International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 05, 2020
ISSN: 1475-7192

Real Time Face Liveliness Detection Using Eye Blinking and Illumination Techniques

Samarth Singh, Prajjwal Pandey and Dr.S. Thenmalar

Abstract--- *One of the most widely used system to recognize the authorized person based on behavioral or physical characteristics is the Biometric system. One of the current issues with this system is that it can be easily spoofed. A spoofing attack is nothing but a situation in which a person or a program successfully identifies themselves as another person in order to use the system without the permission of authorized user thus harming or attacking the biometric recognition system. The Biometric system can be easily spoofed by methods such as using face images of the authorized person, masks or videos which are easily available on social media these days. This paper proposes a real time spoof detection method based on illumination and eye blinking technique. The framework is tested on 100 distinctive user appearances. As indicated by the trial results, the proposed framework accomplishes 99% accuracy in liveness detection.*

Keywords--- *Face Liveness Detection, Spoofing Attack, Luminance, Mean RGB, Entropy, S.V.M.*

I. INTRODUCTION

Biometric is a framework which is utilized for distinguishing a person based on physical appearance or on behavioral attributes of an individual. The biometric systems have gained popularity in recent years because it provides more secure and accurate security which helps in managing identity systems across various applications for example attendance systems, personal mobile phones, nuclear facilities and for protective sensitive or confidential data. The primary function of biometric is to verify and confirm an individual's identity thus preventing impostors from accessing protected information and resources [1]. In the proposed work we will be focusing on the facial recognition part of the biometric system. With advancing technology, the biometric frameworks have gotten savvier and easier to understand than before. However, these systems lack anti-spoofing mechanisms or in simpler words are not capable enough to separate between a genuine and a fake face and thus can be easily spoofed using various methods like videos, masks [2],

Identity theft is the most concerning matter in the security industry and biometric systems across the globe and due to this the popularity of biometric systems get affected which in turn demands for the need of robust anti-spoofing systems. There is an immense requirement for safety efforts against parody assaults among the general public as well. Figure 1 gives a brief overview of face liveness detection in real time. At first alertness of the user is checked by checking eye blinking. If the number of blinks are greater than the threshold value then further illumination features are calculated and these are compared with the threshold values if the values crosses the

Samarth Singh, Student, CSE Department, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India.
E-mail: samarth.singh111@gmail.com
Prajjwal Pandey, Student, CSE Department, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India.
E-mail: 268prajjwal @gmail.com
Dr.S. Thenmalar, Faculty, CSE Department, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India.
E-mail: thenmals@srmist.edu.in

DOI: 10.37200/IJPR/V24I5/PR201756
Received: 11 Feb 2020 | Revised: 05 Mar 2020 | Accepted: 18 Mar 2020

threshold values then the face is labeled as fake face. There are three types of spoofing attacks through which these systems can be fooled i)photographic attack [3] in which the attacker tries to spoof the system with the help of a photograph of a genuine user these image can be in a printed form or can be shown through a printed device. ii) video attack [4] : this is an advanced version of photographic attack in which a video of the genuine user is used these videos can be easily found on internet or on any of the social media sites . iii) mask attack In this attack the attack tries to fool the system with a 3D mask of a genuine user's face. Such attack is difficult to detect. The use of depth analysis of the facial region which was the solution to the above attacks which uses 2D surface fails in the case of this threat.

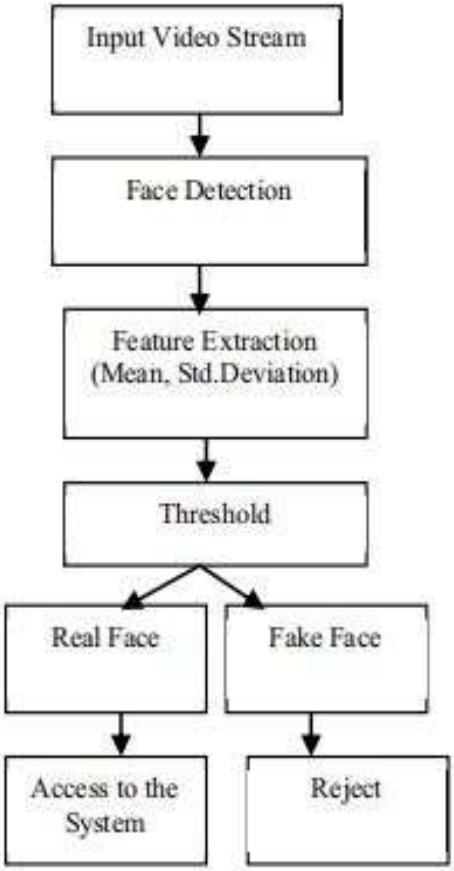


Fig. 1: Overview of Face Liveliness Detection

to detect these spoofing attacks and to overcome the drawbacks in the existing methods this paper proposes an efficient real time technique using eye blinking and illumination characteristics. The proposed method ensures secure FRS, prevents spoof attacks in real time. Using a secure FRS allows prevention of spoof attacks in real time which is elaborated further in more details in the proposed method. The standard deviation of different color channels in a degree of various illumination conditions(illumination features) along with the blinking of the eyes is the main area of focus for this study. Training phase is not necessary in this model thus minimizing complexity and adding to its advantages. Besides, this technique gives better precision in lesser time. Likewise, this strategy can function admirably in an information with partial brightening condition.

DOI: 10.37200/IJPR/V24I5/PR201756
Received: 11 Feb 2020 | Revised: 05 Mar 2020 | Accepted: 18 Mar 2020

II. LITERATURE SURVEY

A. Types of Attacks

Facial spoofing attack is the process with which a user can fool the face recognition system by various methods and thereby can get illegal access to some else privileges or access rights .Some of the methods through which a face recognition system can be fooled are listed below.

1) Photo Attacks. In this attack the attacker attempts to trick the framework by displaying a 2D photo of a genuine client to the recognition system. The image of the user can be taken from a digital camera or may have been taken from the internet if the user has uploaded it on any one of the social media platforms [5]. The picture can be shown on a computerized gadget like telephone, tablet or on a PC or it can be printed on a paper which can be utilized to trick the framework. Further developed photographic assaults that has been is the use of photographic masks [6].These masks contains high resolution image of the genuine user in which space for eyes and mouth are cut out because of which the attacker can make some facial movements of eyes and lips which can easily fool the system.

