Face Spoof Detection Using Machine Learning

Megha
Research Scholar
Meghapurva94@gmail.com
Govt Engineering Collage of Bikaner
Rajasthan

Dhanroop Mal
Assistant Professoor
Drm_nagar07@yahoo.com
Govt Engineering Collage of Bikaner
Rajasthan

Deepak Singh
Assistant Professor
deepakdotmail@rediffmail.com
Govt Engineering Collage of Bikaner
Rajasthan

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. 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. The effect of noise present on classification is minimized by larger values of k. However, there is less distinct boundary generated amongst the classes. The traditional KNN mechanism is enhanced by using several K-values of various classes in order to overcome such drawbacks. The WKNN mechanism is utilized in order to enhance the performance of KNN. In order to analyze the proposed approach, comparisons are made amongst the proposed and existing mechanisms in terms of accuracy and execution time.

Keywords - Face spoof, KNN, SVM

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. 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. Within several applications that mainly include mobile unlocking, there has been an increase in demand of automatic face recognition systems. For mobile phones, face recognition has become another biometric identification technique which is similar to Touch ID that includes fingerprint authentication within iOS systems [1]. Within the Android mobile operating system package, the mobile phone is unlocked using face. As each advanced mobile these days is equipped with a front end camera these days, the face recognition systems do not need any detector further. However, mainly in free police investigations as well as uncooperative subject cases, some concerns related to face parody assaults related to face recognition systems arise here as well. Even though there are some similarities found amongst faces, there are minute differences found in age, skin, color and gender due to which the faces cannot be copied exactly in very easy manner.

There are four broader classifications generated on the basis of various cues involved as vicinity of face spoof detection which are:

i. Motion based methods: An important sign for vitality that includes subconscious motion of any of the organs or muscles present within a live face is identified in order to catch the printed photo attacks within these methods [4]. The movements such as blinking of eye, mouth development as well as rotation of head are some of the examples of movements that are caught here.

ii. Texture based methods: In order to extract image artifacts within the spoof face images such that the attacks within printed photo and replayed videos can be identified, most of the texture based methods are projected. Only a single image is required in order to identify a spoof within these texture based methods which is completely opposite to that of motion based approach.

iii. Methods based on image quality analysis: An example of this mechanism can be given by a biometric physiological property detection mechanism for iris, in which 25 image quality measures, 21 full-reference measures as well as 4 non-reference measures were utilized for identifying distinctive mark and face images. The speculation ability within the cross-database objects is boosted by the projected approach as per the quality through this method.

iv. Methods based on other cues: The projection of certain cues such as spoofing context, voice, IR image etc. from sources is used for identifying the face spoof. Additional requirements are imposed by these systems upon the face recognition systems due to which there application has been minimized.

The steps followed within analysis of image distortion are explained below:

a. There are many unadulterated white specular components present after the standardization of an image is done. Through the shifting of chromaticity value of pixels along with holding of their shade, a specular free image can be generated. There are specular as well as diffused components present within an image [12]. Due to the maximum chromaticity, there is constant localization of diffused pixels at the right half of specular pixels. There is constant chromaticity of diffused points here along with the shifting of specular points. Until the point where no specular components are left within an image is achieved, the specular components are eliminated with each step in an iterative manner by assuming the termination condition as an important part. On the basis of chromaticity value of specular and diffused pixels, the Specular technique is utilized as a diffusive mechanism. Within the MSU database, the specular reflection features are calculated for both genuine as well as spoofed face image of a subject. In order to ensure that the proposed technique works in appropriate manner upon the provided training dataset, the classifier needs to be trained in the initial step on the training dataset. Further, the specular reflection feature is utilized in order to perform the final testing upon the test dataset such that the performance can be enhanced [13].

b. Blurriness Features: Within the mobile telephone cameras, there defocusing of spoofed faces when shorter distance of spoof attacks are generated. The image becomes obscure because of the limited size of spoofing medium. Further, for identifying other spoofed faces, this obtained image can be used as a clue. Initially, the image is taken as input and its obscure version is identified. In order to recognize the difference between the image given for detection and an identical image that has obscured shape is known as blurriness. The amount of blurriness present within the initial input image is chosen by this difference calculated.

c. Chromatic Moment Features: The face detection and standardization is performed at the initial step here. Further, the image is transformed from RGB format to the HSV format. In the next step, the mean, deviation as well as the skewness is calculated. With respect to the three statistical moments, there three features are found to be similar and are also known as the chromatic moment features.

d. Shading Diversity Features: With respect to the colors, there is great appearance found for the genuine faces. The shading reduction is generated due to this diversity. The shading quantization technique is used here for shading reduction. Here, the transformation of input image into an indexed shading image is done. The histogram counts and the number of distinct colors being seen within a normalized image are the two estimations that are made within the shading distribution.

