2015 International Conference on Advanced Computing and Communication Systems (*ICACCS* -2015), Jan. 05 – 07, 2015, Coimbatore, INDIA

SPOOFING FACE RECOGNITION

Y.Binny Reeba,
PG scholar/Department of CSE
Government college of Technology, Coimbatore.
e-mail:binnyreeba18@gmail.com

Dr.R.Shanmugalakshmi
Associate Professor /Department of CSE
Government college of Technology, Coimbatore.
e-mail:drshanmi@gct.ac.in

***Abstract*-Spoofing face recognition is the implementation of detecting facial masks. The algorithm used is Baseline face recognition algorithm, which is mainly based on the functions of face recognition and anti spoofing. The ISV method is used for the face recognition of 2D images by detecting the SURF feature of an image. To differentiate the real faces and mask, anti spoofing is performed by extracting the LBP feature. Finally based on the LBP histograms the features extracted are trained by SVM for feature classification to indicate whether the input will be accessed or not. The SVM classifier was selected because of its high accuracy. This work can be extended in future by detecting the surgically altered faces along with the face mask detection.**

Key Words:-Mask attack, Spoofing face, Reply attack.

I.INTRODUCTION

Face is the most commonly used biometric for identification, and has great application in consumer electronics and software. Face biometric is famous because of its accessibility compared with the other biometrics like finger print or iris. However this advantage is also the weakness for the spiteful situations, gives attackers to create copies and imitate face recognition systems easily.

Spoofing attack is nothing but the act of outwitting a biometric system by submitting a fake evidence to gain authentication. It is very easy to generate such an attack for the face recognition system, since the photographs or videos of the clients can be easily obtained through social networks or captured from the distance. Clients are the persons who are enrolled in a face recognition system. An attacker can access the system by displaying their photos or replaying their recorded videos to the device

This produced vulnerability of face will bring great interest in the biometric community. Because of their simplicity and low cost the printed photo attack and the video replay attacks are increased significantly. There are many anti-spoofing approaches against the above attack is classified into texture analysis, motion analysis and liveness detection. The presence of cues and blurring will examine the texture of captured face image. In recent years the micro texture analysis is done using the multi-scale local binary pattern, which is mainly depends on the quality of the printed image or the video displayed.

The axis and the depth measurements will not be affected by the lighting. Since it can even be used in darkness to at different angles will have the ability to detect the object at in different viewing angles up to 90 degrees. It is to reduce the spoofing attack. The steps to be followed for the 3-D face biometric system are by detection alignment, measurement, representation and matching. In the verification of an image is by matching an input image with to only one image in the database (1:1). For potential match the image is compared to all the images in the database results a score for each match.

II. RELATED WORK

The earlier methods of detecting the mask aims to calculate the difference between the facial skin and the mask material based on their reflectance characteristics.[1] Before 30 years the face thermo gram was not vulnerable to distinguish and detect the plastic surgery, since he reduction in the thermal signature of the face.

Later the differences can be detected better in near-infrared, and utilizes the 1.3-1.7 μm sub band of the upper band. Only by illustration the simple thresholding is suggested for the classification. Later the multi-spectral analysis is done over the above methods, to detect the fake, and it is non distinguishable by eyes of human so the visual images will not be sufficient for the detection of attacks.[2][3] In another they handle the mask attack problem rather than the spoofing because it will not examine the mask which is the repetition of valid users. The authors conduct experiments only on the mask materials such as silicon, skin jell to find the different behavior of such materials mainly the reflectance compared with the face skin mainly on the forehead region.

So the albedo values of illumination at different wavelengths are analyzed. From that values two best wavelengths are selected one from the visual and the other from the near-infrared spectrum .The resultant 2D vectors will have the radiance

[978-1-4799-6438-3/15/$31.00 ©2015 IEEE]

measurements about these measurements are done under the illuminations are at the distance of 30cm are strictly maintained from the sensor are classified as skin or non-skin by the linear discriminant. This method will identify the fake faces are 97.7% classification rate. The practical application was restricted by the possibility of occlusion in the forehead region. Here the analysis are done only on the mask materials also two different wavelength such as 850 and 1450 nm are selected after calculating the albedo values of the facial skin and mask materials at different distance. An SVM classifier is trained to differentiate the genuine and fake attempts and tested on the database of 20 masks of different materials such as plastic, silica gel, paper pulp, plaster and the sponge.[4] It has the classification range of 89%. It removes the range limitation of the face and the mask.

