International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 8 215 - 217

Face Spoof Detection from Single Image Using Various Parameters

Ms. Manisha Pansare
Department of Computer Engineering
Y.T.C.E.M., Bhivpuriroad
Mumbai, India
manisha2810@gmail.com

Prof. Vanita Mane
Department of Computer Engineering
RAIT, Nerul
Mumbai, India
vanitamane1@gmail.com

Prof. Suchita Walke
Department of Information Technology
YTCEM, Bhivpuri road
Mumbai, India
suchita.walke@tasgaonkartech.com

***Abstract*—** To detect duplication of identity during authentication of online payment on mobile or personal computer, the automatic face recognition is widely used now days. The biometric presentation attacks can be performed to gain access to these systems. It is performed by presenting the authorized person's photo or video. Hence it is important to study the various face spoof attacks. Currently proposed face spoof detection techniques have less generalization ability as these are not considering all factors and do not detect the spoofing medium.The four features such as specular reflection, blurriness, chromatic moment and color diversity are used to analyze the image distortion. The different classifiers are trained for printed photo attack and video replay attack to differentiate between genuine and spoof faces. We also propose an approach to detect the spoofing medium by checking the boundary of the captured image during the photo attack and video attack and an approach to detect the blinking of eye for detecting liveness. It gives us high efficiency rather than existing methods.

Keywords-*Face recognition,Face spoof attacks,Image distortion analysis, spoofing medium,liveness*

*****

I. INTRODUCTION

To determine accurately the identity of an individual for different applications, it is necessary to manage more number of solutions. Biometrics such as face, fingerprint, iris, voice, gait etc. are used to recognize individuals based on their physiological, behavioral and chemical attributes. Biometric authentication is more advantageous than traditional schemes such as passwords and ID cards mechanisms. People always use simple passwords because complex passwords are hard to remember, and the same password is usually utilized for different applications. The passwords and ID cards can be easily lost, shared, manipulated or stolen. By using biometrics, the identity of an individual can be confirmed easily based on who the individual is rather than what the individual possesses or what the individual remembers. Using biometrics has indeed become a reality for identity management of person because everywhere the biometric enabled applications are used now a day. [1]

Recognition of face does not require any additional sensor because all smart phones are equipped with a front facing camera. Similar to other biometric modalities, it is important to deal with face spoof attacks on face recognition systems, especially in unconstrained sensing and uncooperative subject scenarios [2].

It has been observed that conventional biometric techniques are vulnerable to spoofing attacks, where a person tries to disguise as another one by altering a biometric trait of the targeted user and presenting it to the biometric system, and can gain access to the system.

II. APPLICATIONS

The proposed system can be used in various areas such as:

- Entertainment: Video game, virtual reality, training programs, interaction between human and robot, to interact human and computer
- Smart cards: Drivers' licenses, voter registration, Immigration, national ID, passports,
- Information security: Parental control of TV, personal device logon, Application security, database security, encryption of files
- Law enforcement and Surveillance: Advanced video surveillance, CCTV control, Portal control, post event analysis,suspect tracking and investigation

III. REVIEW OF LITERATURE

In the literature survey, various authors had proposed different spoofing cue to detect whether the person is real or fake is summarized as below:

For the motion based method, the authors [3],[4],[5],[6] had considered the eye blinking, lip reading digits and differences in optical flow field of 3D objects and 2D planners as spoofing cues for liveness detection respectively.

For the texture based method, the author [6] had used the spoofing cue as difference between features of printed photograph, digital photo and video display. The author [8] had used the combination of LBP-TOP and space-time information as texture descriptor. The author [9] had considered the micro differences between genuine and fake face.

For image quality based method, the author [7] uses the face image quality differences due to the different reflection properties of different materials.

For other cue method, the author [10] recovers 3D facial structure from video or several images captured from different viewpoints. The author [11] captured soft biometric traits such as eye color, age, gender etc. as spoofing cue. The author [12] had chosen one third high frequency components from photo image. The author [13] had considered whether the boundaries of the used display medium can be detected in the view and different spoof detection schemes are proposed accordingly for each scenario. It also described a method exploiting contextual information for detecting the display medium in the provided scene.

IV. PROBLEM STATEMENT

Existing methods capture facial details and differentiate one from the other. As a result, when the same features are used to differentiate a real face from a facke face, they either contain some redundant information for liveness detection or information that is too person specific. These two factors limit the generalization ability of existing methods.
These methods find only attacks and not spoofing medium.

V. PROPOSED WORK

In this system, we have proposed a method in which the problem of methods based on texture features can be solved using image distortion analysis. Without doing any normalization of image, it will find if it is real or fake. By using another method the second problem can be solved, it will find the boundaries around the image. If the boundary around the image is present, then it will detect the spoofing medium whether it is printed photo or mobile or tablet.
The third problem can be solved by checking eye blinking using the same camera.

