Journal of Computer Science

Original Research Paper

Liveness Detection from Real user, Printed Pictures and Pictures on Mobile Devices from Low Resolution Webcam

[1]Hajer Mohamed H Ben Amer, [1]Dr. Leelavathi Rajamanickam and [2]Dr. Anas A. Abboud

[1]Information Technology, SEGi University, Kota Damansara, Malaysia
[2]Malaysia Social Research Study, Kuala Lumpur, Malaysia

Article history
Received: 20-04-2017
Revised: 06-07-2017
Accepted: 19-09-2017

Corresponding Author:
Dr. Anas A. Abboud
Malaysia Social Research Study, Kuala Lumpur, Malaysia
Email: anasalabousy@gmail.com

Abstract: Biometrics data have emerged as one of the most widely used technologies for validation of identity in various sectors. Nevertheless, spoof biometric data are used by attackers to get access to their targets. Hence, a number of approaches have been initiated to detect these spoofed biometric data. As such, this article proposed a complete methodology for liveness detection using low camera resolution, primarily because vast studies do rely on image quality, eyelid motion and facial expression to investigate spoof images. Nevertheless, spoof attacks cannot be diagnosed from low quality images or recorded video on mobile devices. Therefore, this paper initiates a cutting-edge technique to identify spoof attack from printed pictures, as well as videos recorded on mobile devices and built-in low resolution webcam. Moreover, by detecting the movements at the eye region and weighing these movements from a number of opted frames from recorded video, the standard deviation of these weighted movements were determined and finally, the results of these standard deviation values were compared with the priory estimated threshold values retrieved from this study. Furthermore, due to the nature of the data employed in this study, the researchers generated some data for real users by using low resolution building webcam device by recording the face images of the users on mobile device. With that, 100 various videos were used to predict the threshold value for liveness detection. As a result, this method had been successful in analysing user liveness with an accuracy of 97.6%. On top of that, further experiment is required to look into this method with bigger data set.

Keywords: Liveness Detection, Pupil Dynamics, Spoof Attack, Presentation Attack Detection, Biometrics

Introduction

The system of biometric authentication can be defined as a computer vision-based system that employsthe human body, for instance, Face, Fingerprint, Iris, DNA, Voice and/or behavioural characteristics like passwords, signatures, etc., in order to determine a particular personality to activate the authentication based on the results of the diagnosing process (Rute and Louro, 2014). Besides, past these recent years, with the technology advancement, digital biological data have emerged as a common application in various fields for assurance of critical security, for example, border control and airports banking processes. Furthermore, several other applications are associated to forensic, employee and/or student attendance, as well as internet user authentication. Therefore, the application of biometric data has become part and parcel of our lives. However, these biometric systems are exposed to various attacks that use fake biometrics information.

In fact, a good biometric system manages accurate and effective authentication access. The working diagram of a general biometric system is illustrated in Fig. 1.

Hence, as one of the many techniques of the biometric system, face recognition has been in use for almost half a century (Parmar and Mehta, 2013) with vast applications linked to authentication and personality identification (Sharma and Kaur, 2016). Nevertheless, the main challenge for face authentication and identification system is the use of false facial image, which is also known as ‘spoofing attack’, through the application of digital images like mobile images or printed pictures (Galbally *et al*., 2014).

Science Publications

© 2017 Hajer Mohamed H Ben Amer, Leelavathi Rajamanickam and Dr. Anas A. Abboud. This open access article is distributed under a Creative Commons Attribution (CC-BY) 3.0 license.

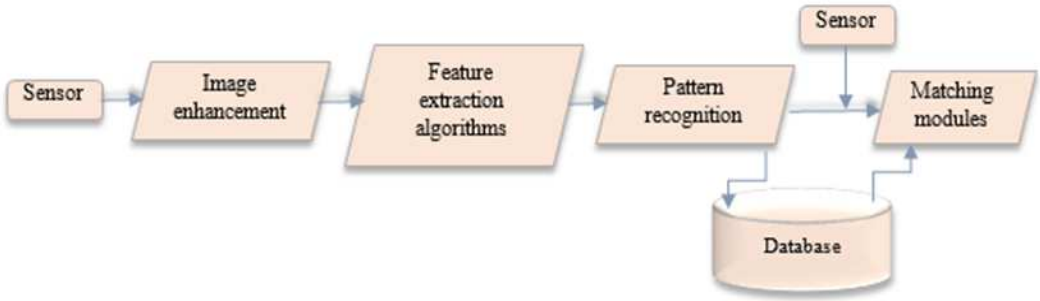

Fig. 1. Diagram flow of the overall processing in a biometric system

Hence, for this purpose alone, numerous algorithms have been developed to detect spoof attack. These algorithms are classified as listed in the following:

Image quality-based method by Shende *et al*., (2014), Shende and Sarode (2016), as well as Chingovska (2015), who claimed that the image quality of a spoof image differs from the original due to the effect of reflection. With that, Wen *et al*. (2015) employed the feature vector of Image Distortion to extract specular reflection, blurriness, chromatic moment and colour diversity. After that, the findings were compared with user image stored in the database to identify user image and lastly, the aspect of liveness was examined by tracking the eye lid motion to detect spoof images. In fact, this method is normally used for previously registered users.

Texture-based algorithms; in which this method assumes that the real user image possesses unique texture properties, in comparison to printed images or images captured on mobile screen. With that, Maatta *et al*. (2012) adopted the Local Binary Patterns (LBP) to extract micro texture, which was employed to enhance image histogram, for usage in the learning algorithm for detection of user liveness. Even though this particular method offered accurate results, it failed with low texture information (Garud and Agrawal, 2016).

Motion-based method; several research studies have employed the optical flow technique to track eyelid motion (Drutarovsky and Fogelton, 2014). In addition, other approaches employ the variance of intensity between the sequenced frames based on threshold to detect blinking (Divjak and Bischof, 2009). In fact, eyelid tracking uses facial landmark (Perception and Technical, 2016). Nevertheless, the drawbacks of these approaches are that they can be strongly affected by the face position captured by camera, image resolution and blinking rate. For example, the blinking tracking approach assumes the blinking rate of the human is approximately 15 to 30 times/min, in which the duration between every two-blink is around 2 to 3 sec with a blink time at almost 205 milliseconds. Therefore, a standard camera can easily capture a face video with more than 15 frames per second, with the interval between the frames not exceeding 70 milliseconds. Next, the camera can capture two or more frames when a face looks into the camera (Garud and Agrawal, 2016). This method, nonetheless, demands the tracking of eyelid position among all frames to identify the closed eyelid status (blinking), thus seeking intensive computation process. Additionally, Polatsek (2015) asserted that computer users tend to reduce their blinking rate in front of a monitor primarily because the tear is inadequately applied on the cornea of the eyes. In turn, this might cause frailer diagnoses for user liveness. Furthermore, some implementations embed additional techniques, for example, passwords and facial expirations, to ensure uncompromised security (Patel *et al*., 2016).

Problem Statement

Spoof attack is a major glitch in the biometric system practices. Therefore, endless techniques have been developed to investigate the aspect of user liveness from face image, through the use of image quality- and texture-based techniques, along with biometric-acquiring equipment, by incorporating motion tracking approaches to track eye blinking or even adding farther access information, for instance, password, to distinguish the real user image from one that is false. Unfortunately, these methods can be computationally time-consuming and costly due to the use of additional sensors, thus requiring storage capability or otherwise, the quality of the image could be, eventually, strongly affected (Garud and Agrawal, 2016). Besides, the literature posits that the available iris-based liveness detection methods rely on pupil dynamics through its interaction with lighting (Czajka, 2015). On the other hand, other approaches (Galbally *et al*., 2012) include the diagnoses of real users using iris images based on image quality; with the assumption that spoof images (printed or on screen) have lower resolution quality.

With that, this article proposes a fast spoof attack detection technique, especially to detect user liveness image from both printed images and recorded user video from low resolution webcam. Moreover, in order to extract the boundary of features in the region of interest (the eyes region) from a number of sequenced frames, a

simple mathematical-based method had been applied to identify spoof images. In fact, a plus point of this method is that it offers accurate results with varied image quality (independent on image quality), thus successful in identifying a spoof user from recorded video. On top of that, the proposed method assumes that the real computer user moved his/her iris randomly to read the content displayed by the monitor and/or to follow the mouse pointer (Rodden and Fu, 2006). Other than that, it has been assumed that the iris movement is quicker than the blinking of the eye (Czajka, 2015), which demands a motion tracking algorithm with a minimum number of frames.