II. LITERATURE REVIEW

Alireza Sepas-Moghaddam, et.al (2018) presented in this paper that there is a huge increase in demand of the face recognition systems. However, there are several spoofing attacks also identified within these applications [24]. In order to present a mechanism for spoofing attack detection, there are several light field cameras utilized lately. 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. Within the approach, there are 100 genuine images involved, amongst which a Lytro ILLUM lenslet light field camera is used to capture 50 subjects and the same camera is used to gather a set of 600 face spoofing attack images. Along with the printed paper, wrapped printed paper, laptop, tablet as well as two separate mobile phones, there are six different types of presentation attacks simulated within IST LLFFSD. 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) presented in this paper that along with the small sample size within the face spoofing issue, the issues of imaging sensor inter-operability and other environment factors might arise due to the presence of spoofing attackers within the systems [25]. Thus, several propositions have been proposed in order to solve these issues. On the basis of anomaly detection concept, a novel and more realistic spoof detection mechanism is formulated here in this paper. 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 [26]. 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 perform feature extraction and train the classifier, the convolutional neural network (CNN) was used along with the handcrafter technique such as LBP-TOP. The preprocessing steps like face detection and refining face regions or enlargement of the original images using specific rescaling ratios is not required within this proposed approach. The temporal features cannot be learned on own by the CNN approach. However, the spatio-temporal features are important for face-spoofing here. 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 [27]. 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. In order to perform spoofing detection, there are two major characteristics presented depending on the NIRD images. Initially, it is obvious that there is spoofing media present around the faces due to which the incident lights are reflected in the similar manner as the areas of face reflect. 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 [28]. Upon the NUAA spoofing dataset, efficient results have been presented which showed that in comparison to other existing approaches, the proposed technique performed better. Within the real face recognition applications being utilized lately, the effective alternatives for detecting spoofs are configured through the proposing of LBPnet and n-LBPnet networks as they provide the highest ROC curves and accuracy as well as low EER. 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 [29]. Before the completely connected layer, a convolution and pooling layer is generated within the LRF-ELM model.

Due to this enhancement, the speed of processing within the model becomes faster. A series of convolution and pooling layers is present however, within CNN approach. 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

The face spoof detection has been widely utilized nowadays for the detection of face spoofing information due to which unauthorized access is prevented in the bio-matrix system. Previously, the detection of face spoofing was done using SVM classification technique. The DWT algorithm was utilized for the analysis of textual features of the test image for the detection of face spoofing in the existing systems. In the classification, textural features act like the training set. The obtained result from the SVM classification distinguishes the test image whether it is a spoofed or non-spoofed face. In the detection process, the accuracy of SVM classification is reduced in some cases as there is similarity between the textual features of the spoofed image and to the original image. 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 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,.....K_n] according to equation given in step 4

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

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

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. RESULT AND DISCUSSION

MATLAB stands for matrix-laboratory. It is a software package which is used to perform numerical computations that are complex in nature. "C" language has been utilized as the programming language in the MATLAB. It has various inbuilt functions that upgraded from version to version. These in-built functions are Image processing, neural networks, GUI, graphics and animation, communications, control system and many more. For the implementation of algorithms, plotting graphs and design user interfaces MATLAB is widely used.

Fig 1: Execution Time

As shown in figure 1, 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.

