Biometric Face Anti-Spoofing And Context Based Detection Techniques : A Review

Karuna Grover
ME Student (ECE)
NITTTR Chandigarh, India

Rajesh Mehra
Joint Professor
NITTTR Chandigarh, India.

***Abstract*:- The biometric technology has shown various developments in the recent times specially in case of face and fingerprint recognition. The path of technological evolution is addressed to external attacks particular to spoofing. Spoofing is referred as presentation through biometric technology. Biometric is convenient technique for identification of people. Face spoofing is problem faced in authentication system. Spoof attacks include replay attack and printed paper attacks includes printed photo of the authenticated user. Facial biometrics is based on spoofing detection which is highly prone to spoofing attacks. Scene detection may either be positive and negative class includes spoofed faces on pictures, videos. Detection influenced by picture quality and lighting.The security issues in face recognition, due to various environmental factors and 3D masks are major threats. In this review paper, the different methods and techniques has been developed for detection of face spoofing.The accuracy of the face recognition can be improved by obtaining more face images from the same person.**

Keywords:- Biometric, Face Spoofing, Spoof Attacks and Security Issues.

I. INTRODUCTION

Biometrics is scientific and technological authentication method based on biological factor and basically used in information assurance. Biometric authentication determines the secure and biological information such as Fingerprint, DNA, Voice Wave, Face, Gestures, Patterns and Signatures.The biometric technology has arised an improvement in biometric technology with the improvements in recognition of the face. In biometric technology with new issues and challenges, biometric system also works on against the external threats.The growing factor of biometric in different environments like as mobile phones and medical fields. The users are more familiar with the use of this technology, and also concerned about the security weakness of this system.Nowadays, users can easily find videos in web-site and about the creation of the fake masks, fingerprints and iris which are used to fool biometric systems.There are more attacks in theoretical andacademic spheres.

Fig 1. Biometric Authentication Traits

Now, an easy hacking of long anticipated new iphone 5s fingerprint reader,using a finger prints spoof is an example of the practical attacks and well-known type of attacks in biometric systems.The research has focused on the spoofing attacks, spoofing is a biometric vulnerability where synthetically produced artefact (e.g., face mask, gummy finger or printed iris image) or try to mimic the behaviour of genuine users (e.g., gait, signature), to fraudulently access the biometric system. The biometric traits used to classify texture based analysis. In this method the assumption of skin texture of face is done which is different from fake faces. Local binary pattern (LBP) method used to analyse texture pattern of face. Spoofing attacks mainly done by photos and 3D face mask. The limitation texture based anti-spoofing method is to input the image exactly, as the live image[2].

Spoofing is an un-authorised access to system of a user by pretending it to be in use. A spoofing attack is an attempt to use privileges of other user by using a photo, video for authorized face of a person. Along with face recognition, texture plays vital role in detection of face spoofing. In face spoofing technique the texture features extracted from images in order to detect the fake face. The local binary pattern is used to detect the texture image [1]. Anti-spoofing is method used to distinguish between authentic user and fake trait. The measures against spoofing can be classified into several categories such as texture based analysis and reflectance based analysis. The lips movement and blinking of eyes used for detecting fake faces.

Fig 2. Original frame of face spoofing

Face spoofing is kind of the attack occurs when fake sample of the face of the valid users preent to acquisition sensor.The types of the attacks consist of different types which are photo attack, video attack and masks attack.The recorded video of the valid users based on the face used as fake sample which increases the chance of insecurity.The attacker represents the fake photo to acquiston sensor. The attacker wears the masks of the face of the user in masks attacks.