Methodology

The main objective of this study is to detect spoof face image from low resolution webcam images. Eye blinking is indeed a commonly used approach to identify user liveness. Although this approach has successfully protected the system from photographs, it has failed with recorded video on mobile or tablet. Moreover, its accuracy is influenced by image resolution. Hence, this study proposes an automatic spoof attack detection of users from low resolution webcam and recorded videos on mobile device. In fact, the first stage refers to data generation, whereby this step generates a dataset of real users from low resolution webcam with varied lighting degrees (high and low) at different environments and backgrounds. Furthermore, a number of fixed images (photographs) had been selected from online free stock photos, in which all images and videos included in this study had a frontal face view with clear eyes, as illustrated in Fig. 2.

Next, the second stage involved a sequence of steps proposed to satisfy accurate detection for spoof user images, as portrayed in Fig. 3.

Therefore, from the depicted problem statement and with consideration of the data characteristics employed, a quantitative-based method had been adopted to detect fake users, whereby the accuracy of the results had been tested empirically.

Besides, this study is part of a master's degree research work that is projected to develop a family protection system exclusively for internet users on personal computer with low resolution webcam, by activating the authentication of internet access based on estimation of users' age.

These images were acquired by using an ASUS built-in camera (UVC WebCam). In addition, a set of real time videos with 100 frames had been recorded to select 10 frames as input for the proposed method using the loop counter approach, which is increased by ten to reduce computation time. Next, the viola-Jones approach was employed for facial feature detection, in which an algorithm was applied to detect the face region by selecting the nearest face to the camera (Viola and Jones, 2004; Gupta and Tiwari, 2015). Later, the face area was segmented in each frame to be keyed into the viola-Jones algorithm, especially to detect the eye region. In precise, this process had successfully diagnosed the eye region accurately as in Fig. 4 (b). In addition, the results of this process were tested experimentally in all frames for all iterations in this study. In fact, the primary purpose of segmenting the eye region had been to reduce the processing time in order to resemble the real time liveness detection as shown in Fig. 4.

The data employed were comprised of video data type for real users, as well as falsely printed pictures or recorded videos on mobile devices, with the following consideration: (i) the real user movement is caused by natural human movement of head and facial features, while (ii) the movement generated by spoof images caused by hand movement of the person who holds the fake pictures.

Additionally, background subtraction is a general technique that is used to determine a foreground object in movement derived from sequence frames from video taken by a fixed camera (Singla, 2014; Philip, 2013), which demands predetermined foreground and background objects, as well as several other various approaches to identify both the foreground and the background objects in the images.

In this study, although the data had been acquired by using a built-in webcam in laptop, the object under investigation was moved and the motion of a particular part from the moving object had been identified. Moreover, as the available techniques for background subtraction have failed in providing accurate results for this case, the ROI was segmented in arrays with varied dimensions in each frame, as given in Table 1. Hence, the images of the arrays had been resized based on the biggest array, as displayed in the pseudo code presented in Fig. 5.

Other than that, the Contrast-Limited Adaptive Histogram Equalization (CLAHE) and the (4×4) Gaussian filter had been applied to improve the gray scale aspect of the images (Zuiderveld, 1994). Later, canny filter boundary detection was performed to extract all the features embedded in the ROI, as illustrated in Fig. 6.

After that, image subtraction was performed, whereby pixel-to-pixel comparison was made for the boundary features in ROI for each two sequenced frames, which resulted in 0, 1 and -1. In this case, zero represents nil change in feature (no movement), while 1 and -1 refer to particular movements in features, as shown in Fig. 7.

