THINK INDIA JOURNAL

ISSN:0971-1260

Vol-22-Issue-41-December-2019

Study on Secure Face Spoofing Detection on Android Device

Ch Laxmi Shalini[1], Hemlata Dalmia[2] and A. Swathi[3]

[1,2]Department of ECE Sreyas Institute of Engineering & Technology Hyderabad

[3]Department of CSE, Sreyas Institute of Engineering & Technology, Hyderabad

ABSTRACT

Face is the commonly used for the biometric device application in software and commercial use due to its unique identification. Face spoofing is the high range attack in government sectors and commercial sectors. Android device can be much convenient to detect and secure face spoofing detection. From last few years it was having more success with the spoofing attack. The spoofing attack can be done in many types like video attack, printed photo, 3D mask and facial attack. Researchers used many types of database are used like CASIA, MSU and Replay attack. Researchers have proposed different types of logarithms for genuine face and fake face based on real time applications.

Keywords: Face Spoofing, Face Unlock, Spoof Detection On Android Device, Biometrics.

I. INTRODUCTION

Now a day's face spoofing is the more vulnerable. For the spoofing attack many biometric techniques are used like fingerprint, face, iris etc.[26] .The cheapest and easiest way of spoofing attack is taking images from social networks and captured from the camera [1]. The different types of face spoofing i.e. printed photograph, a video, a mask etc; attacker can use facial as the other way of spoofing [3]. Compared with other technique, falsifying face biometric data is straight forward no other skills are required for this. In public hiding your face is impossible, thus facial information can be captured even from long distance also [4].The hardware process can also detect the live person when they will be in front of the system which automatically detect the pulse rate in the case of recognisation of finger print[40]. The user should be properly respond to the system or else it shows the replicate in different facial movement [5, 7]. The spoof attack can be done through photographs, videos, mask, and make-up spoofing can be little bit difficult to detect cause of using cosmetics[52]. But it can also be very easy to attack; the other user can also apply wide makeup to spoof[24] . The issues of the face spoofing detection can be solved by analyzing the movement in the face like eye blink and movement of the mouth using ILGS process [8]. In [10] Replay attack is solved by following steps as training, development, and testing. There are many papers published, the training and testing images/videos are already captured [9].

This paper is categorize in different sections. Section I is introduction, section II is Spoofing Attack,section III is about

Literature survey, section IV is Comparison Analysis table, V is conclusion.

II. SPOOFING ATTACK

The information takes more conditions for fake face; the photo or video can be taken without his/her permission to unlock the Android device. This process can be done directly or indirectly from social networks. The types of fake faces are photos; Mask, Replay attack and make up are followed.

ISSN:0971-1260

Vol-22-Issue-41-December-2019

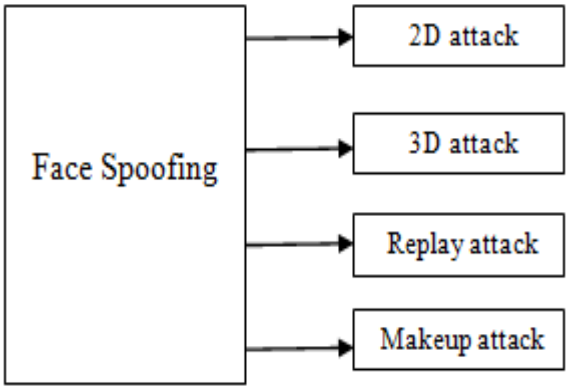

Fig. 1. Attacks in face spoofing

A. 2D ATTACK (PHOTO)

To accesses the biometric modality systems like tablet, laptops and phones the attacker use photograph of 2-D spoof system as shown in fig.2. To capture the face attacker use camera to take photo or can be taken from the social networks [11]. Displaying printed photos on the smart phones, can easy to unlock the device [12].

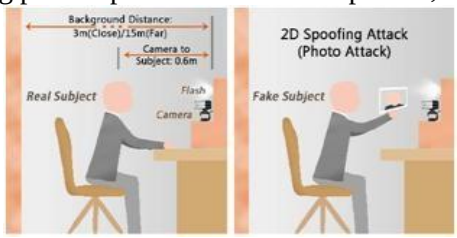

Fig. 2. Example of a 2D Attack [23]

B. 3D ATTACK (MASK):

The photo and printing technologies is more advance in 3D mask attack [21]. The complete 3D image of the face is emulate, the use of cues that can be solution to prevent from the previous attack [6]. The 3D mask is prevented with different kind of materials. The 3D mask attacker can prepare an original face structure with different materials like silicon, papers etc.[17] wearing 3D facial mask, displaying printed photo, are the kind of face spoof attack [21].