2) Video Attacks. This attack is the advanced version of photographic attacks and is also referred as replay attacks. In this attack the attacker does not use a static image but uses a video of authentic client which is replayed for a time on a digital device like cell phone, laptop or on a tablet [7],[8]. Such attack is difficult to detect if a high-quality video is used as it not only shows the movements of the facial region but also it gets difficult to differentiate the textures of a live face and fake face.

3) Mask Attacks. In this attack the attack tries to fool the system with a 3D mask of a genuine user's face. Such attack is difficult to detect. The use of depth analysis of the facial region which was the solution to the above attacks which uses 2D surface fails in the case of this threat. Although the probability of the attacker using 3D masks is much less than the above two attacks. Studies on Face mask spoofing are far less than the 2D mask spoofing and they have recently gained more attention. A mask specific dataset has been recently created which includes face masks of different shapes, size and materials [9],[10]. Earlier such attacks were difficult to perform as they required high revenues and professionals to create them but because of fast growing technology such 3D face models can be easily created easily and at a very feasible price.

B. Techniques

1) Texture based Approaches: This approach is used by Gahyum kim t al [11], Sungmin Eum.Their proposed work is to differentiate between a live face and a paper mask based on the structure and shape of the face. The authors have used power spectrum-based method to exploit information from high frequency and low frequency regions. Local Binary Pattern has been used for examining the textures. The justification given for using frequency information is that a 3-D face have different frequency regions because of which there is a irregular illumination component generated by the face and also the images taken from the 2-D objects lacks the high frequency information as well as it suffers from the loss of information as compared to a 3-D face. The feature extraction is done by the one of the most famous technique for finding texture information in a 2-D image, Local Binary Pattern. These extracted features are then given to Support Vector Machine for classifying the image whether it is live or not. The Database

DOI: 10.37200/IJPR/V24I5/PR201756
Received: 11 Feb 2020 | Revised: 05 Mar 2020 | Accepted: 18 Mar 2020

used by authors are BERC ATM Database and BERC webcam Database images in database are captured from prints and are captured in three different light conditions. However the above approach can be spoofed if a very clear and big size image is used to tackle this issue authors have proposed a system in which a group of images are created having every 4th image from the input feed and from these images energy value is computed and using frequency dynamic descriptor the threshold value for temporal changes in the face are computed. The advantage of this system is that it is easy and fast to compute.

2) Variable Focusing based analysis: This approach is used by Sooyen Kim et al[12] for detecting face liveness detection. Their proposed work is to differentiate between a live face and a paper mask based on the variable focusing. The approach used by the authors is by sequentially focusing between two different positions of an image. In case of 2-D images there is not much difference in the focus value when authors tried to focus between the two points of an image whereas in case of 3-D face the values of focus were different at different points this is because face is a 3D structure and has variable depths thus the focused regions are clearer than the surroundings due to variation in depth. The constraint on which this method relies on is the Degree Of Field(DOF).Degree Of Field finds the range between farthest and nearest objects in a focused image. It helps in determining the focus variation of pixels from a focused image. Focusing effect is increased to increase the accuracy of the system. To calculate the focus value Sum Modified Laplacian is used. At first two images are taken and focusing is done at two random points in case of a face focusing is first done on the nose and then on the eyes since nose is closest to camera and mouth is away the focus value calculated by Sum Modified Laplacian is enough to classify the image whether the image is a 2-D image or a real face. Their study showed that when Depth Of Field is very small false rejection rate is zero and this gradually increases as Depth Of Field increases. Hence for better results Depth of Field is kept small.

3) Feature Level Dynamic Approaches: This is one of the first approach used to counter spoofing methods using 2D planes and is still popular against image print attacks. These techniques mainly depend on the different facial movements. One of the spoofing methods based on feature level approach is eye blinking technique and movement of the pupils in humans' eye. This approach is used by Lin Sun et al [13] G. Pan [15]. H.-K. Jee [14]. Various steps are followed in this technique, first step is the centeroid of eyes is found out and the facial area except the eyes are normalized. After extracting the eye region, they are compared with the images taken over a time period to check the variation in them. If the result crosses the threshold value, then the input is considered as a live image or else it is classified as a fake image. To extract the eye region Gaussian filtering is done to the face because of which a much smoother 3D image is formed. All invalid regions excluding eye are removed using an eye classifier. Viola's AdaBoost methods are used for training this classifier. After this face region is normalized by a particular size as faces are of different sizes and from these face regions, eye regions are extracted. Hamming distance method is then used to compare the sequentially extracted images. Hamming distance is defined by the number of pixels that have different values. If the hamming distance crosses the threshold value the input is considered as live. The experimental result has showed that mean hamming distance of a real face is 30 and that of fake face is 17. Other feature level approach that is used to classify a person whether he is live or not is through lip movement technique. This technique is used by Kooreider et al[7]. The authors have first located the mouth region and then extracted OFL. SVM classifier

DOI: 10.37200/IJPR/V24I5/PR201756
Received: 11 Feb 2020 | Revised: 05 Mar 2020 | Accepted: 18 Mar 2020

is used and 60 videos are recorded for testing purpose and feature vectors are extracted from the mouth region and are fed to SVM classifier. The accuracy achieved in this work is of 73 percent.

4) Optical Flow based analysis: This aapproach is used by Bao et al [16], kollreider et al [17] the authors have classified a fake face image with a live face based on the optical flow. This optical flow is a compilation of four movements moving, rotating, translation and swing. Except swing all other have same optical flow fields for both 2D and 3D images. The authors have conducted the experiment by studying optical flow lines of a constant distance observer, rotation of about perpendicular and view axis and by moving the object forward and backward. The optical flow Fields of a human face are in random directions whereas that of a 2D surface are in uniform directions based on these the liveness of a person can be detected. But This method will fail if illumination of an image changes frequently and this method will not work against 3D objects. Kollreider et al have proposed the method to track and study trajectories of different regions of face. This can be used to detect whether a spoofing attempt was made or not. The basic idea which this method follows is that the regions which are closer to the face generates different motion than the regions that are far away hence nose will create different motion than ears whereas in a 2D image will always create a constant motion for all the regions. Thus, with the knowledge of the movement speed and the positions of face parts liveness data can be easily predicted. For this authors have used main Gabor filters for detecting edges and optical flow pattern matching. This system was tested against the database which contained hundred videos of head rotations.The proposed system have the error rate of 0.75%.

