Detection of Spoofed Face and Medium Using Various Parameters From Single Image

Manisha Pansare[1], Prof. Vanita Mane[2]

Department Of Computer Engineering, Mumbai University

[1]manisha2810@gmail.com

[2]vanitamane1@gmail.com

Abstract—

The Automatic face recognition is used everywhere for authentication of personal computer or mobile while performing any online transaction. To gain the access to these systems, the direct attacks or biometric presentation attacks such as presenting photo or video of the authorized person can be done by intruders easily because the photo's can be available easily on social networks such as face book or anyone. Currently proposed face spoof detection techniques have less generalization ability as it considers only image quality not all specific facial features. Also the existing methods do not detect the spoofing medium and liveness in a single system. The facial features such as eyes, mouth and nose are extracted from the image in the proposed approach. The classifier distinguishes the real face and spoofed face. By finding the boundaries in the image, it detects the spoofing medium and attack type. By capturing the video it also detects the eye blinking or liveness without using any extra hardware.

*Keywords— **Face recognition, Face spoof attacks, Feature extraction, spoofing medium, liveness***

I. INTRODUCTION

Based on physiological, behavioural and chemical attributes, biometrics such as face, iris, fingerprints etc are used to access the different applications as the biometric authentication is more secure and advantageous than traditional schemes such as passwords and ID cards mechanisms. The complex passwords are hard to remember; hence people always use simple and same passwords for different applications. The passwords and ID cards can be easily stolen, shared, or manipulated. 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. Since now days the biometric enabled applications are being used everywhere, the biometrics has indeed become a reality for identity management of person. [1] The systems which uses the face recognition, does not require any additional hardware or sensor as all smart phones or laptops are equipped with a front facing camera. The biometric treats such as face, iris, fingerprints, etc can be spoofed as it can be easily available on social networks and also can be modified, which is major drawback of biometric authentication. The proposed system detects the printed photo and replayed photo attacks. Also it can detect the spoofing medium and eye blinking.

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

II. REVIEW OF LITERATURE

The various authors studied different face spoofing algorithms by considering various cues to detect the spoofed face.The published methods are basically classified into four types such as i) Motion based methods, ii) Texture based methods, iii) Image quality based methods and iv) Methods based on other cues. The authors [3],[4],[5],[6] had studied the motion based methods and 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. 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 colour, 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.

III. PROBLEM STATEMENT

Existing method does not capture facial details but considers the image quality and differentiate one from the other. As a result, when the quality of original captured image is not good then cannot differentiate a real face from a fake face. These factors limit the generalization ability of existing methods. The existing system finds only attacks and not spoofing medium and does not detect the liveness.

IV.PROPOSED WORK

In this system, we have proposed a method in which the problem of existing methods can be solved by extracting the facial details. It detects the face whether it is real or spoofed without adjusting the face in the image. It finds the boundaries around the face. If the boundary around the face 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.

Working principle of the system

This section gives the detailed working of the system as below.

1 Face Detection

The proposed system will ask the user to register. During registration the details of the face will be stored in a database along with the image of the same person and the authentication ID is provided to the user. Whenever for next time the person will try to login, the person has to provided the authentication ID and then the various features will be extracted and compared with the already stored database entries. If it will match then it displays the message that the user is authenticated else the user is not authenticated. The boundaries around the face will be checked. If boundaries are present then the face will be spoofed face, and the spoofing medium is detected. The system also checks for eye blinking. If the eye blink is present then the face will be authenticated else the face will be spoofed face. In the proposed system, first the boundaries of the image will be checked and then eye blinking will be checked. It will give high efficiency because checking the boundaries takes less time than checking eye blinking.

2 Spoof Medium Detection

Face images captured from face spoofs may visually look very similar to the images captured from live faces, thus face spoof detection is rather difficult to perform based on a single face image or a relatively short video sequence only. Depending on the imaging and fake face quality, even for us humans, it is almost impossible to tell the difference between a genuine face and a fake one without any scene information or any unnatural motion or facial texture patterns. However, we can immediately notice if there is something suspicious going on in the view, e.g. if someone is holding a video display or a photograph in front of the camera.

Inspired by how we humans can perform reliable spoof detection only based on the available scene and context information, the proposed system will determine whether a spoofing medium is present in the observed scene.