Fig. 3. Example of a 3D Attack [21]

C. REPLAY-ATTACK (VIDEO):

In this the attacker takes the video of the unknown person from digital camera or phones or tablets after capturing the attacker play that video and unlock the devices[14],[60]. These types of attack is difficult to recognize while detect.

Fig. 4. Example of a Replay- Attack [22]

ISSN:0971-1260

Vol-22-Issue-41-December-2019

D. MAKE UP ATTACK:

The spoof attack can be done through photographs, videos, mask, and make-up spoofing can be little bit difficult to detect cause of using cosmetics[15]. But it can also be very easy to attack; the other user can also apply wide makeup to spoof [13].

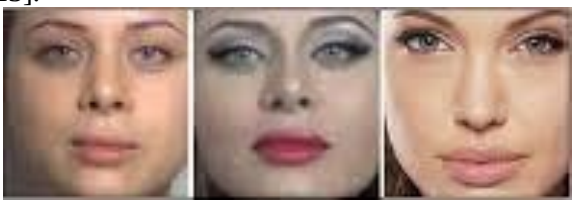

Fig. 5. Example of a make-up attack[11]

III. LITERATURE ANALYSIS

Gang Pan et al. [1] introduced real-time liveness detection algorithm for photo spoofing with less intensity webcam the eye blinking recognition is done with the comparison of cascaded Adaboost and HMM.

Maatta et al. [3] proposed a method that detects based on Micro-Texture Analysis they finalized that using single configuration of LBP Is more efficient among three LBP descriptors of different configuration.

Jukka Komulainen et al. [4],[44] in 2013 introduced Print Attack and Replay Attack spoofing technique identify the genuine and fake pupil with error rate 2%.

Samarth Bharadwaj et al. [5] introduced Motion and texture based techniques were followed and used support vector machine (SVM) and local binary pattern (LBP) to calculate Half Total Error Rate is 7.6%.

Nesli Erdogmus et al. [6] in 2014 3D mask spoofing technique were proposed. This method is based on detection of fake faces, while compared with 3D Detection. It is having Equal Error Rate and more Accuracy than 3D with 7%.

Ivana Chingovska et al. [7] proposed REPLAY- ATTACK used three different types of media attack and two recording. Different types of database were used Public database, CASIA Face database, NUAA photographer.

Housam Khalifa Bashier et al. [8] proposed a method for the problem on textured base analysis also computed a reached description using graphic structures[28],[39]. Through various facial expressions i.e. blinking of the eyes and mouth movements, we can avoid the face spoofing issues using ILGS methodology[62].

Di Wen et al. [9] proposed a method about blurriness of the face, color moments, specular reflection and color diversity specular reflection. In 2008 the author has research on the age identification based on genders[37][45].

Table i. Hter (%) Comparisig of Existing Methodology

Reference	Year	Methodology	Dataset	HTER (%)
Yan Wang et al [6]	2017	CNN	CASIA	10.20
Aziz Alotaibi et al [11]	2016	LBP	Replay-Attack	14.6
Pinto et al.[34]	2015	2D-DFT	Replay-Attack	14.27
UNICAMP [43]	2013	2D-DFT+GLCM	Replay-Attack	15.62
Chingovska et al [7]	2012	LBP	Replay-Attack	15.16
SIANI[35]	2011	Motion	Print-Attack	10.63

ISSN:0971-1260

Vol-22-Issue-41-December-2019

Table II. Accuracy Comparisig Of Existing Methodology

Reference	**year**	**Methodology**	**Dataset**	**ACC (%)**
Tan et al. [32]	2010	Variational Retinex	NUAA Imposter	91.20
Peixoto et al.[33]	2011	DoG	Yale Recaptured	93. 20
Kose and Dugelay [43]	2013	LBP	Kose and Dugelay's	93.5
Kose and Dugelay [56]	2013	Variational Retinex	Kose and Dugelay's	94.47
Arashloo et al. [60]	2015	MLPQ- TOP+MBSIF-TOP	NUAA Imposter	97.70
Manminder Singh[69]		FNR	Print-Attack	98.80