In other words there is no analysis is done on mask are like real faces and can't be spoof any real person.[4] The disadvantage of the above method is that its hardware requirements . Later the printed 3D mask of 16 users is used to generate a 3D database. The face models of person are generated by 3D laser scanner and the mask are made by the 3D printing service. Along with the texture images 3D face models are made with the morpho database having the sample for the face and the mask.[5] The vulnerability analysis over 2D, 2.5D and 3D face recognition systems against 3D mask attacks are analyzed as a micro-texture based counter measure which is applied separately on color images and depth maps. There are three baseline face recognition algorithms are implemented for the observation of the spoofing performances of masks [6] [7].Then a probe sample is compared to the gallery sample of the claimed ID and a decision is made based on the similarity metric. In the analysis, the authors do not have an enrolment set instead of that they give a method that is referred by two methods. In first method the baseline face recognition algorithm are used to recognize the real samples from the database. It will give two types of scores such as real and imposter. In second method which is the mode under spoofing attack, mask samples are considered as the probe set. Each sample is compared the other entire sample input to generate the genuine and mask scores. These are used for both identification and verification. And it is used to gain knowledge about the spoofing potential of the 3D facial masks. Its performance will be degraded by the two problems such as spoofing will not be relevant with the close set identification setting due to that the probe will always have an identity in the sample set which will not based on the quality of the attack.

The mask attack measurement based on the local Binary pattern is tested in two methods they are color images and also the depth maps. [8]A depth map is nothing but a grayscale image that will have the information connecting the distance of the surfaces of the 3d objects from the particular view point. The features extracted from the both 2d and 2.5D images are the multi-scale LBP and the linear SVM classifier is used to determine whether the sample feature belongs to the real sample or an attack sample.[9] The training set will not overlap with the partition which was tested. The testing results are given separately for the 2D and 2.5D modes and the thresholds are calculated for the best performance classification rates. Later the fusion of the score level and the fusion levels are combined and the LBP histograms are calculated for both 2D and 2.5D images. The classification results are as same as the above method. [10][11] By turning the threshold level the best performance is obtained. Since the 2D and 2.5D modes will generate the 89.2% and 82.2% classification rate separately. Then by fusing the two modes will give the classification rate as 93.4%. Another type of detection method is based on the reflectance analysis. It is based on the variational retinex algorithm that will decompose the texture feature into the illumination and the reflectance characteristics [12] [16]. Then the SVM classifier is applied to classify the mask images and the real face images. Then the performance is measured only by theoretically.

III. IMPLEMENTATION

The spoofing face recognition is the authentication method. The basic block diagram for the detection of mask attack is given by

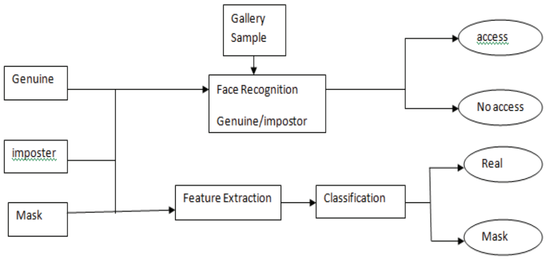


Figure 1: Block diagram for mask detection

The input given to the face recognition system will be genuine, imposter and the mask. Whatever may be the input given, the features are extracted and that result is compared with the gallery sample. Based on the matching, the authentication is provided. The proposed system consists of the following modules, Face Recognition, Anti-spoofing. The spoofing performances of the face in 2D face recognition algorithm that is based on Inter Session Variability (ISV) modeling method. For that, the face images are separated into non-overlapping blocks for training, development and testing, it is possible to evaluate every mask in both 2D and 3D domain.