The boundaries of the used spoofing medium, e.g. the boundary of displayed video or photograph can be observed easily. The boundaries of the image or video will be checked after the person will logins. If the boundaries are present around the image then the spoofing medium is present, can be detected easily. The proposed approach can be operated on single image, single frame or the video sequences.

3 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.

4 Classification

The classification algorithm will classify the face as real or spoofed.

Architecture

The architecture is divided into different modules as explained below

1 New User Registration

The person, who wishes to use system, should be a registered user. Hence, when he will be using the system first time, the details his/her image will be captured and stored in database. When face image will be captured, the specific features of the image are extracted. If the system is not able to capture all the desired features then it asks user to register again else the ID is displayed to the registered user immediately and the image is stored in database by the ID name.

The Fig 6.2.1 shows steps to register the new user in the system

Algorithm for New User Registration

Step1: Capture video
Step2: Capture one frame for processing
Step3: Extract Feature such as eyes from the image
Step4: Does it find the eyes? If yes then go to step 5 else go to step
Step5: Display Message” Human Face”
Step6: Find the total number of .png images in database and generate ID for new registered user
Step7: Store the image of registered user with its ID
Step8: Display Message” Not Human Face….Register with Human Face”

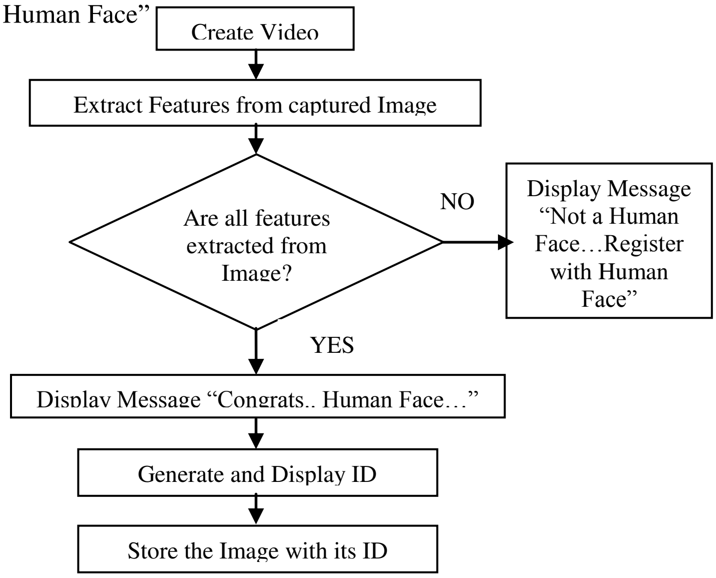

Create Video
Extract Features from captured Image
Are all features extracted from Image?
NO
Display Message “Not a Human Face…Register with Human Face”
YES
Display Message “Congrats.. Human Face…”
Generate and Display ID
Store the Image with its ID

Fig.1 New User Registration

2 Login and Authentication for already existing user

When the person will try to use the system, he/she will do the login process by using the ID created during registration process. At the same time, the person's face image will be captured. The SURF features will be extracted from the captured image. The extracted SURF features of the captured image will be compared with the features of the stored ID image. If the features are not matching, then it displays the message "Non Authenticated User". Else it displays the message "Authenticated User".

Algorithm for Login and Authentication for already existing User

Step1: Enter the User ID
Step2: Capture Temp image of the user
Step3: If features of ID image are matching with Temp image then go to step 4 else go to step 5
Step4: Display message "Authenticated User"
Step5: Display message "Unauthenticated User"

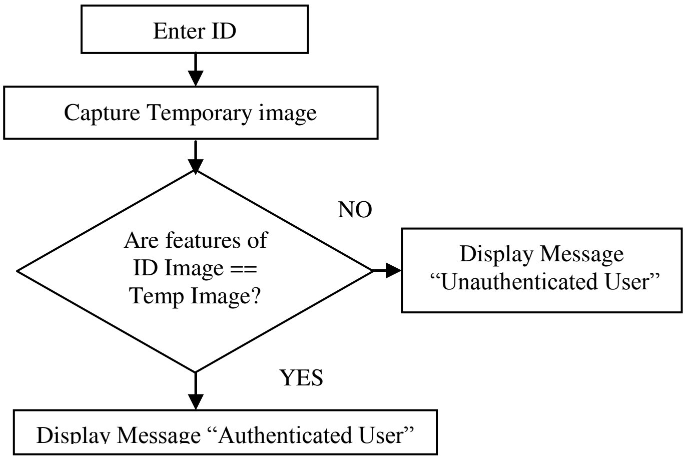

Enter ID
Capture Temporary image
Are features of ID Image == Temp Image?
NO
Display Message "Unauthenticated User"
YES
Display Message "Authenticated User"