Architecture and Algorithms

The architecture of the proposed system works is as shown in fig.1. It works as below:

Register person details with face

The person, who wishes to use system, should be a registered user. Hence, when he will be using the system first time, will enter all his/her details such as name, age, gender, mail id etc. Along with these details his/her image will be captured and stored in database. When face image will be captured, the specific parameters of the image will also be stored.

Login, Image distortion feature extraction and identify

When the person will try to use the system, he/she will do the login process. At the same time, the person's face image will be captured. The four IDA features will be extracted from the captured image .The light reflectance I of an object at specific location x can be decomposed into the following diffuse reflection (I_d) and specular reflection (I_s) components:

$$I(x) = I_d + I_s = w_d(x)\, S(x)\, E(x) + E(x) + w_s(x)\, E(x) \quad (1)$$

Where $E(x)$ is the incident light intensity, $w_d(x)$ and $w_s(x)$ are the geometric factors for the diffuse and specular reflections, respectively, and $S(x)$ is the local diffuse reflectance ratio.
The 2D spoof faces are created by recapturing from original real face images. The formation of spoof face image intensity $I'(x)$ can be calculated as follows:

$$I'(x) = I'_d + I'_s = F(I(x)) + w'_s(x) E'(x) \quad (2)$$

The equation (1) and (2) only model the reflectance difference between genuine and spoof faces and have not considered the final image quality after camera capture. In equation (2), we substitute the diffuse reflection of spoof face image I'_d by $F(I(x))$ because the diffuse reflection is determined by the distorted transformation of the real image $I(x)$. Therefore, the total distortion in $I'(x)$ consists of two parts: i) distortion in the diffuse reflection component (I'_d), and ii) distortion in the specular reflection component (I'_s), both of which are related to the spoofing medium. In particular, I'_d is related with the

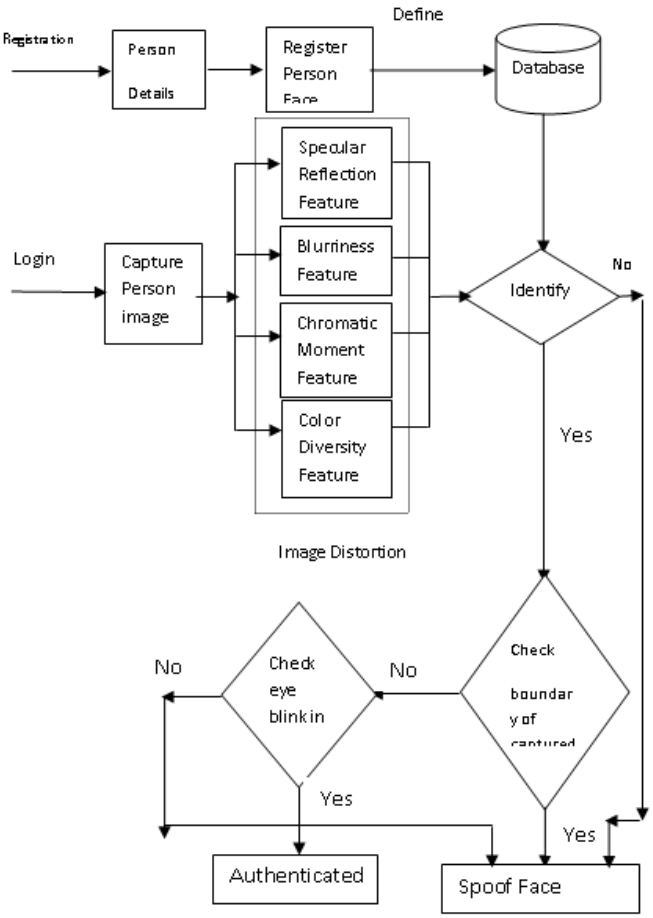

Fig.1 Block diagram of the proposed cascade structure for detection of spoofing face and medium

real face image $I(x)$, while I'_s is not dependent of $I(x)$. The distortion function $F(\cdot)$ in the diffuse reflectance component can be modeled as

$$F(I(x)) = H(G * I(x)) \quad (3)$$

where $G(\cdot)$ is a low pass point spread function and $H(\cdot)$ is a histogram transformation function .
Based on this model, we can analyze the significant differences between real faces and two types of spoof faces i.e. printed photo and replay video or photo attacks.
In printed photo attack, $I(x)$ is first transformed on the paper to the printed ink intensity and then to the final image intensity by diffusion reflection from the paper surface. The $G(\cdot)$ and $H(\cdot)$ are determined by the printer frequency and chromatic fidelity. [2].
In replay video attack, the video is divided into frames. At the same time it will compare the face in frame with the image stored in database.

