International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 08, 2020
ISSN: 1475-7192

An Analysis of Anti-Spoof Mechanisms in Face Liveness Detection

[1]Samarth Singh, [2]Prajjwal Pandey, [3]Thenmalar S

Abstract--*One of the most generally used framework to recognize the authorized person based on behavioral or physical characteristics is the Biometric system. One of the present 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. In this analysis, categorization of face liveness detection is done based on different techniques used for detecting spoofing attacks. This helps in inferring various developed solutions and spoofing attacks associated with them. An investigation of late examinations in the field of face liveness discovery has been laided to provide a simple and clear path for future improvement in the field of face liveness detection.*

Key words--*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 imposters from accessing protected information and resources. Traditionally, the biometric identification systems used chemical information from a person such as DNA, hair strand [1] etc. in order to recognize or identify a person. More general techniques to confirm an individual's identity included passwords or ID cards which can get lost, stolen or tampered thereby undermining the intended security. With advancing technology, the biometric acknowledgment frameworks have gotten more savvy and easy to understand than before. As a result, such biometric frameworks are widely utilized for security purposes worldwide and is one of the quickest developing division of the security business. The complexity of these progressively smart biometric frameworks have arrived at a point where they can undoubtedly distinguish an individual by his/her particular attributes, for example, the facial patterns, retinal and iris acknowledgment, unique mark acknowledgment, handwriting, hand geometry and so on. Compared to the traditional biometric systems these more intelligent versions of the biometric system are easy to use and convenient for the user. Among different strategies, the one which has gained more prominence than the others

[1]*Student, CSE Department, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India, samarth.singh111@gmail.com*
[2]*Student, CSE Department, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India, 268prajjwal@gmail.com*
[3]*Faculty, CSE Department, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India, thenmals@srmist.edu.in*

DOI: 10.37200/IJPR/V24I8/PR280259
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

is the facial recognition technology innovation in light of its explicitness and ease of use over other methods. 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], photographs or pictures.

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. To solve this problem many methods have been tried and tested. These can be split into two categories: Methods which require external hardware and methods that work solely on software [3]. The software-based methods consist of two mainstream methods: intrusive methods and non-intrusive methods. Among these methods, face is the most frequently used biometric feature because it contains enough textural and color information. On the successful detection of a face, the image is pre-processed and a lot of different kinds of facial features are extracted and merged for classification of the input. Only the real, live faces will be accepted and sent for further authentication and processing. One of the major and the most common threats to face liveness detection is the Photo attack [4] since photos can be obtained easily and look nearly like the live faces from a point of view. Mask attack, video attack, model attack and so on are some of the other types of powerful spoof attacks. Hence in order to overcome such spoofing attacks, liveness detection is preferred and created.

II. DATASETS AND TECHNIQUES IN FACE LIVENESS DETECTION

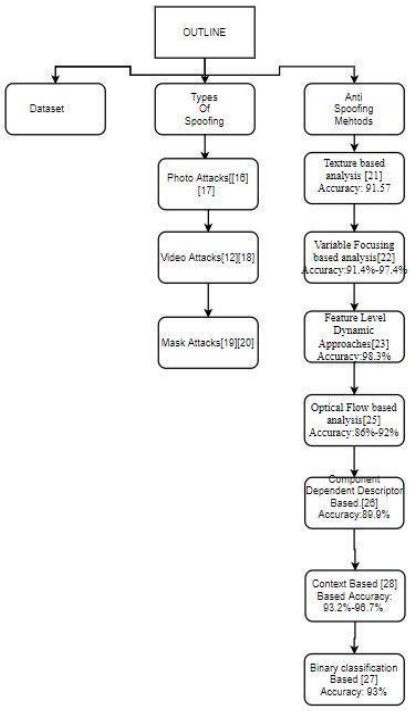

Figure 1: A brief overview of different Datasets and Techniques available in Face Liveness Detection. The methods are tested on different datasets and under different conditions and thus the accuracy may vary according to them.