TABLE III. COMPARISON TABLE OF EXISTING METHODOLOGY BASED ON FACE SPOOFING

S.NO	**AUTHOR NAME**	**YEAR**	**METHODOLOGY**	**RESULTS**	**ACCURACY**
1	Gang Pan et al. [1]	2007	web camera	With less intensity webcam the eye blinking recognition is done with the comparison of cascaded Adaboost and HMM.	EER=6.9%
2	Jiamin Bai et al. [2]	2010	Physics-base method	Gradient image was analyzed	EER=6.7%
3	Maatta et al. [3],[49]	2011	Windows XP and Vista laptops	They finalized that using single configuration of LBP Is more efficient than local binary pattern descriptor.	EER=0.5%
4	Jukka Komulainen et al. [4]	2013	Replay Attack spoofing.	Complexities of individual techniques are not depend on	EER=2%
5	Samarth Bharadwaj et al. [5]	2013	Print Attack and Replay Attack spoofing	Motion and texture based techniques were followed.	HTER=7.6%
6	Nesli Erdogmus et al [7]	2014	Spoofing, Mask attack.	In this they record that fake face detected with classifying rate, while compared with 2D Detection. It is having Equal Error Rate and more Accuracy than 2D.	EER=7%
7	Ivana Chingovska et al [8]	2014	Attack, counter-measures.	The disadvantages is biased Behavior of ignoring the spoofing attacks in the threshold	EER=10%

ISSN:0971-1260

Vol-22-Issue-41-December-2019

				decision process.	
8	Housam Khalifa Bashier et al [9]	2014	Texture analysis, pattern recognition.	The issues of spoof detection can be solved by study human face movement changes like eye blink and movement of mouth using ILGS process.	EER=6.8%
9	Di Wen et al [10]	2015	Face recognition, spoof detection, image distortion analysis, ensemble classifier, cross-database, cross-device	Methods use motion or texture based features using IDA with support vector machine classifiers trained for different spoof attacks.	HTER=7.4%
10	Aziz Alotaibi et al [11]	2016	Face liveness detection, replay attack dataset.	Real face has sharp edges especially at lips and nose part. The research has approach the local binary pattern logarithm	HTER=14.6%
EER: Equal Error Rate ; HTER: Half Total Error Rate					