Fig. 2. Sample of dataset used in this study

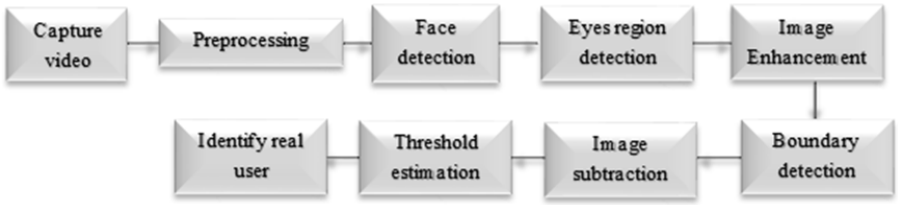

Fig. 3. Flow diagram of research work

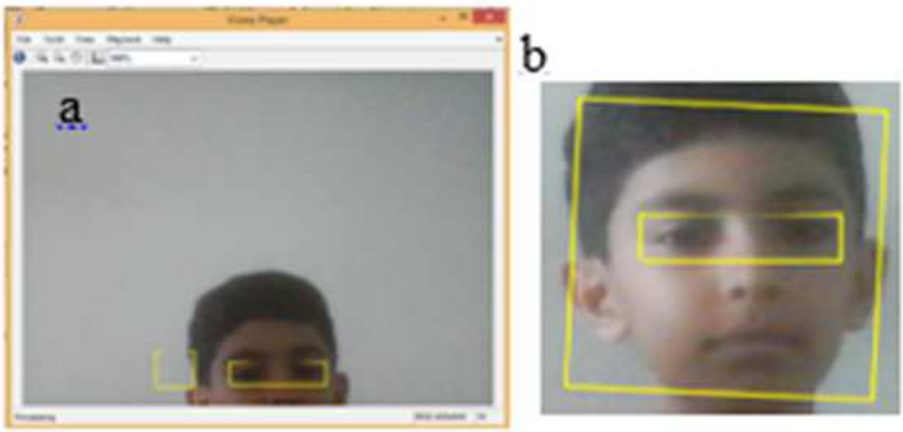

Fig. 4. (a) Inaccurate diagnosis for facial region (b) Accurate detection

```
// find the size of for all segmented regions
for i=1 to last frames
    X_dimension(i)=size(segmented eyes region {1,i},1)
    Y_dimension(i) =size(segmented eye region {1,i},2)
End

// resize all arrays based on the biggest
for i=1to last frame
        Z1{i} = resizem(Eyes_Array{i},[max(X),max(Y)]))
end
```

Fig. 5. Pseudo code of resizing ROI

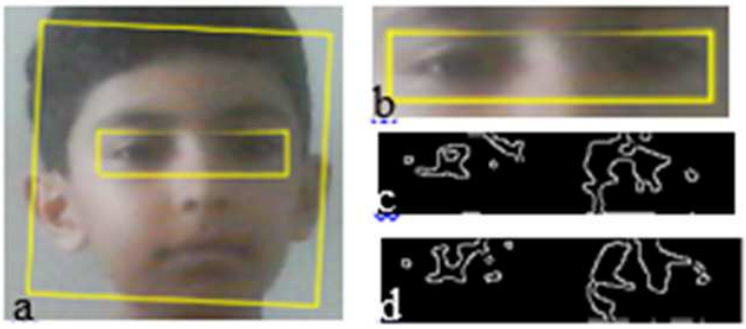

Fig. 6. (a) Real (life) image; (b) Segmented ROI; (c) Boundary in ROI for the first frame; (d) Boundary in ROI for the second frame

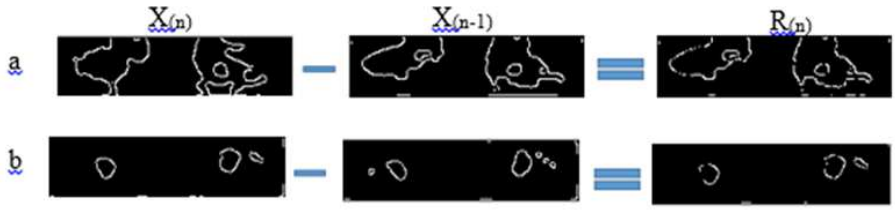

Fig. 7. The results of image subtraction for real user (a) and spoof image (b)

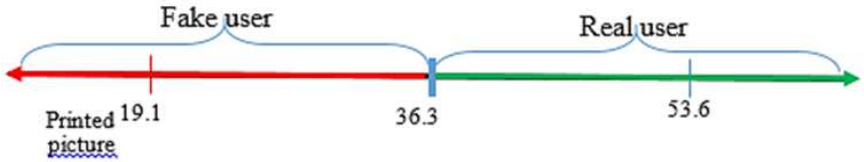

Fig. 8. Threshold estimation

In addition, in order to estimate the threshold values by distinguishing the movements between real and fake user, 100 iterations were performed for two types of datasets, 50 videos of real (living) users and 50 videos for spoof users (printed picture). Next, the weight of the movement (or change) for each array had been calculated, while the subtraction process was performed with Equation 1. Where; f is the number of frames taken from the webcam video; $R_{i,j}$ represents values 0, 1, or -1; and W_f is a vector array of the ROI weight for each frame. After that, the standard deviation for the movement weighed in each video had been calculated (*stdv*) from Equation 2. Where; w_k is the movement weight for frame k ($\forall$ k =1,2,3… n-1) and $\bar{w}$ is the average of the values in vector W:

$$W_f = \sum_{i=1}^{n}\sum_{j=1}^{m} R_{i,j} \quad (1)$$

$$stdv = \sqrt{\frac{\sum_{k=1}^{n-1}\left(w_k - \bar{w}\right)^2}{\left((n-1)-1\right)}} \quad (2)$$

Table 1. Dimensions of the detected ROI and the resizing based on min x axis and max y axis

Frames	Video1	Video2	Video3	Video4	Video5
F_1	36x145	52x210	41x164	41x163	39x156
F_2	34x137	52x207	41x163	41x164	41x164
F_3	34x136	51x205	40x161	41x163	40x162
F_4	36x145	51x205	41x164	40x161	42x167
F_5	37x147	51x205	41x165	41x164	42x169
F_6	37x147	52x207	40x161	41x165	41x165
F_7	37x147	51x204	40x159	40x161	40x159
F_8	37x148	51x203	39x154	40x159	42x167
F_9	38x152	51x204	40x161	39x154	41x162
F_{10}	37x148	51x205	41x163	40x161	42x168
Win.dim	34 x148	51 x210	39x165	39 x165	39 x165

As a result, the average of the calculated standard deviation for the real user videos is ($STDV_{real}$ =53.6), whereas the spoof videos is ($STDV_{fake}$ =16.8) and the average of the interval between the real and the fake ones is (Av =16.9) based on Equation 3. Therefore, the threshold value is (33.7), as estimated from the average of the interval between the (rmse =17.2) values retrieved from real and fake users based on formula (4) depicted in Fig. 8:

Table 2. The calculated differences among each sequenced frame for the boundary features in the segmented ROI for real user images and the standard deviation of the differences in each video

Iterations	I_1	I_2	I_3	I_4	I_5	I_6	I_7	I_8	I_9	I_{10}	I_{12}	I_{13}	I_{14}
Diff. (1&2)	-40	69	71	57	13	-60	-85	58	-52	22	-18	6	9
Diff. (2&3)	61	31	-172	-83	62	18	70	-23	27	0	31	39	-71
Diff. (3&4)	-67	-34	32	-65	-66	-35	6	-14	-26	-14	25	-54	49
Diff. (4&5)	23	-7	40	46	-31	0	-1	5	27	15	-22	23	-43
Diff. (5&6)	-10	-26	-67	92	43	-4	-3	9	-41	90	23	26	9
Diff. (6&7)	-45	31	101	22	-39	54	-18	-37	64	-14	48	-42	40
Diff. (7&8)	14	-54	-50	-107	26	-5	-30	24	-15	40	-94	28	-2
Diff. (8&9)	23	78	63	91	-39	-89	53	76	16	11	30	-20	1
Diff. (9&10)	-38	-40	19	-134	51	4	-46	-131	-3	80	-10	-5	-32
STDV	**41.7**	**48.6**	**85.6**	**88.2**	**46.7**	**42.6**	**47.4**	**68.7**	**37.3**	**37.8**	**43.4**	**32.9**	**36.4**

Table 3. The calculated differences among each sequenced frame for the boundary features in the segmented ROI for printed images (fake user), as well as the standard deviation of the differences in each video

Iterations	I_1	I_2	I_3	I_4	I_5	I_6	I_7	I_8	I_9	I_{10}	I_{11}	I_{12}	I_{13}	I_{14}
Diff. (1&2)	8	12	6	11	-13	10	-13	12	-13	18	6	-27	18	18
Diff. (2&3)	-6	11	37	2	0	-15	2	10	2	-14	37	-5	-24	-14
Diff. (3&4)	11	13	-44	3	-2	-28	3	13	3	10	-44	-8	39	10
Diff. (4&5)	4	-52	42	-5	3	1	-5	-11	-5	4	42	-57	-4	4
Diff. (5&6)	-6	43	-8	-11	0	14	14	4	14	6	-8	22	21	6
Diff. (6&7)	-2	-35	0	6	12	-7	6	-3	6	8	0	21	8	8
Diff. (7&8)	-8	26	14	1	-14	2	-13	-16	-13	-7	14	-23	-8	-7
Diff. (8&9)	12	7	-34	-1	2	-30	-1	-10	-1	14	-34	0	-40	14
Diff. (9&10)	3	-5	-6	6	-2	13	7	15	7	7	-6	-34	38	7
STDV	***7.6***	***29.4***	***28.6***	***6.5***	***8***	***16.8***	***9.1***	***11.8***	***9.1***	***10***	***28.6***	***25.8***	***26.9***	***10***