The boundary checking

The intensity of the pixels around the image in rectangular shape is calculated. If it is above the threshold value, then it will find the spoofing medium whether it is photo or a mobile phone. If the intensity of pixels is below the threshold value then it will check for eye blinking for liveness detection.

Boundary Detection Algorithm

Step1. Create grey scale image
Step2. Count total pixels

Step3. Check height and width of image
Step4. Consider i pixel with value = 0
Step5. Find pixel RGB value and put in array
Step6. Check for consecutive value RGB
Step7. If it is same then store its RGB value in array and goto step 6 else clear array and goto step 4 with i = j

Liveness detection

Anti-spoofing without any additional devices will be preferable because it reduces the cost of required hardware and can be easily integrated into existing face recognition system. The human eyes blink once every 2 to 4 seconds, so the blinking of eye is checked for detecting the liveness.
If the system finds the blinking of eye, then it will say that liveness is detected else the liveness is not detected.

Eye Blinking Algorithm

Step1. Create frames of video clips
Step2. Consider first frame
Step3. Find eye location on image in x and y coordinates
Step4. Put the pixel value in variable
Step5. Consider next consecutive frame
Step6. Check for x and y coordinates for this frame, if the value is different, then goto step 8
Step7. Check for another frame, if it is not last frame goto step 5 else goto step 9
Step8. Eye blink is present
Step9. Eye blink is not present

Authenticated and spoof face

When the person will login at that time if the captured image matches with the image stored in database and also satisfies all other conditions, then the system will display it as authenticated person else it will display that it is spoofed face.

VI. METHODOLOGY

The proposed system is basically divided into four modules such as registration, image distortion feature extraction from image of logged person, boundary detecting and liveness detection.

1. Module 1 will register the person details along with his image in database.
2. Module 2 will verify the logged person's image by extracting image distortion features with the data stored in database. If it is not matching then it will detect it as a spoofed face. Else it will proceed to detect boundaries around the image.
3. Module 3 will find the boundaries around the image. If the total number of pixels around the image is more than the threshold then it will detect it as spoofed face. Else it will proceed for liveness detection.
4. Module 4 will check the eye blinking. If eye blinking is present then it will display as authenticated face else spoofed face.

VII. CONCLUSION

Image distortion analysis for face detection technique is used to detect the fake faces.
Due to image quality analysis, it is easy to find out real and fake users because fake face images always have different color, reflection, blurriness features. The proposed system uses the image distortion analysis to detect whether the face is spoofed or real. Also it not only checks the image quality but also it checks for liveness. Along with this, the proposed system also detects the spoofing medium and finds the type of attack on biometric whether it is printed photo or video replay attack. Hence the proposed system is more efficient and secure than uni-biometric system. The multi biometric system is used for various applications.

VIII. REFERENCES

[1]. Komulainen, Jukka, Software-based countermeasures to 2D facial spoofing attacks.
[2]. Di Wen, *Member, IEEE*, Hu Han, *Member, IEEE*, and Anil K. Jain, *Life Fellow, IEEE,"* Face Spoof Detection With Image Distortion Analysis*",* IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 4, APRIL 2015
[3]. K. Kollreider, H. Fronthaler, M. I. Faraj, and J. Bigun, "Real-time face detection and motion analysis with application in 'liveness' assessment," IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 548–558, Sep. 2007.
[4]. L. Sun, G. Pan, Z. Wu, and S. Lao, "Blinking-based live face detection using conditional random fields," in Proc. AIB, 2007, pp. 252–260.
[5]. W. Bao, H. Li, N. Li, and W. Jiang, "A liveness detection method for face recognition based on optical flow field," in Proc. IASP, Apr. 2009, pp. 233–236.
[6]. S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, "Computationally efficient face spoofing detection with motion magnification," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), Jun. 2013, pp. 105–110
[7]. J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition," IEEE Trans. Image Process., vol. 23, no. 2, pp. 710–724, Feb. 2014.
[8]. 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.
[9]. J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection with component dependent descriptor," in Proc. IJCB, Jun. 2013, pp. 1–6.
[10]. T. Wang, J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection using 3D structure recovered from a single camera," in Proc. ICB, Jun. 2013, pp. 1–6.
[11]. Z. Zhang, D. Yi, Z. Lei, and S. Z. Li, "Face liveness detection by learning multispectral reflectance distributions," in Proc. FG, Mar. 2011, pp. 436–441.
[12]. J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of Fourier spectra," *Proc. SPIE*, vol. 5404, pp. 296–303, Aug. 2004.
[13]. J. Komulainen, A. Hadid, and M. Pietikäinen, "Context based face antispoofing," in Proc. BTAS, Sep./Oct. 2013, pp. 1–8.