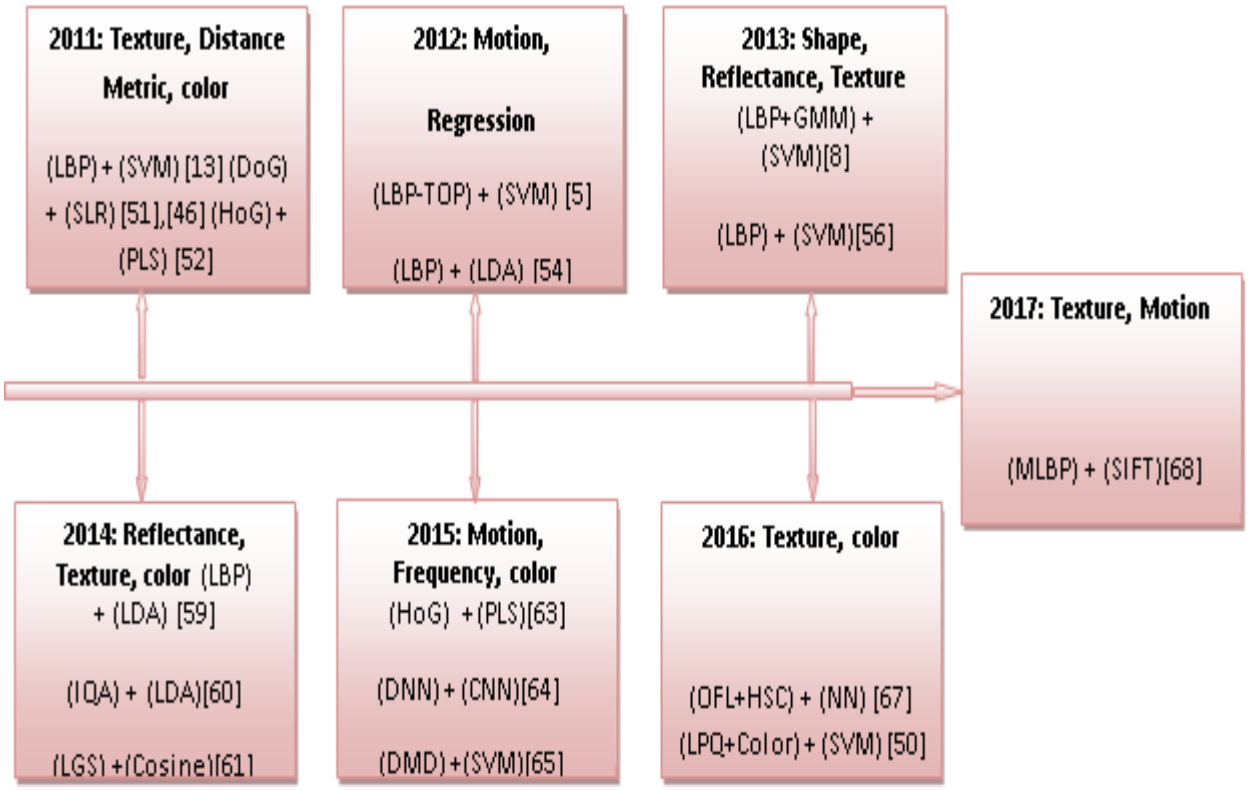

Fig. 6. Timeline of face spoofing detectors in the last decade

ISSN:0971-1260

Vol-22-Issue-41-December-2019

TABLE IV: SUMMARY OF AVAILABLE FACE SPOOFING DATASETS

S.NO	DATA BASE	TYPES OF ATTACK	YEAR	FAKE/REAL
1	NUAA Photograph Imposter	Flat printed photo Warped photo	2010	7506/5015
2	Print-Attack	Flat printed photo	2011	200/200
3	Yale Recaptured	Flat printed photo	2011	1920/640
4	Casia Face Anti Spoofing	Warped photo Eye-cut photo Video playback	2012	450/150
5	Replay- Attack	Flat printed photo Video playback	2012	1000/200
6	3D Mask Attack	Mask	2013	85/170
7	Kose and Dugelay	Mask	2013	198/200
8	MSU-MFSD	Flat printed photo Video playback	2014	210/70
9	UVAD	Video playback	2015	16268/808

Aziz Alotaibi et al [10] proposed a method of real face has sharp edges especially at lips and nose part. The research has approach the local binary pattern logarithm using different information at spread image.

Javier Galbally et al.[18] proposed a method on anti- spoofing techniques, two types of techniques are used hardware based and software based biometric to detect the face. The author used three types of datasets[47][68].

Xiaoyang Tan et al.[22] introduced about the face liveness detection used with single image. In this the result was classified with nonlinear to linear error is 76.7%.

Roberto Tronci et al.[35] proposed a method using SVM classifier the 2-D and 3-D attacks are also used to detect. video analysis are used to detect the motion clues.

Allan da Silva Pinto et al.[50] introduced about the photo based spoofing attack with different technologies based on monitor i.e. LCD,LED based on smart phones devices.

Murali Mohan Chakka et al.[53] proposed a method using different database i.e. CASIA,UNICAMP,etc. for 2d facial spoofing. By using this database the error rate is 10.63% [54],[67].

Samarth Bharadwaj et al.[44] proposed a method on motion and textured based using multiple local binary pattern technologies. using CASIA based dataset the error is14.44%.

In face spoofing different types of dataset are used as shown in Table. IV, NUAA Photograph Imposter, Print- Attack, Yale Recaptured etc. photos from NUAA can be taken from the cheap webcams[30]. The Yale Recaptured collects the images from fifty centimeter distance[20],[36].

IV. **CONCLUSION**

In this paper the face spoofing attack is most commonly done by using printed photos, videos, mask etc, because it is low cost and it can be very easy to unlock the android devices like tablet, laptops, smart phones.

Presently biometric authentications are using various parameters to identify the results i.e. False Acceptance Rate (FAR) and False Rejection Rate (FRR) to measure accuracy, precision of the users input. In this False Acceptance Rate shows that this model is classified a wrong input as belonging to the choose user, while False Rejection Rate records the biometric classifies the users biometric as incorrect. The researchers used two datasets but we scope to use more than two datasets. The ratio of Negative false rejection (NFR) to

ISSN:0971-1260

Vol-22-Issue-41-December-2019

genuine gives FRR. Mathematically these parameters are derived. Many of the researchers are using only two to three parameters, but there is a scope of using all the parameters. In the fig.7 the finally half total error rate reached to 10.2% but we have scope to reduce the error rate. From the previous paper the accuracy rate is up to 98.8% as shown in fig.8.