Table 4. The calculated differences among each sequenced frame for the boundary features in the segmented ROI for video of user face on mobile device, as well as the standard deviation of the differences in each video

ITERATIONS	I_1	I_2	I_3	I_4	I_5	I_6	I_7	I_8	I_9	I_{10}	I_{11}	I_{12}	I_{13}	I_{14}
DIFF. (1&2)	-30	-12	-4	5	-1	9	34	-46	-34	13	-20	-15	-10	**-29**
DIFF. (2&3)	-12	29	-7	-17	-10	-41	-23	7	19	19	19	30	9	**2**
DIFF. (3&4)	30	-27	10	1	14	49	40	11	-11	27	33	-11	-49	**-19**
DIFF. (4&5)	-1	-5	-24	19	1	-23	9	24	14	9	13	24	-11	**-41**
DIFF. (5&6)	4	-4	39	-41	-22	9	-18	24	-15	-16	19	-15	-25	**39**
DIFF. (6&7)	-28	2	-23	14	5	20	0	24	-24	-15	-14	-4	-30	**27**
DIFF. (7&8)	17	7	-1	14	2	-2	-6	24	16	15	-36	16	34	**-1**
DIFF. (8&9)	-7	4	7	-6	-32	1	-13	24	26	-13	-12	12	8	**18**
DIFF. (9&10)	37	-3	-5	2	9	-32	50	24	-83	-10	-29	-43	-8	**-35**
STDV	**23.6**	**15.1**	**18.9**	**18.6**	**14.9**	**27.8**	**26.9**	**23**	**34.5**	**16.7**	**24.4**	**23.2**	**24.4**	**28.5**

$$AV = \frac{STDV_{real} - STDV_{fake}}{2} \quad (3)$$

where, m is the total number of iterations (m = 50 iterations), x is the standard deviation value of each video (i) and i = 1 to m.

Moving on, in order to validate the proposed method, three types of video images had been used; real user (life), printed photograph and video on mobile device. The results of calculation for each iteration are tabulated in Table 2-4 for each data type, respectively.

Results and Discussion

The total number of iterations performed for validation had been 42 iterations with 14 iterations for each data type. The preliminary results indicated 97.6% of accuracy among all data types, with only one failure in diagnosing, as highlighted in Table 1.

The findings demonstrate that the threshold had successfully distinguished between the real user and the printed pictures (spoof data). As such, one can concluded that the proposed method had been successful in diagnosing user liveness especially that derived from video on device such as Laptop copmuter.

Conclusion

Biometrics data have emerged as one of the most widely used technologies for validation of identity in various sectors. In this paper,a complete methodology for liveness detection using low camera resolution was proposed. The results show that the proposed method successfully analyze user liveness with an accuracy of 97.6%. In a future, we aim to experiment the proposed method on very big data sets.

Acknowledgment

The authors would like to express greatest appreciation to SEGI, University for financial support. Furthermore, Full thanks to support by Ministry of Education, Libya under the MSc. Scholarship programs.

Author's Contributions

Hajer Mohamed H Ben Amer: Designed the research plan and organized the study.

Dr. Leelavathi Rajamanickam: Coordingated the mouse work.

Dr. Anas A. Abboud: Participated in experiments, coordinated the data-analysis and contributed to the writing of the manuscript.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and there are no ethical issues involved.

References

Chingovska, I., 2015. Trustworthy biometric verification under spoofing attacks: Application to the face mode.

Czajka, A., 2015. Pupil dynamics for iris liveness detection. IEEE Trans. Inform. Forens. Security, 10: 726-735. DOI: 10.1109/TIFS.2015.2398815

Divjak, M. and H. Bischof, 2009. Eye blink based fatigue detection for prevention of computer vision syndrome. Conference on Machine Vision Applications, May 20-22, Yokohama, Japan, pp: 350-353.