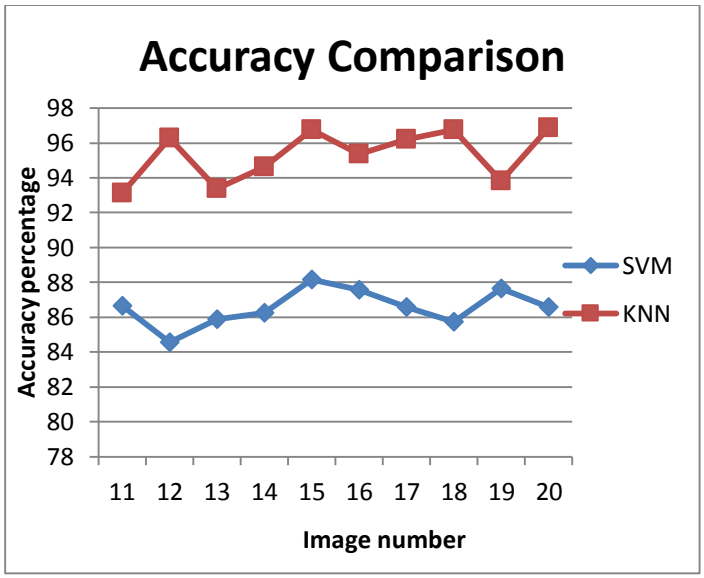

Fig 2: Accuracy Comparison

As shown in figure 2, 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

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. REFERENCES

[1] Q. Yang, S. Wang, and N. Ahuja, "Real-time specular highlight removal using bilateral filtering," 2010, ECCV, pp. 87–100

[2] V. Christlein, C. Riess, E. Angelopoulou, G. Evangelopoulos, and I. Kakadiaris, "The impact of specular highlights on 3D-2D face recognition," 2013, SPIE

[3] R. Tan and K. Ikeuchi, "Separating reflection components of textured surfaces using a single image," 2005, IEEE Trans. Pattern Anal. Mach. Intell., vol. 27, no. 2, pp. 178–193

[4] J.-F. Lalonde, A. A. Efros, and S. G. Narasimhan, "Estimating the natural illumination conditions from a single outdoor image," 2011, Int. J. Comput. Vision, vol. 98, no. 2, pp. 123 – 145

[5] H. Han, S. Shan, X. Chen, S. Lao, and W. Gao," Separability oriented preprocessing for illumination-insensitive face recognition," 2012, ECCV, pp. 307–320

[6] X. Gao, T.-T. Ng, B. Qiu, and S.-F. Chang, "Single-view recaptured image detection based on physics-based features," 2010, ICME, pp. 1469–1474

[7] F. Crete, T. Dolmiere, P. Ladret, and M. Nicolas, "The blur effect: perception and estimation with a new no-reference perceptual blur metric," 2007, SPIE: Human Vision and Electronic Imaging XII

[8] P. Marziliano, F. Dufaux, S. Winkler, and T. Ebrahimi, "A no-reference perceptual blur metric," 2002, ICIP, vol. 3, pp. 57–60

[9] Y. Chen, Z. Li, M. Li, and W.-Y. Ma, "Automatic classification of photographs and graphics," 2006, ICME, pp. 973–976

[10] B. E. Boser, I. M. Guyon, and V. N. Vapnik, "A training algorithm for optimal margin classifiers," 1992, 5th ACM Workshop on Computational Learning Theory, pp. 144–152

[11] 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

[12] 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

[13] 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

[14] 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

[15] 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.

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

[17] L. Best-Rowden, H. Han, C. Otto, B. Klare, and A. K. Jain, "Unconstrained face recognition: Identifying a person of interest from a media collection," 2014, IEEE Trans. Inf. Forensics Security, vol. 9, no. 12, pp. 2144–2157

[18] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in Proc. IEEE BIOSIG, 2012, pp.1–7

[19] T. de Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel," LBP-TOP based countermeasure against face spoofing attacks," in Proc. ACCV Workshops, 2012, pp. 121–132

[20] N. Erdogmus and S. Marcel, "Spoofing in 2D face recognition with 3D masks and anti-spoofing with kinect," in Proc. IEEE BTAS, 2013, pp.1–6

[21] N. Evans, T. Kinnunen, and J. Yamagishi, "Spoofing and countermeasures for automatic speaker verification," in Proc. INTERSPEECH, 2013, pp. 925–929

[22] A. Rattani, N. Poh, and A. Ross, "Analysis of user-specific score characteristics for spoof biometric attacks," in Proc. CVPR Workshops, 2012, pp. 124–129

[23] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face antispoofing database with diverse attacks," in Proc. ICB, 2012, pp. 26–31

[24] 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

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

[26] 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

[27] 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)

[28] 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

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