$$FRR = \frac{NFR}{Genuine} \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

$$FAR = \frac{NFR}{impostor} \quad \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

$$EER = (FAR = FRR) \quad \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

$$HTER = \frac{FAR + FRR}{2} \quad \ldots\ldots\ldots\ldots\ldots\ldots (4)$$

$$ACC = 100 \left\langle \frac{1 - FAR \times impostor + FRR \times genuine}{impostor + genuine} \right\rangle \quad \ldots\ldots\ldots\ldots\ldots\ldots (5)$$

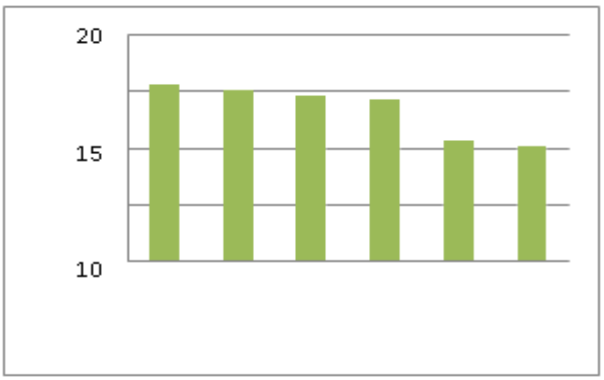

Fig. 7. HTER(%) over the last decate

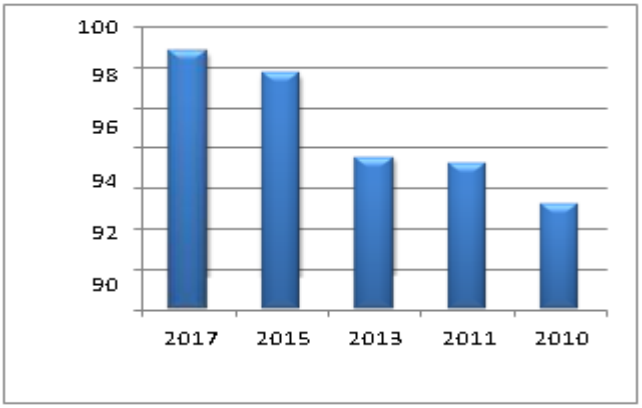

Fig. 8. Accuracy(%) over the last decate REFERENCES

[1] Pan, Gang, Lin Sun, Zhaohui Wu, and Shihong Lao. "Eyeblink- based anti-spoofing in face recognition from a generic web camera." In 11th IEEE International Conference on Computer Vision, pp. 1-8, 2007.

[2] Jiamin Bai ; Tian-Tsong Ng ; Xinting Gao ; Yun-Qing Shi, “Is Physics-based Liveness Detection Truly Possible with a Single Image?”, Proceedings of 2010 IEEE International Symposium on Circuits and Systems, pp.3425-3428,2010.

ISSN:0971-1260

Vol-22-Issue-41-December-2019

[3] Zinelabidine Boulkenafet ; Jukka Komulainen ; Abdenour Hadid, " Face Spoofing Detection Using Colour Texture Analysis", vol.11, No.8, pp.1818-1830,2016.

[4] Jukka Komulainen ; Abdenour Hadid ; Matti Pietikäinen ; André Anjos ; Sébastien Marcel, " 2013 International Conference on Biometrics (ICB) ", pp.1-7,2013.

[5] Samarth Bharadwaj ; Tejas I. Dhamecha ; Mayank Vatsa ; Richa Singh, "Computationally Efficient Face Spoofing Detection with Motion Magnification" 2013 IEEE Conference on Computer Vision and Pattern Recognition Workshops ", pp.105-110,2013.

[6] Sandeep Kumar, Sukhwinder Singh & Jagdish Kumar, "A Study on Face Recognition Techniques with Age and Gender Classification" In IEEE International Conference on Computing, Communication and Automation (ICCCA), pp. 1001-1006, May 2017.

[7] Nesli Erdogmus, and Sébastien Marcel, "Spoofing Face Recognition With 3D Masks",IEEE Transactions on Information Forensics and Security, vol.9, No.7, pp. 1084-1097.

[8] Ivana Chingovska ; André Rabello dos Anjos ; Sébastien Marcel, " Biometrics Evaluation Under Spoofing Attacks ",vol.9,No.12,pp.2264-2276,2014.