II. RELATED WORK

Gustavo Botelho de Souza et.al., 2017 [4] suggested two LBP-based Convolutional Neural Networks, LBP net and n-LBP net. It works with high-level (deep) texture features instead of handcrafted ones. Many metrics used in different works over the NUAA dataset were calculated, such as the ROC (Receiver Operating Characteristic) curve, Accuracy rate and HTER (Half-Total Error Rate). The integration of the LBP descriptor in a deep learning architecture is a suitable and robust alternative to prevent such criminal activities as it gives maximum accuracy in comparison to other state-of-the-art techniques. ***Lei Li et.al.,2018 [5]*** discussed a comprehensive overview of the recent advances in face anti-spoofing state-of-the-art, discussing existing methodologies, available benchmarking databases, reported results and, more importantly, the open issues and future research directions. Additionally, and in contrast with previously available surveys, also an example of a promising approach to PAD was described, explaining the different problems that can be encountered in the experimental analysis. The importance of PAD evaluation using public databases and following the defined protocols for allowing a fair comparison against the state-of-the-art techniques was stressed. The results of the experimental work, using the CASIA face anti-spoofing and Replay-Attack databases have clearly shown the advantage of including colour information, rather than only grey-scale images, when developing a face a spoofing attack countermeasure***. Menotti et al.,2015 [6]*** have investigated two deep representation research approaches for detecting spoofing in different biometric modalities. In the first one, they approached the problem by learning representations directly from the data through architecture optimization with a final decision-making step atop the representations. In the second approach, filter weights are trained for a given architecture using the well-known back propagation algorithm. The results strongly indicate that spoofing detection systems based on convolutional networks can be robust to attacks already known and possibly adapted, with little effort, to image-based attacks. ***S. R. Arashloo et.al.,2015 [7]*** proposed multiscale dynamic texture descriptor based on binarized statistical image features on three orthogonal planes (MBSIF-TOP). Also, by combining MBSIF-TOP with a blur tolerant descriptor, namely the dynamic multiscale local phase quantization representation (MLPQ-TOP), the robustness of the spoofing attack detector can be further improved. The fusion of the information provided by MBSIF-TOP and MLPQ-TOP is realized via a kernel fusion approach based on a fast kernel discriminant analysis (KDA) technique. The fused system has been demonstrated to outperform the state of the art face spoofing detection systems in most of the benchmarking tests adopted by the research community. ***Zhibin Pan et al.,2017[8]*** discussed an effective diamond sampling structure to decrease the feature dimensionality significantly by fixing the number of sampling neighbours to a constant of 8. A simple and new average method on the radial direction is used to enhance the noise-robustness. An effective adaptive quantization threshold strategy is proposed to restore the noise-corrupted non-uniform patterns back to possible uniform patterns. DLABP method significantly outperforms other related state-of-the-art methods both in noise-free and high level noise conditions. Hence, DLABP is more robust and discriminative meanwhile with the advantage of low feature dimensionality.

III. CONTEXT BASED FACE SPOOFING DETECTION

In this technique the fake faces are detected by using descriptors. The face and the upper half of the body is analysed by using the descriptor. A specific detector used to determine fake input image and the input face image determine a spoofing medium detector afer that the medium input the spoofed image [13].

3.1 Spectra Fourier Analysis :-This method focus on the detection of the sample of the spoofed images. The high frequency of the fake image should be less than the real image. The frequency of the deviation of the image should be small. If the median of the image is small than the threshold then the input image is the sample of the spoofed image[14].

3.2 Spoofing detection on Visual Dynamics :-The dynamic mode algorithm is used to transform sequences of the videos to corresponding image sequence. The extract features for each sequnace of the image use local binary histogram and local binary pattern gives final classification input [15].

3.3 Shape and texture Analysis :-This method adopted the powerful features about the gabor and LBP wavelets describes the macroscopic information.The gradient orientation of the localised portion of the image have some local shape characterstics. The low level descriptor tranforms the data in to linear representation. The vector in SVM classifier combines the individual SVM ouputs for recognising a fake image or a live person in front the camera [16].

IV. UNIQUE FEATURE EXTRACTION TECHNIQUES

In the indirect attacks, criminals exchange internal messages in the system modules. The high majority of attacks to biometric systems are in the direct mode due to the simplicity for the attackers. So scoffing detection becomes a necessary approach. The different ways of spoofing detection are [9]:-

4.1 Local Binary Pattern(LBP):-This technique based on local texture pattern.the selected pixels converted into binary codes.the LBP working is described as under [10]:

The input image is divided into cells and then the center pixel is selected from each cell. After that compare selected pixels with the neighbours pixel.And then, replace the neighbour pixel with 0 if center ixel is more than neighbour pixel or with 1 if the center pixel is less than the neighbour pixel.finally,collect all replced neighbour pixel values and convert binary values to decimal values, which represents the center pixel selected from the cell.