5) Component Dependent Descriptor based analysis: This technique is used by Jianwei yang [18]. The steps followed by author for detecting liveness are at first the face is split into six different parts which includes left eye area, right eye area, nose area, mouth area and facial area. The authors have analyzed that micro textures are important for liveness detection. Capturing a face by camera and capturing a printed photo by camera produces very different results based on micro textures this is mainly because of vary in appearance change in reflection caused by gamma correction and due to limited resolution of images. Local Binary Pattern (LBP), Local Phase Quantization (LPQ) and histogram of oriented gradients are found out. Component based coding is performed on these extracted features. Then weights are assigned to these features and dissimilarity of micro textures between real and fake images are found out based on the Fisher criterion analysis. The classifier used in this method is SVM. The provided algorithm is experimented and tested on CASIA, Print-Attack and NUAA database.

6) Binary classification-based analysis: This approach is used by Tan et al [19], Peixoto et al [20]. The authors have stated that the live face and an image are different from each other in two ways first both are different in dimensions and second is that the surface of a live face is different from the surface of a image. This in combination with the noise, illumination makes the real face and a photo face different. In this Lambertian model is used to extract important information about the surface of a image or live face. The latent samples are withdrawn by two methods namely Gaussian based method and Variation Retinex-based Method. In Gaussian based printer and camera, it gets deformed and has lower image quality compared to live face and thus it fails in having high frequency details. The authors have formulated this problem as a binary classification problem and sparse logistic regression is used as a classifier for classifying the data. To test this model authors have used a database with fifty thousand of images and they have also tested the model against NUAA database. But in this model Authors have failed to deal with the

DOI: 10.37200/IJPR/V24I5/PR201756
Received: 11 Feb 2020 | Revised: 05 Mar 2020 | Accepted: 18 Mar 2020

images having bad illumination surroundings because of which there was problem in determining the borders of an image when projected from an LCD screen as high frequency areas were getting blurred due to reflection. To solve this problem Peixoto et al has proposed to prefilter the image to normalize the image.

III. PROPOSED WORK

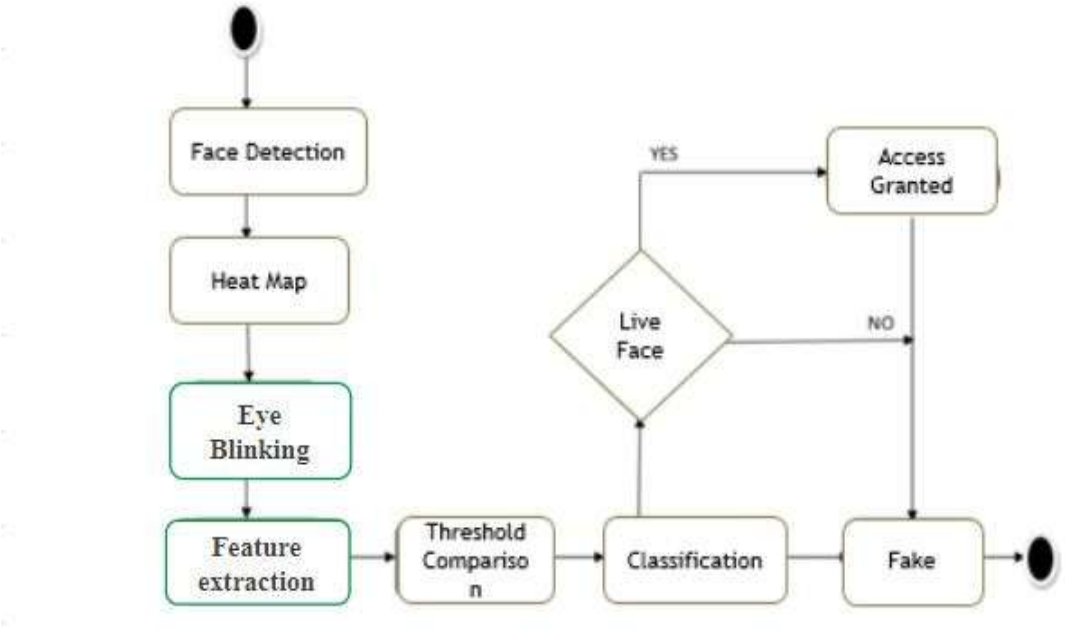


Fig. 2: Flow diagram

This framework works in real time. Picture of client is captured from live video. As shown in figure 2, Camera Opens up and starts processing the video and each frame is recorded. This input frame is used for testing the liveness. For detecting face in an input image Viola jones algorithm is used. Which uses S.V.M Classifier to detect faces and mark the points on the faces for eye detection. It is one of the best algorithms which can be used for object detection in real time. This method is proposed by Paul Viola and Michael Jones [21]. It is essentially created for face detection. The main reason for choosing this algorithm is because of its robustness and speed[22].

Importing and Getting Data: 50th frame image is taken so that the system can adjust to the light level this is done using getimage() function

Modules Description

1. Feature Extraction

1.1) luminance calculation

Luminance of a picture is characterized as density of live light leaving from a surface in some particular direction. As face is a 3-D structure hence value of luminance for each part of face varies. Luminance of a picture can be found out through the following steps. Image is converted into an array using Image.formarray(im), and

DOI: 10.37200/IJPR/V24I5/PR201756
Received: 11 Feb 2020 | Revised: 05 Mar 2020 | Accepted: 18 Mar 2020

using ImageStat.Stat(im) we can find the mask and calculate the statistics for the given image. If there is a a mask present in the input then the area covered by the mask is on ly taken into consideration. After that getting the mean values of each band and multiplying with the specific values, we will get the luminance.

◊(0.299*(r) + 0.587*(g) + 0.114*(b))

1.2) Energy

Energy of face can be determined using following steps. For assessing vitality of picture, picture should go through some pre-forms like select just single channel of picture, on this fourier transform is applied, log of past value is found out and afterward finally summarize all qualities for finding energy of an image

1.3) Entropy

Entropy is a factual proportion of irregularity that can be utilized to describe the surface of the information picture. Entropy of picture can be determined at every pixel position (i, j). for determining the entropy, RGB picture ought to be changed over in grayscale picture.