Fig. 2 Login and Authentication for already existing User

3 Extracting Facial Features and Detecting spoofing Medium

After providing authentication, it detects the facial features and shapes in the image. 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 boundaries are present then it displays the message "Spoofing medium is present and face is the spoofed face". Else it displays message "No spoofing medium present and it is real face".

Algorithm for extracting facial features and detecting spoofing medium

Step1: Get stored Temp Image
Step2: Extract SURF and MSER features of the image
Step3: Count total pixels in grey scale image
Step4: Check height and width of image
Step5: Consider i pixel with value = 0
Step6: Find pixel value in grey scale image and put in array
Step7: Check for consecutive value
Step8: If it is same then store its value in array and go to 6 else go to clear array and go to 4 with i = j (j= current pixel value)

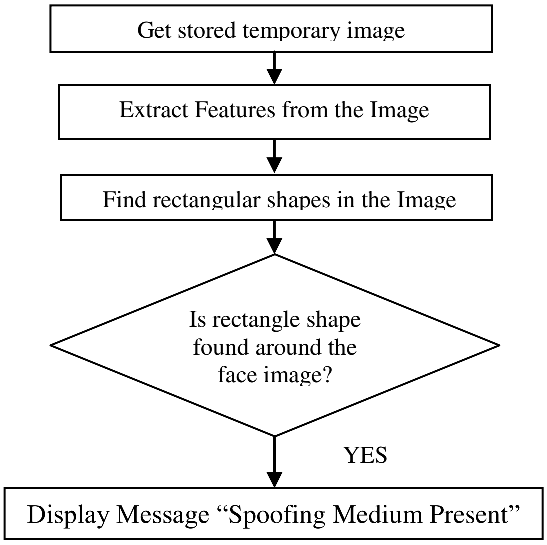

Get stored temporary image
Extract Features from the Image
Find rectangular shapes in the Image
Is rectangle shape found around the face image?
YES
Display Message "Spoofing Medium Present"

Fig. 3 Extracting Facial Features and Detecting Spoofing Medium

4 Eye Blinking (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
Step4: Put the pixel value in variable
Step5: Consider next consecutive frame
Step6: Find the pixel value for current frame, if the value is different, increment Eye blink count by 1 and decrement frame count by 1, go to step 7
Step7: If frame count =0 then go to step 8 else go to step 5
Step8: If Eye Blink Count > Threshold value then Display message "Eye blink is present" else display message "Eye blink is not present"

5 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.