[9] Housam Khalifa Bashier, Lau Siong Hoe, Pang Ying Han, Liew Yee Ping and Chiang Mee Li, "Face spoofing detection based on improved local graph structure", International Conference on Information Science & Applications (ICISA), pp.no 1-4, 2014.

[10] Di Wen, Hu Han, and Anil K. Jain, "Face Spoof Detection with Image Distortion Analysis", IEEE Transactions on Information Forensics and Security,2015,vol.1, No.4, pp.746-761,2015.

[11] Sandeep Kumar, Sukhwinder Singh & Jagdish Kumar, "Automatic Face Detection Using Genetic Algorithm for Various Challenges", International Journal of Scientific Research and Modern Education, Vol. 2, No 1, Page Number 197-203, 2017 with ISSN: 2538-4155.

[12] Aziz Alotaibi, AusifMahmood, "Enhancing Computer Vision to Detect Face Spoofing Attack Utilizing a Single Frame from a Replay Video Attack Using Deep Learning", International Conference on Optoelectronics and Image Processing (ICOIP),pp.1-5,2016.

[13] Andre Anjos, Murali Mohan Chakka and S ´ ebastien Marcel "Motionbased counter-measures to photo attacks in face recognition." IET Biometrics, vol. 3, no. 3, pp. 147-158, 2014.

[14] Jianwei Yang ; Zhen Lei ; Dong Yi ; Stan Z. Li, "Person-Specific Face Antispoofing With Subject Domain Adaptation", IEEE Transactions on Information Forensics and Security,vol.10,No.4,pp. 797-809,2015.

[15] Cunjian Chen, Antitza Dantcheva, Thomas Swearingen,, "Spoofing Faces Using Makeup: An Investigative Study" , IEEE International Conference on Identity, Security and Behavior Analysis (ISBA), 2017.

[16] Sandeep Kumar, Sukhwinder Singh & Jagdish Kumar, "A Comparative Study on Face Spoofing Attacks" In IEEE International Conference on Computing, Communication and Automation (ICCCA), pp. 1104-1108, May 2017.

[17] Kudzaishe Mhou ; Dustin van der Haar ; Wai Sze Leung, "Face spoof detection using light reflection in moderate to low lighting", pp.47-52,2017.

[18] J. Galbally, S. Marcel, and J. Fierrez, "Biometric antis poofing methods: A survey in face recognition," IEEE Access, vol. 2, no. 1530-1552, 2014.

[19] Sandeep Kumar, Sukhwinder Singh and Jagdish Kumar "Automatic Live Facial Expression Detection Using Genetic Algorithm with Haar Wavelet Features and SVM" in Wireless Personal Communication Springer Journal (SCI) Published DOI: 10.1007/s11277-018-5923-y.

ISSN:0971-1260

Vol-22-Issue-41-December-2019

[20] 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.

[21] N. Erdogmus and S. Marcel, "Spoofing face recognition with 3d masks," IEEE Trans. Inf. Forensics Security, vol. 9, no. 7, pp. 1084–1097, Jul. 2014.

[22] 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.

[23] Sandeep Kumar, Sukhwinder Singh and Jagdish Kumar, "A Multiple Face Detection Using Hybrid features with SVM Classifier" in the Springer Conference on Data Communication and Networks (Co located with GUCON 2018) with ISBN: 978- 981-13-2254-9 (Scopus Index- Springer Journal.

[24] D. C. Garcia and R. L. de Queiroz and, "Face-spoofing 2d- detection based on moir´e-pattern analysis," IEEE Trans. Inf. Forensics Security, vol. 10, no. 4, pp. 778–786, Apr. 2015.

[25] http://www.comp.hkbu.edu.hk/v1/proj/sre/2018/pc1/

[26] Keyurkumar Patel, Hu Han, and Anil K. Jain, " Secure Face Unlock: Spoof Detection on Smartphones" , vol.11 ,No.10,pp. 2268-2283, 2016.

[27] Patrick P. K. Chan ; Weiwen Liu ; Danni Chen ; Daniel S. Yeung ; Fei Zhang, "IEEE Transactions on Information Forensics and Security",vol.13,No.2,2018.

[28] I. Chingovska, "The 2nd Competition on Counter Measures to 2D Face Spoofing Attacks"Zahid Akhtar, Gian Luca Forest , "Face Spoof Attack Recognition Using Discriminative Image Patches", Hindawi Publishing Corporation, pp.14,2016.