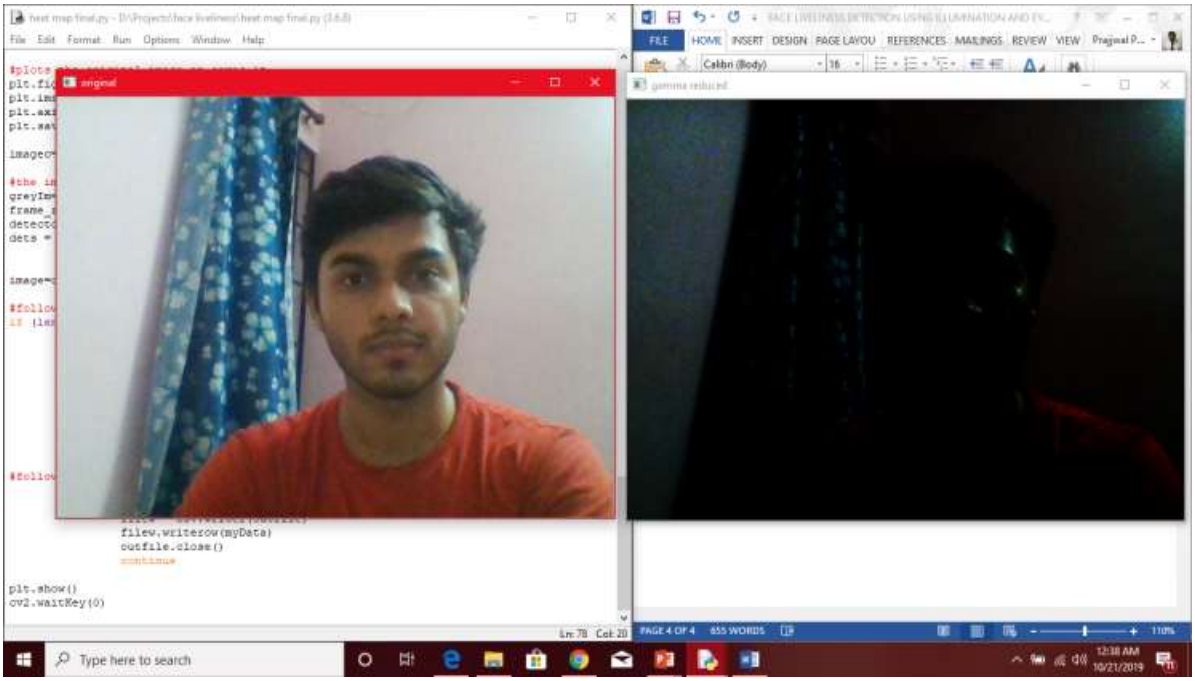


Fig. 3: Grey scale converted image

1.4) Mean RBG

Picture is comprised of three essential shading segments Red, Green and Blue. These three parts can be isolated from a picture and their value can be determined utilizing picture handling tools. Mean estimation of these segments is used for determining face liveness.

1.5) Mean YCbCr

This can be found out by using RGB elements [23].

DOI: 10.37200/IJPR/V24I5/PR201756
Received: 11 Feb 2020 | Revised: 05 Mar 2020 | Accepted: 18 Mar 2020

y= .299 * r + .587 * g + .114 * b

cb= 128 - .169 * r - .331 * g + .5 * b

cr= 128 + .5 * r - .419 * g - .081 * b

2. Heat Map

Converting our image into heat map. First, we will convert our image to gray scale image. Then we will get the shape of the image i.e height, width and channels where height represents the number of pixel rows in the image or the number of pixels in each column of the image array and width represents the number of pixel columns in the image or the number of pixels in each row of the image array. Then making the array of gray scale image in order to get lower and upper value of pixels along x axis and y axis by using above shape values and then flatten() them into single dimension so that entropy can be calculated. Then the entropy values are calculated using entropy function for each pixel value and stored into an array of row and column. We will apply the colour map. The colour map can be applied using the lookup table in the gamma function which will return the lookup table. Entropy and gamma reduced images are saved in order to record the liveliness. Then the gamma image is converted into greyscale image and resized.

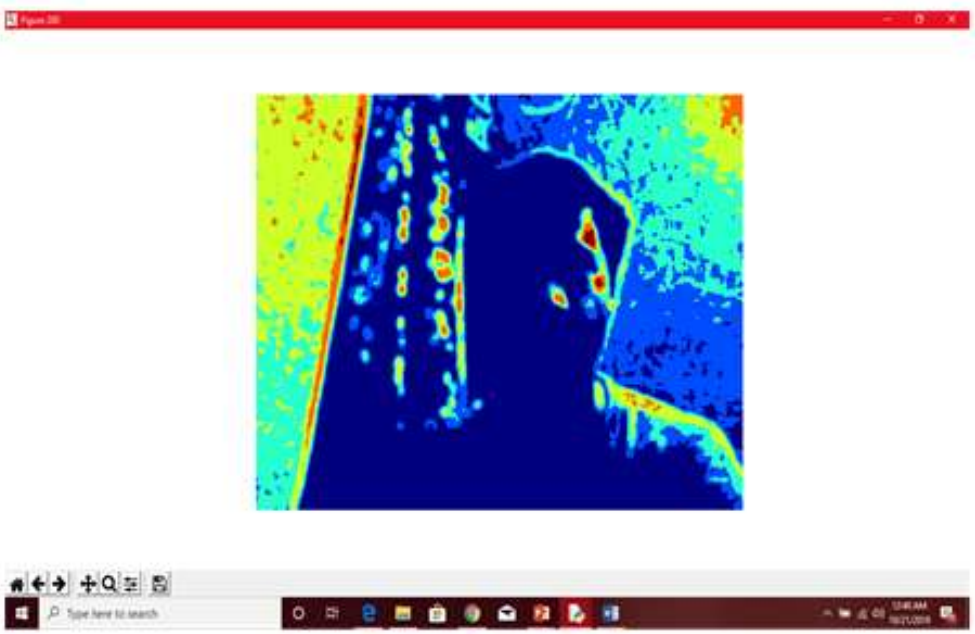


Fig 4: Heatmap converted image

3. Eye Blinking Check

$$\mathrm{EAR} = \frac{\|p_2 - p_6\| + \|p_3 - p_5\|}{2\|p_1 - p_4\|}$$

DOI: 10.37200/IJPR/V24I5/PR201756
Received: 11 Feb 2020 | Revised: 05 Mar 2020 | Accepted: 18 Mar 2020

Euclidean distances is computed between the two sets of vertical eye landmarks. Then the Euclidean distance between the one pair of horizontal eye landmarks are computed. Then two constraints are defined one for checking eye aspect ratio and other for counting eye blinks The eye opening state is being determined by the ratio called eye aspect ratio. It determines the state of the eye as it is a constant value which falls to 0 when the eye is closed and a constant value when the eye is open. The Library that is used to determine the location of 68 coordinates (x,y) on the face of a person is called dlib which maps the facial points on person's face. Dlib is used to detect faces and has pre-trained models. The dataset named iBUG300-W is used to identify these points. Dlib's pre-trained face detector is initialized based on modification to the standard i.e Histogram of Oriented Gradients and Linear SVM. slider slides on whole image and trained on SVM on both positive and negative examples) method for object detection The input frame is converted into grey scale and then then face is detected in this grey scale image from this image facial coordinates are converted into an NumPy array From this the eye aspect ratio is calculated and if the value reaches zero then the number of blinks are incremented.