4.2 Co-ocurrence of adjacent local binary patterns(Co ALBP):- CoALBP is local descriptor pattern method which extract the spatial data from the adjacent LBP in four directions.

4.3 Local Phase Quantisation(LPQ):- This technique use short term fourier transform(SIFT) for extraction of local phase information from main pixel.

4.4 Binary Statistical Image Features(BSIF):-This technique helps in sorting binary pattern for each pixel in an image .The numer of filter used for finding the pattern depnds length of pattern.

4.5 Reflection is specular:-The feature of this technique normalise illumination of face.The components of specular selection are seprated by this method.

4.6 Feature of blurriness:-The spoof faces are defocused so they are more chances of blurred image.The blurredness calculated differentiating the input image and blurred image.

4.7 Variations features:-This techniques helps in detecting images which are recaptured.The system unable to detect the color variation but human eye detect the variation of color between fake and original image.

4.8 Dynamic Mode Decomposition: - This mode applied on a set of frames and Eigen values is computed for the frames so dynamics modes are created. The single dynamic mode selection is done with phase angle 0 to the closest value.

V. VARIOUS APPROACHES IN FACE SPOOFING

Face spoofing detection can be done by various ways, using different descriptors. Some of the descriptors based on global approaches.

The descriptors are described as:-

1. Local Binary Pattern (LBP):
2. Gabor Filter
3. LDA (Local Descriptor Analysis)
4. PCA (Principle Component Analysis)

PCA and LDA based on facial feature for the face recognition. In PCA descriptor, small features used to identify an individual person. The spoof attacks based on the same facial features like nose, mouth, eyes etc. The skin texture attack is done by placing face in electronic device or on printed paper. Such attacks can only be detected by LBP.LBP computes the histogram of each region. The Gobar filter is robust to many factors but the performance of Gabor filter is not much good as compared to LBP. When Gabor and LBP combined together gives the best performance. Overall the spoof detection is best in LBP based on accuracy, complexity and computational cost [3].

Table 1 Various Approaches in face spoofing

DESCRIPTOR	FEATURES	LIMITATIONS
PCA	The dimension of data is reduced, easy to use and learn the whole image of face taken into consideration.	Time required to find Eigen values is more so it is more time consuming. It is affected by lighting conditions.
LBP	Used in texture description, fast and efficient computation, moving objects by subtracting background of image.	Face localisation are not detected, large regions increase the error rate, can be used in binary and gray image only.
LDA	Identify individuals of same faces, grouped individual faces with same features ,lighting variations solved because it is used within class	More complex method, difference between classes affect within class.
GABOR FILTER	Captures spatial frequency, localisation, and orientation. .	Sensitive to illumination changes.

VI. BIOMETRIC ANTI-SPOOFING TECHNIQUES

The anti-spoofing technique depends on different modes based on the biometric system. The techniques are described as:-

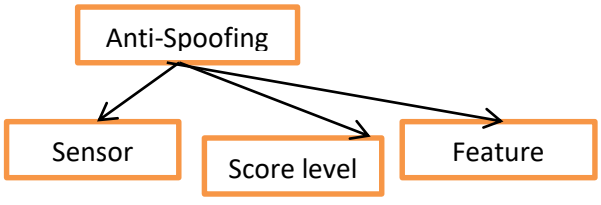

Fig 3. Different types of anti-spoofing biometric levels

6.1. Sensor Level Technique: - This is a hardware based technique. This method is used to add specific device to the sensor to detect the features. The hardware approaches based on characteristics are such as intrinsic properties of a living body, involuntary signals of a living body which can be attributed to the nervous system. Good examples are the pulse, blood pressure, perspiration, pupillary unrest (hippus), brain wave signals [18].