[29] Sandeep Kumar, Sukhwinder Singh and Jagdish Kumar "Live Detection Of Face Using Machine Learning with Multi-Feature Method" in Wireless Personal Communication Springer Journal (SCI) Published.

[30] 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.

[31] H. Yu, T.-T. Ng, and Q. Sun, "Recaptured photo detection using specularity distribution," in Proc. ICIP, 2008, pp. 3140–3143.

[32] A. Pinto, W. Robson Schwartz, H. Pedrini, and A. De Rezende Rocha, "Using visual rhythms for detecting video-based facial spoof attacks," IEEE Trans. Inf. Forensics Security, vol. 10, no. 5, pp. 1025–1038, May 2015.

[33] Pinto, H. Pedrini, W. R. Schwartz, and A. Rocha, "Face spoofing detection through visual codebooks of spectral temporal cubes," IEEE Trans. Image Process., vol. 24, no. 12, pp. 4726–4740, Dec. 2015.

[34] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li, "Face liveness detection by learning multispectral reflectance distributions," -in Proc. FG, 2011, pp. 436–441.

[35] R. Tronci, D. Muntoni, G. Fadda, M. Pili, N. Sirena, G. Murgia, M. Ristori, and F. Roli, "Fusion of multiple clues for photo-attack detection in face recognition systems," in Proc. IJCB, 2011, pp. 1– 6.

[36] R. Raghavendra and C. Busch, "Robust scheme for iris presentation attack detection using multiscale binarized statistical image features," IEEE Trans. Inf. Forensics and Security, vol. 10, no. 4, pp. 703–715, Apr. 2015.

[37] O. Komogortsev, A. Karpov, and C. Holland, "Attack of mechanical replicas: Liveness detection with eye movements," IEEE Trans. Inf. Forensics and Security, vol. 10, no. 4, pp. 716– 725, Apr. 2015.

ISSN:0971-1260

Vol-22-Issue-41-December-2019

[38] A. Czajka, “Pupil dynamics for iris liveness detection,” IEEE Trans. Inf. Forensics and Security, vol. 10, no. 4, pp. 726–735, Apr. 2015.

[39] I. Chingovska and A. Rabello dos Anjos, “On the use of client identity information for face antispoofing,” IEEE Trans. Inf. Forensics and Security, vol. 10, no. 4, pp. 787–796, Apr. 2015.

[46] T. de Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel, “Can face anti-spoofing countermeasures work in a real world scenario?” in Proceedings of the 6th IAPR International Conference on Biometrics (ICB ’13), pp. 1–8,Madrid, Spain, June 2013.

[47] J. Galbally and S. Marcel, “Face anti-spoofing based on general image quality assessment,” in Proceedings of the 22nd International Conference on Pattern Recognition (ICPR ’14), pp. 1173–1178, Stockholm, Sweden, August 2014.

[48] R. Chaudhry, A. Ravichandran, G. Hager, and R. Vidal, “Histograms of oriented optical flow and Binet-Cauchy kernels on nonlinear dynamical systems for the recognition of human actions,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR ’09), pp. 1932–1939, Miami, Fla, USA, June 2009.

[49] Z. Boulkenafet, J. Komulainen, and A. Hadid, “Face antispoofing based on color texture analysis,” in Proceedings of the IEEE International Conference on Image Processing (ICIP ’15), pp. 2636–2640, Quebec City, Canada, September 2015.

[50] Allan S. Pinto, H´elio Pedrini, William Schwartz, Anderson Rocha,” Video-Based Face Spoofing Detection through Visual Rhythm Analysis”, SIBGRAPI, 2012, pp. 221–228.

[51] Tiago de Freitas Pereira, André Anjos, José Mario De Martino, Sébastien Marcel, “LBP − TOP Based Countermeasure against Face Spoofing Attacks”, .ACCV, 2012, pp. 121–132.

[52] K. Kollreider , H. Fronthaler, J. Bigun, “Non-intrusive liveness detection by face images”, Image and Vision Computing, Elsevier, 27 (2009) 233–244.

[53] Murali Mohan Chakka ; André Anjos ; Sébastien Marcel ; Roberto Tronci , "Competition on counter measures to 2-D facial spoofing attacks", International Joint Conference on Biometrics (IJCB),pp.1-6,2011.

[54] William Robson Schwartz ; Anderson Rocha ; Helio Pedrini, " Face spoofing detection through partial least squares and low-level descriptors", International Joint Conference on Biometrics (IJCB), pp.1-8,2011.