Fig. 5: Eye blinking check

4. Classification

When the system starts its execution and if there are multiple faces present then it captures only one face at a time, The face which is closest is processed using face detector. All the above mentioned features values are calculated and are temporarily saved for comparison. There are predefined values stored in the database for fake and live face images. At first number of eye blinks are checked if the system finds the number of eye blinks less than the threshold value then the input is not further processed and the input is categorized as a fake input. If the eye blinking value lies in the range of pre-defined values then all other chromatic modules are calculated these modules are further tested against the threshold values and accordingly the input is categorized as live or fake. Working of framework is straight forward on the grounds that there is no need of human interaction once program starts its execution.

IV. EXPERIMENTAL RESULTS

Our system not only successfully passed all the spoofing attacks but also checked for alertness. By calculating the entropy, rgb, luminance and number of eye blinks.

DOI: 10.37200/IJPR/V24I5/PR201756
Received: 11 Feb 2020 | Revised: 05 Mar 2020 | Accepted: 18 Mar 2020

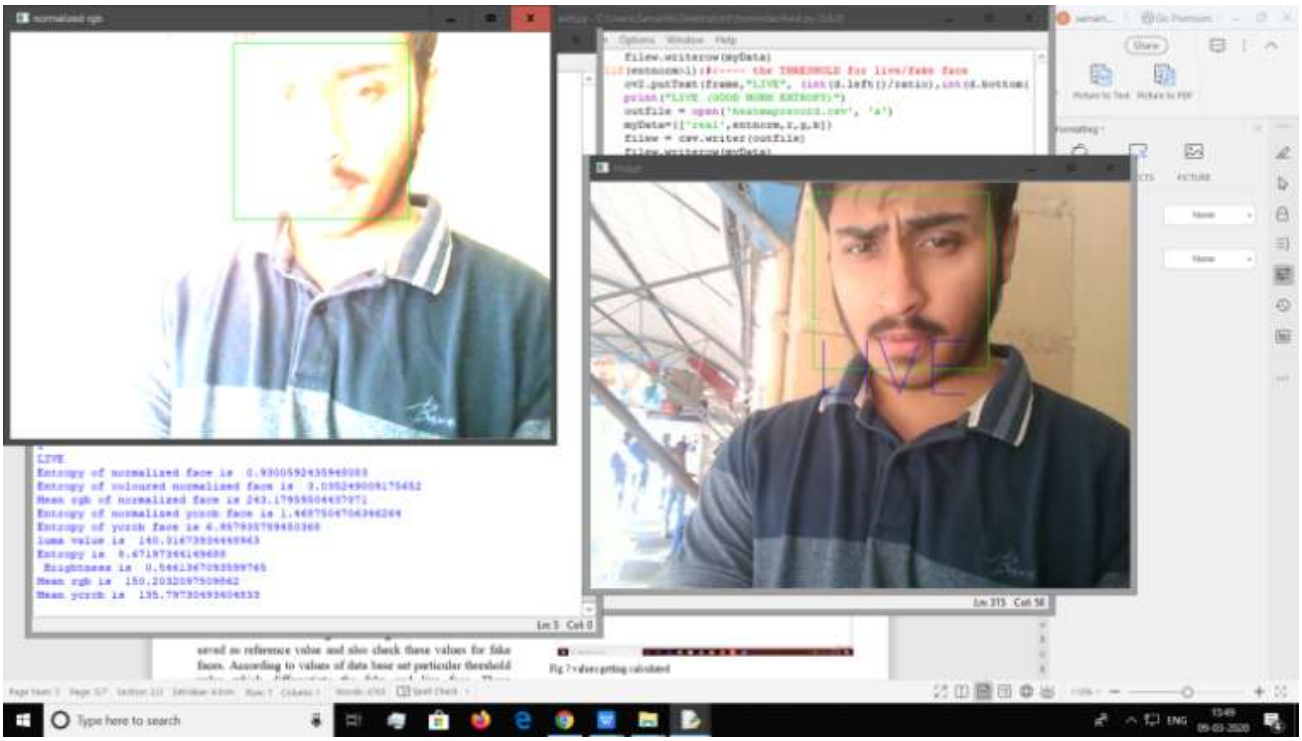


Fig. 6: Liveness testing in outdoor environment

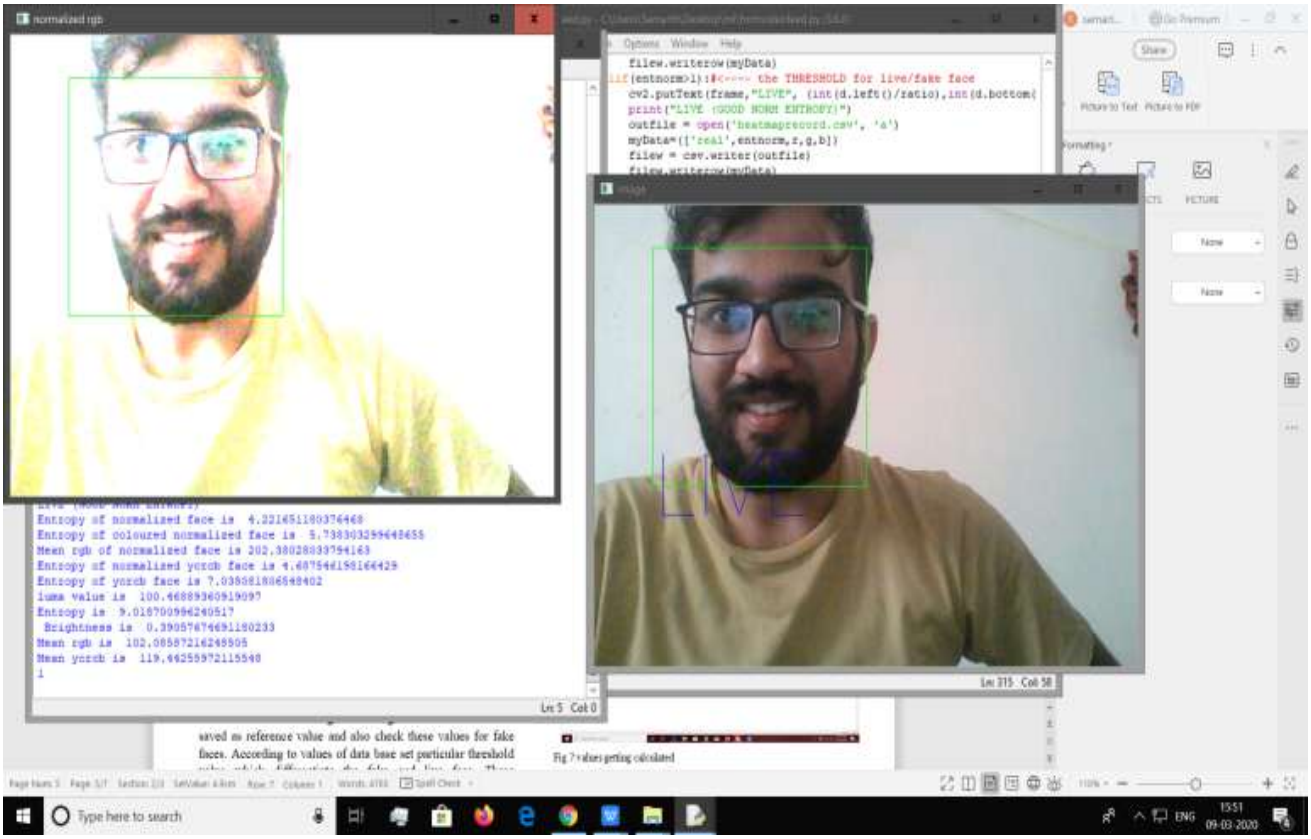


Fig. 7: liveness testing in indoor environment

DOI: 10.37200/IJPR/V24I5/PR201756
Received: 11 Feb 2020 | Revised: 05 Mar 2020 | Accepted: 18 Mar 2020

This system is tested on 100 unique users. The system is tested in both indoor and outdoor environment and in various light conditions. At first face is detected then the modules stated above are applied and the live and fake results are stored in an excel file.