DOI: 10.37200/IJPR/V24I8/PR280259
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

Datasets

NUAA- Nanjing University of Aeronautics and Astronautics: NUAA database contains collection of photographs taken from cheap web cameras [5-8]. It contains real and fake samples of fifteen subjects. The database is created in three phases with two weeks of time in each phase. Photographs are taken in various illumination conditions. The database contains 2383 pictures of real faces and 3912 pictures of fake samples each having definition of 640 x 480 pixels.

REPLAY ATTACK: Replay attack is a challenging dataset which is created by Idiap Research Institute, in Switzerland. This dataset contains various attack scenarios such as replaying the video, 2D printed photograph attack and cell phone photograph attack displayed on the screen[9-11].The database is created with the help of 50 clients and contains 1300 video clips of video and photographic attacks having resolutions of 320 by 240 pixels.

CASIA FASD: CASIA dataset CASIA is the second largest database available for face recognition and verification problems for the public. The dataset contains a total of 494,414 samples in total. This dataset is used for research purposes of face recognition [12-14]. Dataset is created with the help of 10,575 subjects. It contains both real and spoof attacks in various qualities and scenarios. It contains printed photo attack, cut photo attack and replay video attacks.

PRINT-ATTACK DB - This database is created by IDIAP Research Institute is available to public and is very often used in facial spoofing research process [15]. 50 subjects are used to create this database. The database has 200 videos of live faces and 200 videos of fake 2D photographs. The database is divided into sub parts consisting of Training data to train classifier, spoofing data to test the algorithm, Test data to find errors and Development data which is used to estimate threshold. Videos recorded in this database are recorded in various light conditions, one with uniform lighting and background and second with non-uniform background and light conditions.

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. 2.2.1. 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 [16]. 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 [17].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.

DOI: 10.37200/IJPR/V24I8/PR280259
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

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 [12],[18]. 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.

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 [19],[20]. 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. Furthermore, now a person can create a face mask by himself with the help of affordable 3D printer.

Techniques

Texture based Approach:

This strategy is utilized by Gahyumkim t al [21], SungminEum. Their proposed work is to separate between a live face and a paper mask dependent 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 districts. Local Binary Pattern has been used for examining the textures. The justification given for utilizing recurrence data is that a 3-D face have diverse frequency areas as a result of which there is a irregular frequency segment created by the face and furthermore the pictures of 2-D objects does not have the high frequency data just as it experiences the loss of data when contrasted with a 3-D face.. The feature extraction is done by the one of the most renowned strategy for discovering surface data in a 2-D picture, LB. These extricated highlights are then given to Support Vector Machine for grouping the picture whether it is live or not. The Database utilized by creators are BERC ATM Database and BERC webcam Database.

Pictures in these databases are captured from prints and are caught in three distinctive light conditions However the above methodology can be parodied if an extremely clear and large size picture is utilized. To tackle this issue authors have proposed a framework in which a gathering of pictures are made having each fourth picture from the information 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.

DOI: 10.37200/IJPR/V24I8/PR280259
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

Variable Focusing based analysis:

This approach is used by Sooyen Kim et al[22] for detecting face liveness detection. Their proposed work is to recognize a live face and a paper cover dependent on the variable focusing. The methodology utilized by the creators is by consecutively focusing between two unique places of a picture. 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). DegreeOf 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 is sufficient to characterize the picture whether the picture is a 2-D picture or a genuine face.. Their study showed that when Depth of Field is very small false rejection rate is zero and this step by step increments as Depth Of Field increases. Henceforth for better outcomes Depth of Field is kept small.