[55] N. Kose, J.-L. Dugelay, Classification of captured and recaptured images to detect photograph spoofing, in Proc. ICIEV, pp. 1027– 1032.

[56] S. Chakraborty, D. Das, “An overview of face liveness detection”, IJIT, 3 (2) (2014) 11–25.

[40] J. Yang, Z. Lei, D. Yi, and S. Li, “Person-specific face antispoofing with subject domain adaptation,” IEEE Trans. Inf. Forensics and Security, vol. 10, no. 4, pp. 797–809, Apr. 2015.

[41] J. Sanchez, I. Saratxaga, I. Hernaez, E. Navas, D. Erro, and T. Raitio, “Toward a universal synthetic speech spoofing detection using phase information,” IEEE Trans. Inf. Forensics and Security, vol. 10, no. 4, pp. 810–820, Apr. 2015.

[42] N. Kose and J.-L. Dugelay, “Reflectance analysis based countermeasure technique to detect face mask attacks,” in Proceedings of the 18th International Conference on Digital Signal Processing (DSP ’13), pp. 1–6, IEEE, Fira, Greece, July 2013.

[43] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, “A face antispoofing database with diverse attacks,” in Proceedings of the 5th IAPR International Conference on Biometrics (ICB ’12), pp. 26–31, IEEE, New Delhi, India, April 2012.

ISSN:0971-1260

Vol-22-Issue-41-December-2019

[44] S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, "Faceanti- spoofing via motion magnification and multifeature videolet aggregation," Tech. Rep. IIITD-TR-2014-002, 2014.

[45] S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, and A. T. S. Ho, "Detection of face spoofing using visual dynamics," IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 762–777, 2015.

[57] P. Meadowcroft, Card fraud - will PCI-DSS have the desired impact?, Card Technology Today, 20 (3) (2008) 10–11.

[58] H. Hasan, S. Abdul-Kareem, "Fingerprint image enhancement and recognition algorithms: a survey, Neural Computing and Applications", 23 (6) (2013) 1605-1610, Springer.

[59] D. Menotti, G. Chiachia, A. Pinto, W.R. Schwartz, H. Pedrini, A.X. Falc˜ao, A. Rocha, Deep "Representations for Iris, Face, and Fingerprint Spoofing Detection", IEEE TIFS, 10 (4) (2015) 864–879.

[60] J. Yang, Z.Lei, S. Liao, S.Z. Li, "Face liveness detectionwith component dependent descriptor", in Proc. ICB, 2013, pp. 1–6.

[61] K.B.Housam, S.H. Lau, Y.H. Pang, Y.P. Liew,M.L. Chiang, "Face Spoofing Detection Using Local Graph Structure", in Proc. ICISA, 2014, pp. 270–273.

[62] R.M. Al Eidan, Hand biometrics: Overview and user perception survey, in Proc. ICIA, 2013, pp. 252–257.

[63] Z. Akhtar, G. Fumera, G.-L. Marcialis, F. Roli, Evaluation of serial and parallel multibiometric systems under spoofing attacks, in Proc. BTAS, 2012, pp. 283–288.

[64] N.M.Duc, B.Q.Minh, Your Face isNOT Your Password. FaceAuthentication Bypassing Lenovo-Asus-Toshiba, San Francisco, CA, USA: Black Hat, 2009.

[65] H. Yu, Y. Chen, J. Liu, X. Jiang, Lifelong and fast transfer learning for gesture interaction, Journal of Information & Computational Science 11 (4) (2014) 1023-1035.

[66] W. Zhao, R. Chellappa, P. J. Phillips, A. Rosenfeld, Face Recognition: A Literature Survey, ACMComputing Surveys, 35 (4) (2003) 399–458.

[67] Tanvi Dhawanpatil ; Bela Joglekar ,"Face Spoofing Detection using Multiscale Local Binary Pattern Approach" International Conference on Computing,Communication, Control and Automation (ICCUBEA),PP.1-5,2017

[68] Akbulut, Y., Sengur, A., Budak, U., & Ekici, S, "Deep learning based face liveness detection in videos".International Artificial Intelligence and Data Processing Symposium (IDAP), PP.1- 4,2017.

[69] Manminder Singha,∗, A.S. Arora, "A robust anti-spoofing technique for face liveness detection with morphological operations", Elsevier,Optik, Vol. 139, PP. 347-354.2017.