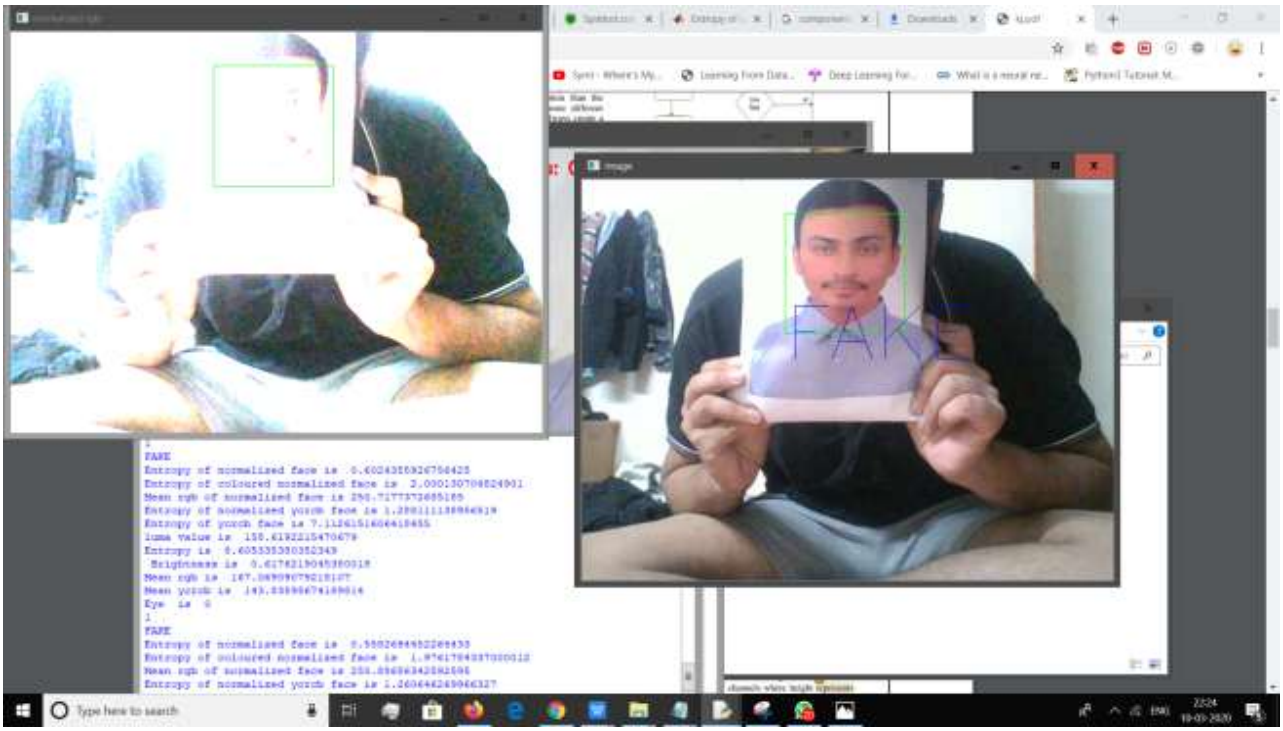


Fig. 8: Photo attack test

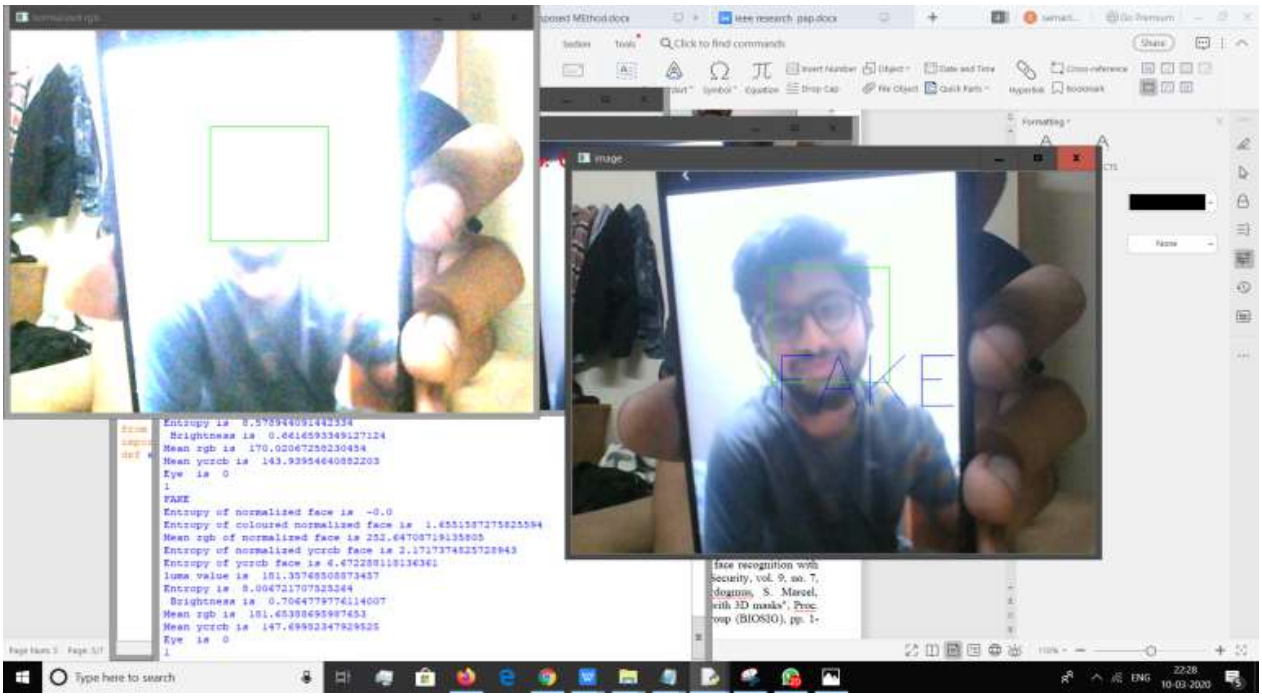
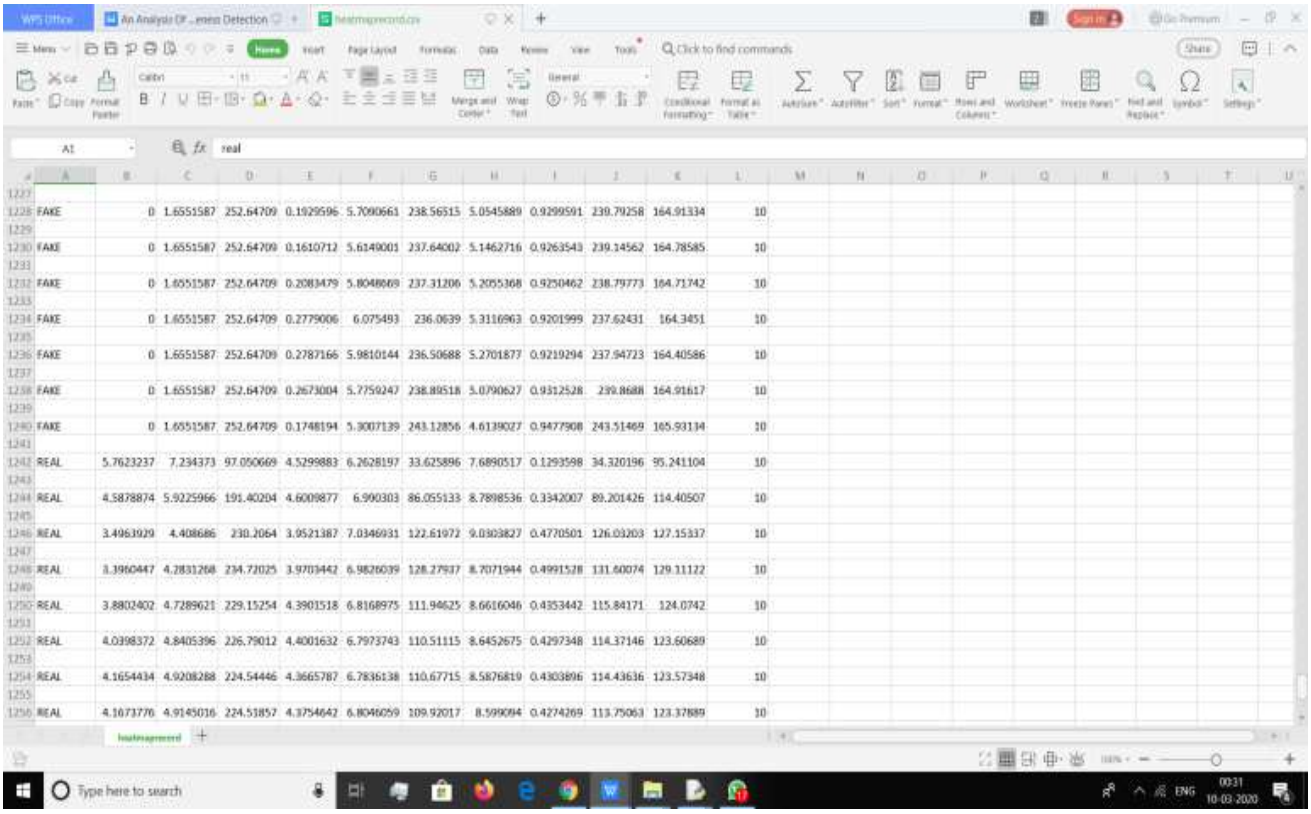


Fig. 9: Video attack test

DOI: 10.37200/IJPR/V24I5/PR201756
Received: 11 Feb 2020 | Revised: 05 Mar 2020 | Accepted: 18 Mar 2020



FAKE	0	1.6551587	252.64709	0.1929596	5.7090661	238.56515	5.0545889	0.9299591	239.79258	164.91334	10	
FAKE	0	1.6551587	252.64709	0.1610712	5.6149001	237.64002	5.1462716	0.9263543	239.14562	164.78585	10	
FAKE	0	1.6551587	252.64709	0.2083479	5.8048669	237.31206	5.2055368	0.9250462	238.79773	164.71742	10	
FAKE	0	1.6551587	252.64709	0.2779006	6.075493	236.0639	5.3116963	0.9201999	237.62431	164.3451	10	
FAKE	0	1.6551587	252.64709	0.2787166	5.9810144	236.50688	5.2701877	0.9219294	237.94723	164.40586	10	
FAKE	0	1.6551587	252.64709	0.2673004	5.7759247	238.89518	5.0790627	0.9312528	239.8688	164.91617	10	
