from the face regions. A face spoofing detection mechanism is proposed here in order to merge the two features mentioned. As per the experiments conducted and simulation results achieved it is seen that the proposed mechanism provides accurate and robust results.

Gustavo Botelho de Souza, et.al (2017) proposed two LBP-based Convolutional Neural Networks which are namely LBPnet and n-LBPnet within the face recognition systems in order to detect spoofing [11]. Upon the NUAA spoofing dataset, efficient results have been presented which showed that in comparison to other existing approaches, the proposed technique performed better. In comparison to other approaches that integrate huge amount of handcrafter information for identifying the attacks, the proposed approaches have provided efficient results. Thus, the deep texture features are concluded to be rich sources of information in order to perform face spoof detection as per these outcomes. A suitable and robust alternative is thus introduced as an alternative for preventing spoofing attacks by integrating the LPB descriptor with the deep learning architecture.

Yaman AKBULUT, et.al (2017) proposed a deep learning-based face spoof detection mechanism on the basis of (LRF)-ELM and CNN which are two different deep learning models [12]. There are also higher numbers of completely connected layers present within the CNN model. The proposed approach is evaluated by several simulations performed on two face spoof detection databases which are NUAA and CASIA. Several results achieved were compared with the already existing approaches and it was seen that the proposed approach provided better results in comparison to already existing techniques.

III. RESEARCH METHODOLOGY

For the classification of face spoofing, KNN classifier has been utilized in this work. The training samples are represented by n dimensional numeric attributes in the KNN classifier. A point in an n-dimensional space is represented by every sample. In the n-dimensional pattern space, the greater part of the training samples is stored. In case an unknown sample is given, the k-nearest neighbor classifier match with the k training samples and choose that pattern space which is closest to the unknown sample. Euclidean distance defined the term "closeness". Nearest neighbor classifiers assigned break even with weight to every attribute unlike the decision tree. But this condition leads to confusion when large amount of irrelevant attributes are present within the data. For the prediction purpose, nearest neighbor classifiers has been utilized in order to present a genuine valued prediction for a given unknown sample. In this case, the average value of the genuine valued associated with the k nearest neighbors of the unknown sample is given back by the classifier. In the machine learning algorithm, the k-nearest neighbors' algorithm is considered as the

simplest method among all. The DWT algorithm will be utilized for the analysis of features associated with a test image. KNN classifier will be applied on the detected features in order to classify whether the face is spoofed or non-spoofed.

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(Xi,x)

End for

4. Compute set I containing indices for the k smallest distance d(Xix)

Return majority lable for (Yi where i belongs to I}

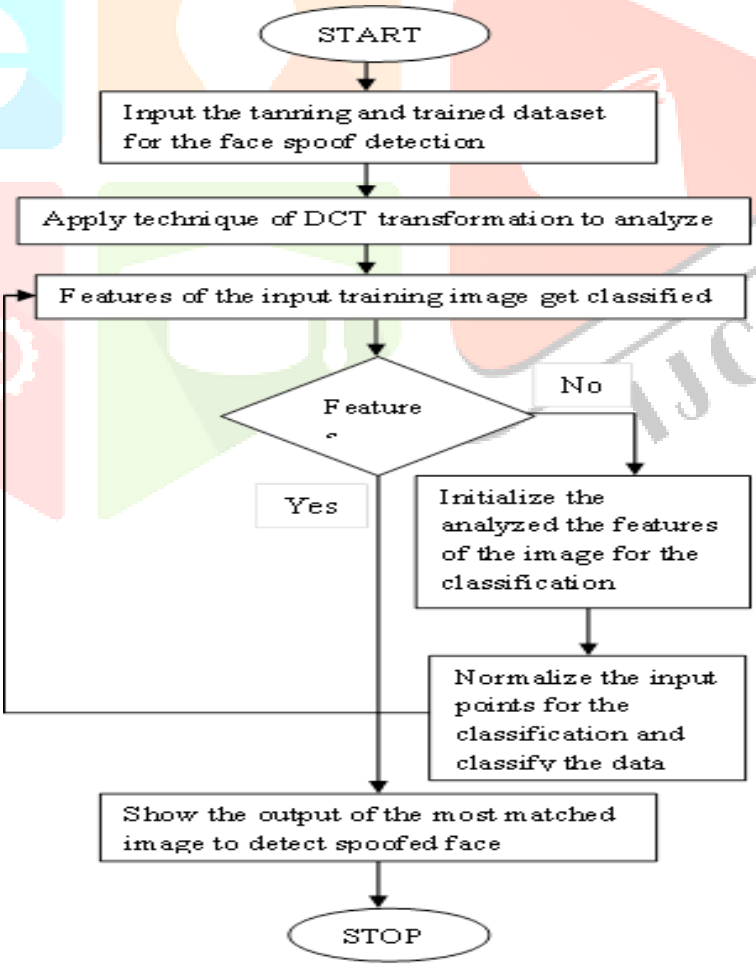

Fig 1: Proposed Flowchart

IV. EXPERIMENTAL RESULTS

The proposed technique has been implemented in MATLAB and the results are compared with already existing technique in terms of accuracy and execution time such that the performance of this proposed algorithm can be evaluated.