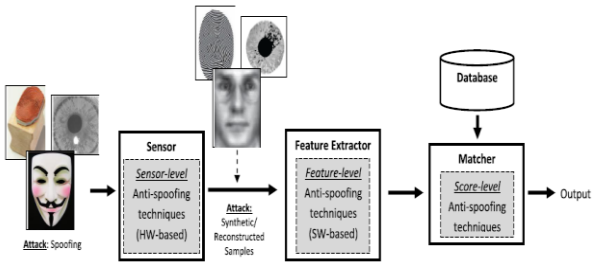

Fig.4 Face Spoofing Tehniques

6.2 Feature-Level Technique: - In this method, sample determines with the standard sensor fake trait is detected. The real and fake traits are distinguished from the biometric sample and not directly from human body. The face and iris is detected from the high resolution of face [17].

6.3 Score Level Technique*:* - This method based on the hardware and software approach analysed in the field of fingerprints ant spoofing. The protection technique based on biometric system of score level protects spoofing attempts. This technique designed as supplementary measures to the sensor-level and feature-level techniques. The two biometric module and anti-spoofing technique are combined to form scores.

VII. NUAA DATASET DESCRIPTION

The NUAA photo data base is collected using several webcams from an electronic market.The database is collected in three forms in an interval of two weeks between two sessions and the condition of each session is different. The 15 subjects were numbered from 1 to 15, and each session captured the images of both live subjects and their photographs.The samples from the three sessions of the samples from the database.The left pair from a actual human and right a photo.There will be changes in appearance for the recognition system.All the images in the database are color pictures with same pixels.Each from each session use webcams to capture series of data images.During image capturing ,each subject see webcam with neutral expression. In this way live human look like a photo [11].

Table 2 Detailed Summary

Sub_id	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Live Person															
Part 1	Y	Y	Y	Y	Y	Y	Y	Y	Y						
Part 2	Y		Y	Y	Y	Y		Y							
Part 3				Y		Y	Y			Y	Y	Y	Y	Y	Y
Photos															
Part 1	Y	Y	Y	Y	Y	Y	Y	Y	Y						
Part 2	Y	Y	Y	Y	Y	Y	Y	Y	Y						
Part 3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

NUAA Photograph Imposter Database contains images obtained from real and fake faces. This dataset contains 3,491 images for training (1,743 from real faces and 1,748 from printed ones) and 9,123 test images (3,362 real and 5,761 fake facial images). They were obtained from different people in terms of gender, age, etc., and on different capture sessions (also varying the cameras used for such task), making the database very realistic.

Fig.5 Example of face image dataset

Details of their involvement in an individual part are described in table 2. Individual parts and face images of both live subjects and their photos are considered.

Fig.6 Example of Dissimilar Attacks in Image Datasets [12]

In order to collect the sample of the photo, high definition photo for each subject use camera to take 2/3 of the whole area of the photograph. The photos are developed in different ways,firstly the photo is printed on the paper with common size. The five cataegoies of the photo attacks simulated before the webcam.

VIII. CONCLUSION AND FUTURE SCOPE

It has been concluded that many methods and techniques are explained to discriminate between the real and the fake face images.The biometric approaches are grouped in different categories.i.e sensor based, score level and feature based.In this review paper,the features of colour based analysis correlates for the face spoof attackers. The diiferent face spoofing detection detection techniques are described using feature extraction, biometric and context based technique. Briefly explained the NUAA face image dataset. NUAA photo data base is collected using several webcams from an electronic market.The database is collected in three forms in an interval of two weeks between two sessions and the condition of each session is different. The 15 subjects were numbered from 1 to 15, and each session captured the images of both live subjects and their photographs.The samples from the three sessions of the samples from the database.

The face spoofing can be done using variety of descriptors with global approaches.The attackers can break the system by defocusing the camera, if the only colour texture analysis is done to detect the spoofed faces.So in order to solve the problem of defocusing, distortion features are applied with colour features for better and effective result in spoof detection. In the future, several posiible research has been suggested for improving the performace in face sppofing detection and face recognition.The feature vectors can be

generated for fusion process to increase the facercognition performance.

REFERENCES

[1] 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", IEEE Transactions on Circuits and Systems—II: Express Briefs, Vol. 64, No. 12, pp. 1397-1401, December 2017.