FAKE	0	1.6551587	252.64709	0.1748194	5.3007139	243.12856	4.6139027	0.9477908	243.51469	165.93134	10	
REAL	5.7623237	7.234373	97.050669	4.5299883	6.2628197	33.625896	7.6890517	0.1293598	34.320196	95.241104	10	
REAL	4.5878874	5.9225966	191.40204	4.6009877	6.990303	86.055133	8.7898536	0.3342007	89.201426	114.40507	10	
REAL	3.4963929	4.408686	230.2064	3.9521387	7.0346931	122.61972	9.0303827	0.4770501	126.03203	127.15337	10	
REAL	3.3960447	4.2831268	234.72025	3.9703442	6.9826039	128.27937	8.7071944	0.4991528	131.60074	129.11122	10	
REAL	3.8802402	4.7289621	229.15254	4.3901518	6.8168975	111.94625	8.6616046	0.4353442	115.84171	124.0742	10	
REAL	4.0398372	4.8405396	226.79012	4.4001632	6.7973743	110.51115	8.6452675	0.4297348	114.37146	123.60689	10	
REAL	4.1654434	4.9208288	224.54446	4.3665787	6.7836138	110.67715	8.5876819	0.4303896	114.43636	123.57348	10	
REAL	4.1073776	4.9145016	224.51857	4.3754642	6.8046059	109.92017	8.599094	0.4274269	113.75063	123.37889	10	