Drutarovsky, T. and A. Fogelton, 2014. Eye blink detection using variance of motion vectors. Proceedings of the European Conference on Computer Vision, Springer, pp: 436-448. DOI: 10.1007/978-3-319-16199-0_31

Galbally, J., S. Marcel and J. Fierrez, 2014. Image quality assessment for fake biometric detection: Application to iris, fingerprint and face recognition. IEEE Trans. Image Process., 23: 710-724. DOI: 10.1109/TIP.2013.2292332

Galbally, J., J. Ortiz-Lopez, J. Fierrez and J. Ortega-Garcia, 2012. Iris liveness detection based on quality related features. Proceedings of the 5th IAPR International Conference on Biometrics, Mar. 29-Apr. 1, IEEE Xplore Press, New Delhi, India, pp: 271-276. DOI: 10.1109/ICB.2012.6199819

Garud, D. and S.S. Agrawal, 2016. A review : Face liveness detection. Int. J. Adv. Res. Comput. Commun. Eng., 5: 336-339. DOI: 10.17148/IJARCCE.2016.518 3

Gupta, A. and R. Tiwari, 2015. Face detection using modified viola Jones algorithm. Int. J. Recent Res. Math. Comput. Sci. Inform. Technol., 1: 59-66.

Maatta, J., A. Hadid and M. Pietikainen, 2012. Face spoofing detection from single images using texture and local shape analysis. IET Biometr., 1: 3-10. DOI: 10.1049/iet-bmt.2011.0009

Parmar, D.N. and B.B. Mehta, 2013. Face recognition methods and applications. Int. J. Comput. Technol. Applic., 4: 84-86.

Patel, K., H. Han and A.K. Jain, 2016. Secure face unlock: Spoof detection on smartphones. IEEE Trans. Inform. Forens. Security, 11: 2268-2283. DOI: 10.1109/TIFS.2016.2578288

Perception, M. and C. Technical, 2016. Eye blink detection using facial landmarks. Proceedings of the 21th Computer Vision Winter Workshop, Feb. 3-5, Slovenia.

Philip, A.S., 2013. Background subtraction algorithm for moving object detection using denoising architecture in FPGA. Int. J. Sci. Res., 2: 151-157.

Polatsek, P., 2015. Blink rate tracking of computer user. Bachelor Thesis, Slovak University of Technology in Bratislava.

Rodden, K. and X. Fu, 2006. Exploring how mouse movements relate to eye movements on web search results pages. Proceedings of ACM SIGIR Workshop on Web Information Seeking and Interaction, (ISI' 06), pp: 29-32.

Rute, A. and C. Louro, 2014. Liveness detection in biometrics. Proceedings of the International Conference of the Biometrics Special Interest Group, Sept. 9-11, IEEE Xplore Press, Darmstadt, Germany, pp: 1-14. DOI: 10.1109/BIOSIG.2015.7314611

Sharma, N. and R. Kaur, 2016. Review of face recognition techniques. Int. J. Adv. Res. Comput. Sci. Software Eng., 6: 29-37.

Shende, P.M. and M.V. Sarode, 2016. Multiple biometric system application: Iris and fingerprint recognition system. Int. J. Applic. Innovat. Eng. Manage., 5: 34-38.

Shende, P.M., M.V. Sarode and M.M. Ghonge, 2014. A survey based on fingerprint, face and iris biometric recognition system, image quality assessment and fake biometric. Int. J. Comput. Sci. Eng. Technol., 4: 129-132.

Singla, N., 2014. Motion detection based on frame difference method. Int. J. Inform. Comput. Technol., 4: 1559-1565.

Viola, P. and M.J. Jones, 2004. Robust real-time face detection. Int. J. Comput. Vis., 57: 137-154. DOI: 10.1023/B:VISI.0000013087.49260.fb

Wen, D., H. Han and A.K. Jain, 2015. Face spoof detection with image distortion analysis. IEEE Trans. Inform. Forens. Security, 10: 746-761. DOI: 10.1109/TIFS.2015.2400395

Zuiderveld, K., 1994. Contrast Limited Adaptive Histogram Equalization. In: Graphics Gems IV, Academic Press Professional, Inc., pp: 474-485.