Inter Session Variability (ISV) modeling is developed for speaker recognition. Later it is applied for face recognition purpose. Enrolled persons are described with Gaussian Mixture Models (GMM) which is built by set of blocks of pixels extracted from the gallery. ISV aims to make the client models as reliable by eliminating (inter-session) variation in between the clients. First 12×12 blocks are separated from the facial image by moving the sampling window by one pixel at a time. Then the mean and variance normalisation is applied and the first 45 2D DCT co-efficients (lowest frequency) are separated. By the distribution of the feature vectors, a GMM is estimated using background model (UBM) adaptation for each input. Finally, ISV modeling is used to separate the client variation.

The SURF key-points are detected by using Hessian matrix approximation. This is implemented by the second order Gaussian derivatives then the Hessian matrix is approximated using the box filters. Later the key points are localized in both scale and image space by allowing a non maximum suppression in a 3x3x3 neighborhood.

In anti-spoofing it is more difficult to detect the attacks with motion analysis and also the liveness detection methods. For this purpose, the texture analysis remains as a more reliable approach that can be adopted. Naturally, human skin is different from mask materials with its optical characteristics, such as reflectance or scattering.

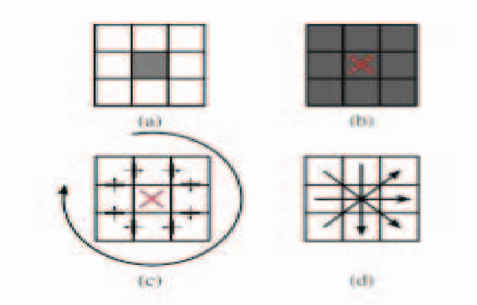
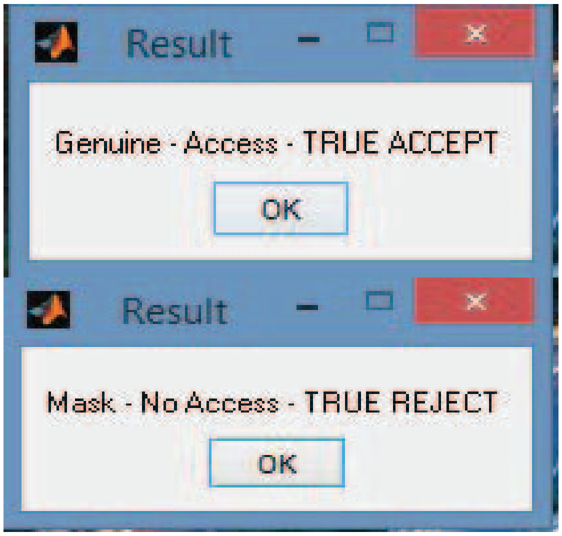


Figure 2: Extended set of LBP

The LBP value for each pixel is calculated by comparing the adjacent pixels in 3 × 3 neighborhood with the value of that pixel which will form a 8-bit binary number. The extension to the original operator will eliminate patterns with two bitwise transitions. This will reduce the number of different labels which will results the 59 uniform patterns. The LBP operator can also be extended to change the method of encoding. The occurrences of the LBP in the whole image or in blocks are mapped into histograms and then considered as feature vectors are classified. Because the extracted LBP are collected into histograms, the classification can be done by computing histogram similarities. So the test samples are compared with the $\chi 2$ metric, resulting in two distances, and . The final result is computed as - . Then the SVM classifier is used to generate the result as original or mask.