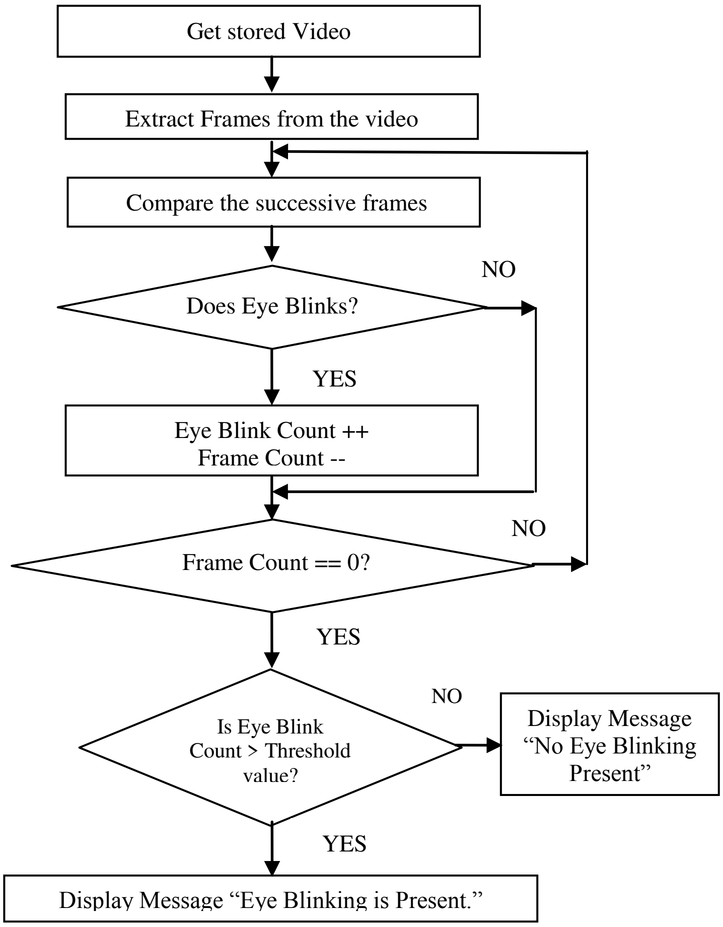

Get stored Video
Extract Frames from the video
Compare the successive frames
Does Eye Blinks?
NO
YES
Eye Blink Count ++
Frame Count --
Frame Count == 0?
NO
YES
Is Eye Blink Count > Threshold value?
NO
Display Message "No Eye Blinking Present"
YES
Display Message "Eye Blinking is Present."

Fig.4 Detection of Eye Blinking

V.RESULTS AND DISCUSSIONS

In the existing system, there is particular interest in considering the quality of the captured image to distinguish the real face or spoofed face. Also the existing is not detecting the spoofing medium and liveness of the face. The proposed system detects the real or spoofed face by extracting the SURF and MSER features from the image. It also detects the spoofing medium by considering the intensity of image. Also by comparing the successive frames from the captured video, it finds the liveness.

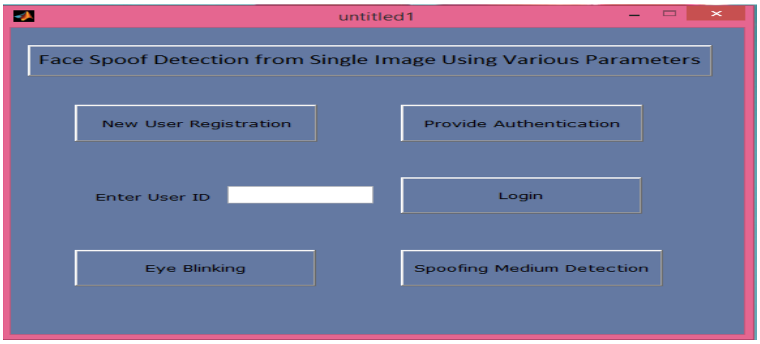
The Fig.5 is a home screen of the system. The pushbutton New User Registration is for the user is not an existing user and using the system first time. By clicking this button, the new user can do the registration of his/ her image and get the User ID.

The pushbutton Provide Authentication is used to check whether the registered face is human face or not.

The pushbutton Login is used to do login for already existing user. By pressing this button, it checks whether the user is authenticate or unauthenticated.

The pushbutton Spoofing Medium Detection is used to detect the spoofing medium.

The pushbutton Eye Blinking is used to detect the liveness.