Feature Level Dynamic Approach:

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 methodology is utilized by Lin Sun et al [23] G. Pan [6]. H.-K. Jee [24]. Various steps are followed in this technique, first step is to find the middle coordinates of both the eyes and then the face region 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 size as faces are of different sizes and from these face regions, eye regions are extracted. Hamming separation technique is then used to differentiate about the consecutively extricated pictures. Hamming separation is described by the sum of pixels that have different values. If the hamming distance crosses the threshold value, the input is considered as live. The experimental result has demonstrated that mean hamming distance of a genuine and fraud face is 30 and 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[16]. The authors have first located the mouth region and then extracted OFL. SVM classifier is used and 60 videos are recorded for testing purpose. Feature vectors are drawn out from the mouth area and are fed to SVM classifier. The accuracy achieved in this work is of 73 percent.

DOI: 10.37200/IJPR/V24I8/PR280259
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

Optical Flow based approach:

This methodology is used by Bao et al [25], kollreider et al [17] the creators have grouped a phony face picture with a live face based on the optical flow. This optical flow is a compilation of four movements moving, rotating, translation and swing. The creators have led the investigation 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 irregular directions whereas that of a 2D surface are in uniform directions based on these the liveness of a person can be distinguished. But This strategy will come up short if illumination of a picture changes every now and again and this technique won't neutralize 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 fundamental thought which this strategy follows is that the areas which are nearer to the face produces unexpected movement in comparison to the locales that are far away thus nose will make a different movement in comparison to ears while a 2D picture will consistently make a steady movement for all the districts. Thus, with the knowledge of the movement speed and the positions of face parts liveness data can be easily predicted. For this author have used main Gabor filters for detecting edges and optical flow pattern matching. This system was tested against the database which contained hundred recordings of head rotations. The proposed framework has the error rate of 0.75%.

Component Dependent Descriptor based approach:

This technique is is utilized by Jianwei yang [26]. The means followed by creator for identifying liveness are at first the face is split into six different parts which incorporates left eye territory, right eye territory, nose area, mouth area and facial region. The authors have analysed that micro textures are significant for liveness detection. Capturing a face by camera and capturing a printed photograph by camera creates totally different outcomes depending on micro textures this is mainly because of vary 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 methodology is SVM. The provided algorithm is experimented and tested on CASIA, Print-Attack and NUAA database.

Binary classification-based analysis:

This methodology is utilized by Tan et al [5], Peixoto et al [27]. The creators have expressed that the live face and a picture are not the same as one another in two different 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 mix with the noise, illumination makes the genuine face and a photograph 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 disfigured and has lower picture quality contrasted compared with live face and in this way, it fails in having high frequency details. The authors have defined this issue as a binary classification issue and sparse logistic regression is

DOI: 10.37200/IJPR/V24I8/PR280259
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

used as a classifier for grouping the information. To test this model creators have utilized a database with fifty thousand of pictures and they have likewise tried the model against

NUAA database. But in this model Authors have have neglected to manage the pictures having awful brightening environmental factors on account of which there was issue in deciding the borders of a picture when anticipated from a LCD screen as high recurrence territories were getting obscured because of reflection. To tackle this issue Peixoto et al has proposed to prefilter the picture to standardize the picture.

Context based analysis:

This strategy is utilized by Komulainen et al [28]. This is the one of the first method which attempts to recognize a satirizing gadget before the camera, basically it works on framework in which background information can be changed. It checks whether an individual is holding an image or advanced gadget to parody the framework by remaining before the camera. The idea that this method follows is that as humans rely on the background and scenery information to detect if someone is trying to spoof the system or not similarly their system tries to detect the face and the upper body and background information to check the spoofing attempt. Their mechanism extract information of spoofing medium detector and upper body which is based on HOG descriptor. This data is then gone through SVM classifier to group the given information. The proposed strategy works smoothly on single video frame. The alignment of the lower body, upper body and face is detected using a detector that is tested and trained on real photo spoofing scenarios examples, it checks whether a display device or medium is present or not. Along these lines, first the framework distinguishes face and chest area independently and afterward checks on the off chance that there is any gadget or medium present or not, at that point it at last checks the arrangement and give the outcome. They have tried their framework against CASIA Face Anti-parody database which comprises of thousands of phony pictures and recordings of different characteristics, measures and having diverse illumination conditions. This strategy was tried on CASIA Face Anti-Spoofing database and it gave an error rate of 3.3% - 6.8%.