IV. RESULT



Genuine - Access - TRUE ACCEPT

Mask - No Access - TRUE REJECT

Figure3: Results as access or not

The LBP values are calculated for the input images are given as

Input	LBP per block	Data	MLBP	tLBP
Real	195.33	731	131.71	252.01
Mask	194.45	752.	137.89	253.45

Table: Extended LBP values

Performance Metrics

It contains two types of error as commonly they are false fake FFR and the FLR

The accuracy of the system is measured by the equation of

(1)

The half total error rate is calculated by

(2)

The Performance of the system by using the ISV modeling is given as

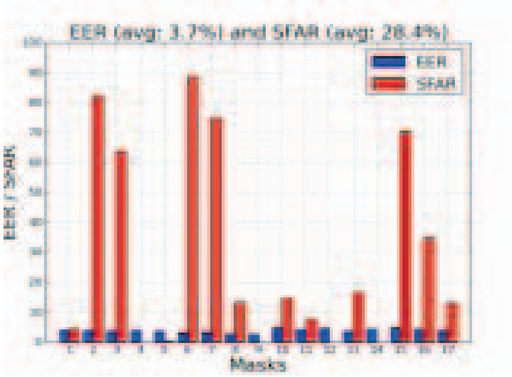


Figure 4: Performance evaluation by ISV method

V.CONCLUSION

Spoofing attacks continue to be a security threat for biometric recognition systems and face is among the most vulnerable traits due to its high accessibility. Utilization of masks for face spoofing attacks has become easier and cheaper with Spoofing face recognition is by implementing the For the detection of the facial masks, The Baseline face recognition algorithm, is used for face recognition and anti spoofing. To differentiate the real faces and mask, anti spoofing is performed by extracting the LBP feature. The SVM classifier was used because of its accuracy which will give the better improvement in its performance.

VI.REFERENCES

[1] Nelsi Erdogmus and sebastien Marcel ,"Spoofing face recognition using 3D mask" Information forensics and security, IEEE Transactions on july. 2014.

[2] I. Pavlidis and P. Symosek, "The imaging issue in an automatic face/disguise detection system," in Workshop on Computer Vision Be- yond the Visible Spectrum: Methods and Applications, 2000, pp. 15–24

[3] Y. Kim, J. Na, S. Yoon, and J. Yi, "Masked fake face detection using radiance measurements," Journal of the Optical Society of America A, vol. 26, no. 4, pp. 760–766, 2009

[4] Z. Zhang, D. Yi, Z. Lei, and S. Li, "Face liveness detection by learning multispectral reflectance distributions," in IEEE International Conference on Automatic Face Gesture Recognition and Workshops, March 2011, pp. 436 –441.

[5] J. Yan, Z. Zhang, Z. Lei, D. Yi, and S. Li, "Face liveness detection by exploring multiplescenic clues," in International Conference on Control, Automation, Robotics and Vision, 2012.

[6] N. Kose and J.-L. Dugelay, "Countermeasure for the protection of face recognition systems against mask attacks," in IEEE International Conference on Automatic Face and Gesture Recognition, April 2013.

[7] "On the vulnerabilityof face recognition systems tospoofing mask attacks," in IEEE International Conference on Acoustics, Speech, and Signal Processing, May 2013.

[8] N. Kose and J.-L. Dugelay,"Shape and texture based counter measure technique to detect face mask attack" in proc.IEEE Conf, CVPRW, June 2013.

[9] "Reflectance analysis based countermeasure technique to detect face mask attacks," in International Conference on Digital Signal Processing, July 2013.

[10] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Li, "A face antispoofing database with diverse attacks," in IAPR International Conference on Biometrics, 2012, pp. 26–31

[11] N. Erdogmus and S. Marcel, "Spoofing in 2d face recognition with 3d masks and anti-spoofing with kinect," in Biometrics: Theory, Applica- tions and Systems (BTAS), 2013.

[12] M.C.WallaceR.,McLarenM.andM.S.,"Inter-session variability modelling and joint factor analysis for face authentication," in International Joint Conference on Biometrics, 2011, pp. 1–8.

[13] N. Erdogmus and J.-L. Dugelay, "On discriminative properties of tps warpingparametersfor3dfacerecognition,"in International Conference on Informatics, Electronics & Vision (ICIEV), 2012, pp. 225–230.

[14] B. B. Amor, M. Ardabilian, and L. Chen, "New experiments on icp based 3d face recognition and authentication," in International Conference on Pattern Recognition, vol. 3, 2006, pp. 1195–1199.