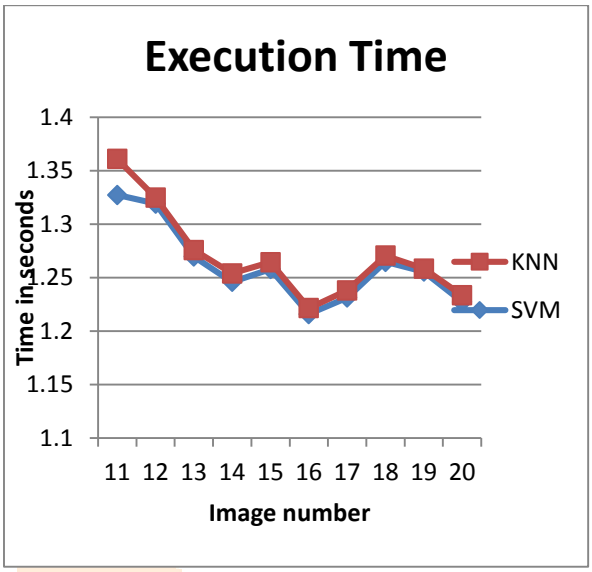

Fig 2: Execution Time

As shown in figure 2, comparisons are made amongst the proposed KNN classification approach as well as the already existing SVM classification approach in terms of the execution time. As per the results achieved it is seen that in comparison to SVM classification approach, there is minimization of execution time within the KNN classification approach.

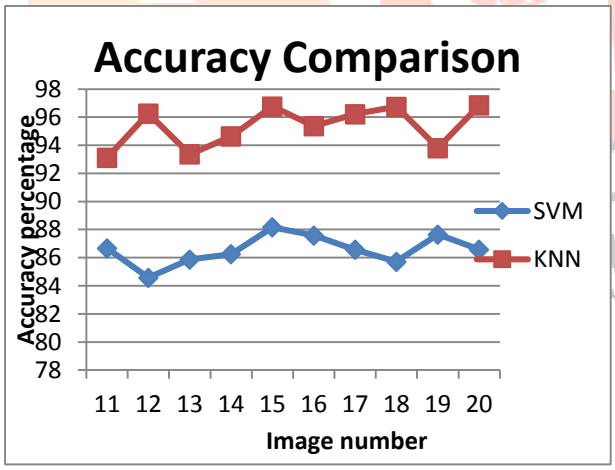

Fig 3: Accuracy Comparison

As shown in figure 3, comparisons are made amongst the proposed KNN approach and SVM based face spoof detection approach in terms of accuracy. As per the analysis, it is seen that the accuracy if proposed KNN approach has accuracy for face spoof detection than previous approach.

V. CONCLUSION AND FUTURE SCOPE

In order to identify the spoofed faces that are added due to unauthorized access to the data, the face spoof technique is proposed. In order to identify the textual features from input image, the DWT technique is utilized. For the classification of spoofed as well as non-spoofed faces, the already existing SVM classified is applied. As per the results achieved it is seen that the approximate equal classifiers can be classified by applying KNN classifier for performing classification in this proposed work. With respect to accuracy as well as execution time, the analysis of results has been done. As per the results achieved it is seen that there is increase in accuracy as well as decrease in execution time through the application of novel approach in the proposed work.

VI. ACKNOWLEDGEMENT

I would specially like to thanks my worthy guide **Dr.Neetu Sharma**, who supervised me to complete this research paper. Her technical advice, ideas and constructive criticism contributed to the success of this paper. She suggested me many ideas and solved my puzzles. Her motivation and help has been of great inspiration to me.

REFERENCES

[1] A. Bashashati, M. Fatourechi, R. K. Ward, and G. E. Birch, "A survey of signal processing algorithms in brainccomputer interfaces based on electrical brain signals," 2007, Journal of Neural Engineering, vol. 4, no. 2, pp. R32–R57

[2] C. Hou, F. Nie, C. Zhang, D. Yi, and Y. Wu, "Multiple rank multi-linear SVM for matrix data classification," 2014, Pattern Recognition, vol. 47, no. 1, pp. 454 – 469

[3] Y. Lin, F. Lv, S. Zhu, M. Yang, T. Cour, K. Yu, L. Cao, and T. Huang," Large-scale image classification: Fast feature extraction and svm training," 2011, IEEE CVPR, June pp. 1689–1696

[4] C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines," 2011, ACM Trans. Intell. Syst. Technol., vol. 2, no. 3, pp. 27:1–27

[5] S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, "Computationally efficient face spoofing detection with motion magnification," in Proc. CVPR Workshops, 2013, pp. 105–110.

[6] J. Komulainen, A. Hadid, and M. Pietik¨ainen, "Context based Face Anti- Spoofing," in Proc. BTAS, 2013, pp. 1–8

[7] Alireza Sepas-Moghaddam, Luis Malhadas, Paulo Lobato Correia, Fernando Pereira, "Face spoofing detection using a light field imaging framework", 2018, IET Biometrics, 2018, Vol. 7 Iss. 1, pp. 39-48

[8] Shervin Rahimzadeh Arashloo, Josef Kittler, "An Anomaly Detection Approach to Face Spoofing Detection: A New Formulation and Evaluation Protocol", 2017, IEEE

[9] Muhammad Asim, Zhu Ming, Muhammad Yaqoob Javed, "CNN Based Spatio-temporal Feature Extraction for Face Anti-spoofing", 2017 2nd International Conference on Image, Vision and Computing

[10] Xudong Sun, Lei Huang and Changping Liu, "Context Based Face Spoofing Detection Using Active Near-Infrared Images", 2016 23rd International Conference on Pattern Recognition (ICPR)

[11] Gustavo Botelho de Souza, Daniel Felipe da Silva Santos, Rafael Gonçalves Pires, Aparecido Nilceu Marana, and João Paulo Papa, "Deep Texture Features for Robust Face Spoofing Detection", 2017, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—II: EXPRESS BRIEFS, VOL. 64, NO. 12

[12] Yaman AKBULUT, Abdulkadir SENGÜR, Ümit BUDAK, Sami EKICI, "Deep Learning based Face Liveness Detection in Videos", 2017, IEEE