III. CONCLUSION

Face recognition frameworks give a sheltered and secure strategy for validation and distinguishing proof;however these frameworks can likewise be tricked. This examination gives an outline of different techniques for face liveness recognition. It categorized liveness detection based on various approaches like feature level approach, optical level approach, categorization based on illumination technique etc. The most frequently faced issues that decreases the precision of the system are the effect of variation in illumination characteristics and negative effect of amplified noise which lessens the nature of surface data. Liveness detection techniques should also note the alertness of the user that is it should check whether the user is attentive or not so that an intruder cannot get access of the system if the user is sleeping. Reflection because of Eye scenes ought to be considered in succeeding advancement of face liveness detection. Datasets on which these studies are tested should contain more intelligent recordings where the user performs certain tasks should be included in non-interactive video sequences. Datasets for future assaults must take into thought of assaults from high quality texture videos and 3D silicon masks.

DOI: 10.37200/IJPR/V24I8/PR280259
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

The primary point of this examination is to give a reference to simple, stable and secure development of face liveness detection in near future.

REFRENCES

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 MicroTexture Analysis, Proc. International Joint Conference on Biometrics (UCB 2011), Washington, D.C.,USA
3. 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.
4. S. Chakrabroty, D. Das. "An Overview of Face liveness Detection,"International Journal on Information Theory, 2014, 3(2):11-25.
5. 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.
6. G. Pan, L. Sun, Z. Wu, and S. Lao, ‘‘Eyeblink-based anti-spoofing in face recognition from a generic webcamera,’’ in Proc. IEEE 11th Int. Conf.Comput. Vis. (ICCV), Oct. 2007, pp. 1–8.
7. M. de Marsico, M. Nappi, D. Riccio, and J. Dugelay, Moving facespoofing detection via 3D projective invariants,’’ in Proc. IEEE Int. Conf Biometrics (ICB), Mar./Apr. 2012, pp. 73–78
8. 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
9. T. de Freitas Pereira, A. Anjos, J. M. de Martino, and S. Marcel, ‘‘LBP-TOP based countermeasure against face spoofing attacks,’’ in Proc. Int. Workshop Comput. Vis. Local Binary Pattern Variants (ACCV), Nov. 2012, pp. 1– 12.
10. S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, Computationally efficient face spoofing detection with motion magnification,’’ in Proc. IEEE Int. Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), Jun. 2013, pp. 105–110.
11. I. Chingovska, A. Anjos, and S. Marcel, ‘‘On the effectiveness of local binary patterns in face antispoofing,’’ in Proc. IEEE Int. Conf. Biometrics Special Interest Group (BIOSIG), Sep. 2012, pp. 1–7.
12. 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.
13. 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
14. D. Wen, H. Han, and A. K. Jain, “Face spoof detection with image distortion analysis,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 4, pp. 746–761, Apr. 2015.
15. A. Anjos and S. Marcel, ‘‘Counter-measures to photo attacks in facerecognition: A public database and a baseline,’’ in Proc. IEEE Int. Joint Conf. Biometrics (IJCB), Oct. 2011, pp. 1–7
16. 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.
17. 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.
18. 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
19. N. Erdogmus, S. Marcel, "Spoofing face recognition with 3D masks", IEEE Trans. Inf. Forensics Security, vol. 9, no. 7, pp. 1084-1097, Jul. 2014.
20. 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.
21. 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
22. 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.

DOI: 10.37200/IJPR/V24I8/PR280259
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

23. 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.
24. 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
25. 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.
26. 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
27. B. Peixoto, C. Michelassi and A. Rocha, Face liveness detection under bad illumination conditions, In ICIP, pages 3557-3560, 2011.
28. Jukka Komulainen, Abdenour Hadid, Matti Pietikainen, Context based Face Anti-Spoofing, Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on Pages: 1-8, 2013

DOI: 10.37200/IJPR/V24I8/PR280259
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020