Fig. 10: Excel file storing results

V. CONCLUSION

In this study, illumination and eye blinking based technique is used for detecting face liveness. A real time web camera is used for detecting eye blinking and for calculating above mentioned modules for detecting the liveness. The novelty of out proposed work lies in two folds, at first we check the alertness of the user by checking whether the user is blinking eye or not, Secondly to further improve the performance we calculate various illumination modules from the input live feed. This system is tested on 100 different users in various light conditions and environment. In light of the trial results 99% face liveness detection precision is accomplished in a remarkable time which is better than the other existing techniques. Our future work will focus on improving accuracy with less features and on more accurately detecting eye blinking with glasses on.

REFERENCES

[1] J.A. Unar, W. C. Seng, A. Abbasi. "A review of biometric technology along with trends and prospects," *Pattern Recognition*, 2014, 47(8):2673-2688.

[2] J. Maatta, A. Hadid, M. Pietikainen, Face Spoofing Detection From Single images Using Micro Texture Analysis, *Proc. International Joint Conference on Biometrics (UCB 2011), Washington, D.C.,USA*

[3] S. Chakrabroty, D. Das. "An Overview of Face liveness Detection, "*International Journal on Information Theory*, 2014, 3(2):11-25

[4] P. P. K. Chan, W. Liu, D. Chen, D. S. Weung, F. Zhang, X. Wang, et al. "Face liveness Detection Using a Flash Against 2D Spoofing Attack," *IEEE Transactions on Information Forensics and Security*, 2018, 13(2):521-534.

DOI: 10.37200/IJPR/V24I5/PR201756
Received: 11 Feb 2020 | Revised: 05 Mar 2020 | Accepted: 18 Mar 2020

[5] Y. Li, K. Xu, Q. Yan, Y. Li, R. H. Deng, "Understanding OSN-based facial disclosure against face authentication systems", *Proc. ACM Asia Symp. Inf. Comput. Commun. Security (ASIACCS)*, pp. 413-424, 2014.

[6] K. Kollreider, H. Fronthaler, J. Bigun, "Evaluating liveness by face images and the structure tensor", *Proc. IEEE Workshop Autom. Identificat. Adv. Technol. (AutoID)*, pp. 75-80, Oct. 2005

[7] 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.[8] I. Chingovska, A. Anjos, S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing", *Proc. IEEE Int. Conf. Biometrics Special Interest Group (BIOSIG)*, pp. 1-7, Sep. 2012

[8] N. Erdogmus, S. Marcel, "Spoofing face recognition with 3D masks", *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 7, pp. 1084-1097, Jul. 2014.

[9] N. Erdogmus, S. Marcel, "Spoofing 2D face recognition systems with 3D masks", *Proc. Int. Conf. Biometrics Special Interest Group (BIOSIG)*, pp. 1-8, Sep. 2013.

[10] G. Kim, S.Eum, J. K. Suhr, D. I. Kim, K. R. Park, and J, Kim, Face liveness detection based on texture and frequency analyses, *5th IAPR International Conference on Biometrics (ICB)*, New Delhi, India. pp. 67-72, March 2012

[11] Sooyeon Kim, Sunjin Yu, Kwangtaek Kim, Yuseok Ban, Sangyoun Lee, Face liveness detection using variable focusing, Biometrics (ICB), *2013 International Conference on*, On page(s): 1 – 6, 2013.

[12] Lin Sun, Gang Pan, Zhaohui Wu, Shihong Lao, Blinking-Based Live Face Detection Using Conditional Random Fields, ICB 2007, Seoul, Korea, International Conference, on pages 252-260, August 27-29, 2013.

[13] H. K. Jee, S. U. Jung, and J. H. Yoo, Liveness detection for embedded face recognition system, *International Journal of Biological and Medical Sciences*, vol. 1(4), pp. 235-238, 2006

[14] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," *in Proc. ECCV*, 2010, pp. 504–517.

[15] Wei Bao, Hong Li, Nan Li, and Wei Jiang, A liveness detection method for face recognition based on optical flow field, In Image Analysis and Signal Processing, 2009, IASP 2009, International Conference on, pages 233 –236, April 2009.

[16] K. Kollreider, H. Fronthaler, J. Bigun, "Evaluating liveness by face images and the structure tensor", *Proc. IEEE Workshop Autom. Identificat. Adv. Technol. (AutoID)*, pp. 75-80, Oct. 2005.

[17] Jianwei Yang, Zhen Lei, Shengcai Liao, Li, S.Z, Face Liveness Detection with Component Dependent Descriptor, Biometrics (ICB), 2013 International Conference on Page(s): 1 – 6, 2013

[18] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," *in Proc. ECCV*, 2010, pp. 504–517.

[19] B. Peixoto, C. Michelassi and A. Rocha, Face liveness detection under bad illumination conditions, *In ICIP*, pages 3557-3560, 2011.

[20] P. Viola, and M. J. Jones, "Robust real-time face detection, "*International journal of computer vision* 57.2 (2004): 137-154.

[21] Reese, K., Zheng, Y., Elmaghraby, A.: A comparison of face detection algorithms in visible and thermal spectrums. *In: International Conference on Advances in Computer Science and Application* (2012)

[22] D. Wen, H. Han, and Anil K. Jain, "Face spoof detection with image distortion analysis," *IEEE Transactions on Information Forensics and Security* 10.4, 746-761, 2015.

DOI: 10.37200/IJPR/V24I5/PR201756
Received: 11 Feb 2020 | Revised: 05 Mar 2020 | Accepted: 18 Mar 2020