untitled1

Face Spoof Detection from Single Image Using Various Parameters

Fig.5 Home screen of the system

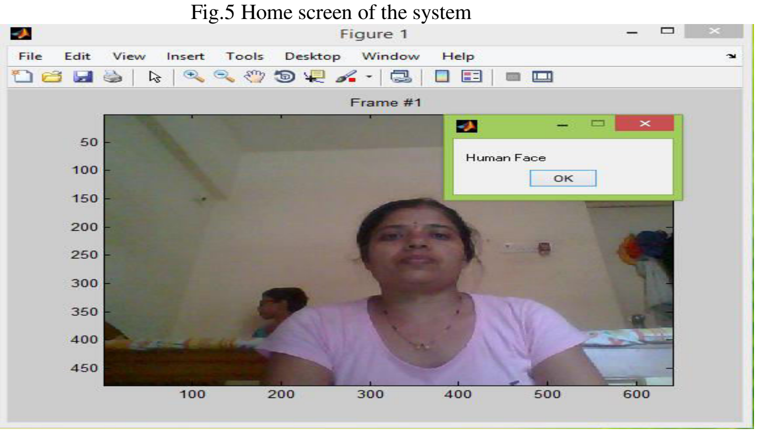


Figure 1

Frame #1

Human Face

Fig.6 Detect Human Face

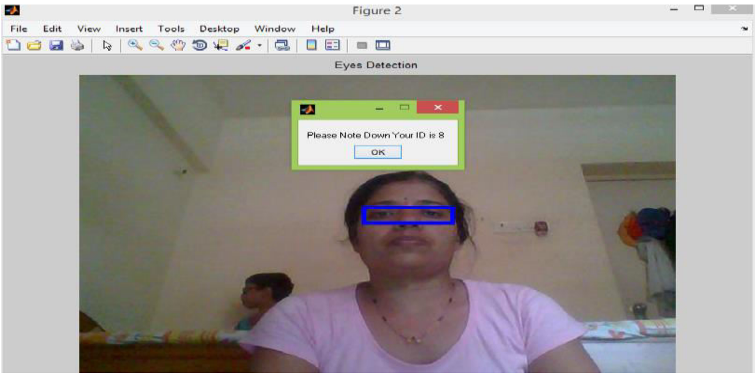


Figure 2

Eyes Detection

Please Note Down Your ID is 8

Fig.7 Display User ID

Fig.6 and 7 occurs by pressing the New User Registration button. It detects whether the registered user is human or not by extracting facial features. After that it displays the User ID for the new registered user.

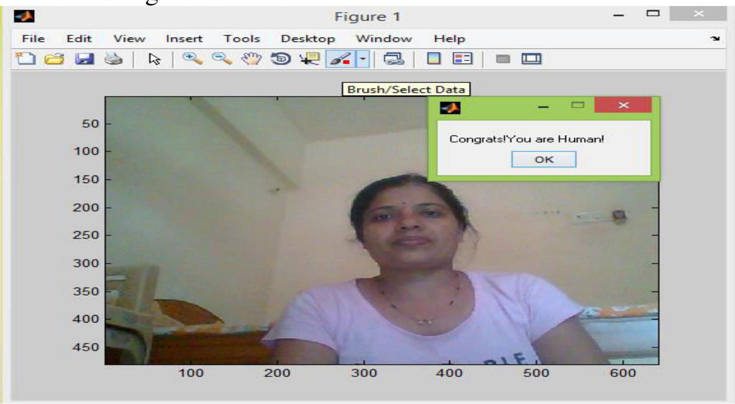
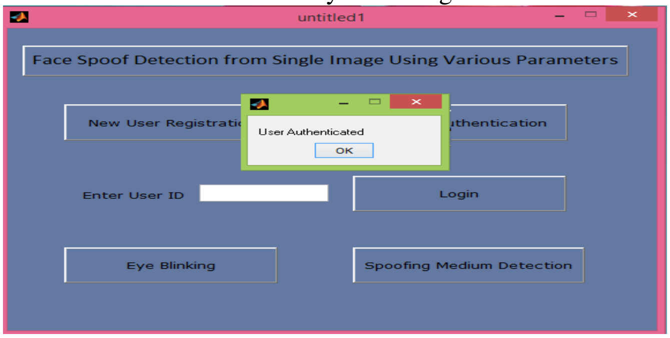


Figure 1

Congrats!You are Human!

Fig.8 Provide Authentication

The fig.8 occurs by pressing the Provide Authentication button which asks for providing authentication and checks if the face is human face or not by extracting the facial features.


untitled1
Face Spoof Detection from Single Image Using Various Parameters
New User Registrati
thentication
Enter User ID
Login
Eye Blinking
Spoofing Medium Detection
OK

User Authenticated

Fig.9 Authenticate the user

Fig. 9 occurs by pressing the Login button. It checks whether the person is authenticated or not.