[2] Aziz, A. Z. A., & Wei, H. (2018, August). Polarization Imaging for Face Spoofing Detection: Identification of Black Ethnical Group. In 2018 International Conference on Computational Approach in Smart Systems Design and Applications (ICASSDA) (pp. 1-6). IEEE.

[3] Dhawanpatil, T., & Joglekar, B. (2017, August). Face Spoofing Detection using Multiscale Local Binary Pattern Approach. In 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA) (pp. 1-5). IEEE.

[4] Lei Li, Paulo Lobato Correia, Abdenour Hadid, "Face recognition under spoofing attacks: countermeasures and research directions", Special Issue: Face Recognition and Spoofing Attacks of IET Biometrics, Vol. 7, Issue: 1, pp. 3 - 14, Jan 2018.

[5] D. Menotti et al., "Deep representations for iris, face, and fingerprint spoofing detection", IEEE Transactions on Information Forensics and Security, Vol. 10, No. 4, pp. 864–879, April 2015.

[6] S. R. Arashloo, J. Kittler, and W. Christmas, "Face spoofing detection based on multiple descriptor fusion using multiscale dynamic binarized statistical image features", IEEE Transactions on Information Forensics and Security, Vol. 10, No. 11, pp. 2396–2407, Nov. 2015.

[7] Zhibin Pan, Xiuquan Wu, Zhengyi Li, and Zhili Zhou, "Local Adaptive Binary Patterns Using Diamond Sampling Structure for Texture Classification", IEEE Signal Processing Letters, Vol. 24, Issue: 6, pp. 828 - 832, June 2017.

[8] Galbally, J., Marcel, S., & Fierrez, J. (2014). Biometric Antispoofing Methods: A Survey in Face Recognition. IEEE Access, 2(1530-1552), 1.

[9] Chingovska, I., Yang, J., Lei, Z., Yi, D., Li, S. Z., Kahm, O., ... & Komulainen, J. (2013, June). The 2nd competition on counter measures to 2D face spoofing attacks. In Biometrics (ICB), 2013 International Conference on (pp. 1-6). IEEE.

[10] X.Tan, Y.Li, J.Liu and L.Jiang. Face Liveness Detection from A Single Image with Sparse Low Rank Bilinear Discriminative Model, In: Proceedings of 11th European Conference on Computer Vision (ECCV'10), Crete, Greece. September 2010.

[11] NUAA Imposter Database. (2019). Retrieved from http://parnec.nuaa.edu.cn/xtan/data/nuaaimposterdb.html.

[13] Komulainen, J., Hadid, A., & Pietikainen, M. (2013, September). Context based face anti-spoofing. In Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on (pp. 1-8). IEEE.

[12] Li, J., Wang, Y., Tan, T., & Jain, A. K. (2004, August). Live face detection based on the analysis of fourier spectra. In Biometric Technology for Human Identification (Vol. 5404, pp. 296-304). International Society for Optics and Photonics.

[13] Tirunagari, S., Poh, N., Windridge, D., Iorliam, A., Suki, N., & Ho, A. T. (2015). Detection of face spoofing using visual dynamics. IEEE transactions on information forensics and security, 10(4), 762-777.

[14] Määttä, J., Hadid, A., & Pietikäinen, M. (2012). Face spoofing detection from single images using texture and local shape analysis. IET biometrics, 1(1), 3-10.

[15] Chingovska, I., Anjos, A., & Marcel, S. (2012). On the effectiveness of local binary patterns in face anti-spoofing. In Proceedings of the 11th International Conference of the Biometrics Special Interes Group (No. EPFL-CONF-192369).

[16] Pan, G., Sun, L., Wu, Z., & Lao, S. (2007). Eyeblink-based anti-spoofing in face recognition from a generic webcamera.

[17] Bharadwaj, S., Dhamecha, T. I., Vatsa, M., & Singh, R. (2013). Computationally efficient face spoofing detection with motion magnification. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (pp. 105-110).

[18] Yang, J., Lei, Z., Liao, S., & Li, S. Z. (2013, June). Face liveness detection with component dependent descriptor. In 2013 International Conference on Biometrics (ICB) (pp. 1-6). IEEE.