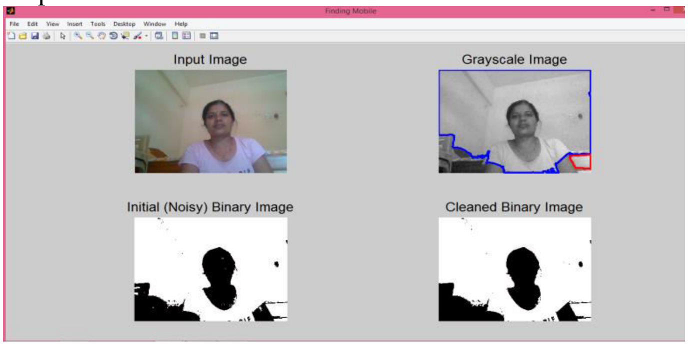
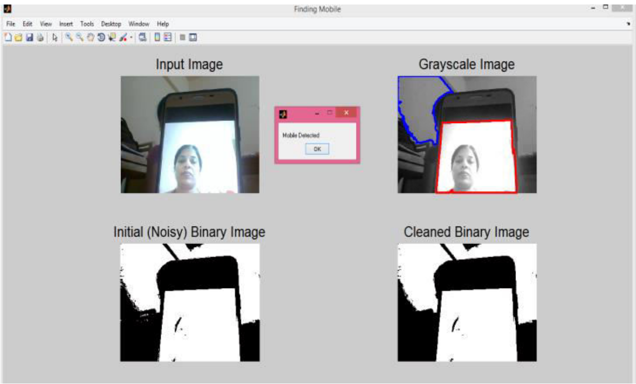

Finding Mobile
File Edit View Insert Tools Desktop Window Help
Input Image
Grayscale Image
Initial (Noisy) Binary Image
Cleaned Binary Image

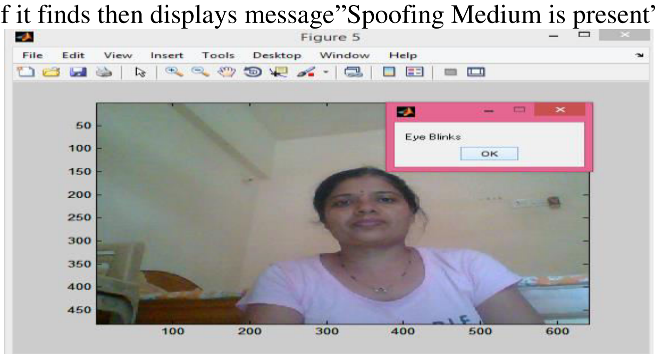
Fig.10 Extract Facial Features and Detect spoofing medium


Finding Mobile
File Edit View Insert Tools Desktop Window Help
Input Image
Grayscale Image
Initial (Noisy) Binary Image
Cleaned Binary Image
OK

Mobile Detected

Fig.11 Extract Facial Features and Detect spoofing medium

Fig. 10 and 11 occurs when Spoofing Medium Detection button is clicked. It checks for the boundaries around the face. If it finds then displays message"Spoofing Medium is present".



Eye Blinks

Fig.12 Detection of Eye Blinking

The Fig. 12 occurs by pressing the Eye Blinking button. It compares all the successive frames and if the Eye blink count is greater than the threshold value then displays message "Eye Blinks".

VI .CONCLUSION AND FUTURE SCOPE

Our system is used to detect the spoofed face and medium. The spoofed faces have different features than the real face. This can be detected by extracting the facial features. The image captured during registration can be used after certain period by considering few features from face which can never be changed after certain age. As a result, experimental results show that the proposed method has better generalization ability. This system checks the liveness by checking the eye blinking. Along with these it will also detect the spoofing medium. Hence it is more efficient and secure than uni biometric system. The proposed system can be enhanced by considering the lightning conditions of laptop camera.

REFERENCES

[1] 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

[2] Komulainen, Jukka, Software-based countermeasures to 2D facial spoofing attacks.

[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] Nixon K, Aimale V & Rowe R (2008) Spoof detection schemes. In: Handbook of Biometrics,403–423. Springer-Verlag.

[5] 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.

[6] 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.

[7] 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

[8] 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

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

[10] T. de Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel, "LBP–TOP based countermeasure against face spoofing attacks,"Wrkshp,12

[11] T. de Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel, "Can face anti-spoofing countermeasures work in a real world scenario"Proc. ICB

[12] 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.

[13] 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.

[14] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li, "Face liveness detection by learning multispectral reflectance distributions," in Proc. FG, Mar. 2011

[15] 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.

[16] J. Komulainen, A. Hadid, and M. Pietikäinen, "Context based face antispoofing," in Proc. BTAS, Sep./Oct. 2013, pp. 1–8.

[17] G. Chetty, "Biometric liveness checking using multimodal fuzzy fusion," in Proc. IEEE FUZZ, Jul. 2010, pp. 1–8.

[18] N. Kose and J. Dugelay, "Classification of captured and recaptured images to detect photograph spoofing," in *Proc. ICIEV*, May 2012