ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Deliberation on Face Anti-Spoofing Techniques

Deveshree R. More[1], Prof.Vanita Mane[2]

M.E. Student, Department of Computer Engineering, YTCEM, Bhivpuri Road, Karjat, Mumbai, India[1].

Assistant Professor, Department of Computer Engineering, RAIT, Nerul, Navi Mumbai, India[2].

ABSTRACT: A spoofing attack is a situation in which one person successfully masquerades as another by falsifying data and thereby gaining illegitimate access .Face recognition is a widely used biometric approach in recent years. Face biometric systems are vulnerable to spoofing attack. Spoofing attacks are of several types such as photograph, video or mask. A easier technique to bypass face recognition systems is to use photographs of spoofed identity. Various counter measures are present and good results have been reported on the publicly available databases. Facial image textures are used for detecting whether there is a live person in front of camera or a face print. Anti-spoofing technique based on motion analysis is used to measure the correlations between the client head movements and the background scene. Liveness detection techniques try to capture signs of life from the image by analyzing spontaneous movements which can't be detected in photographs. In this content, study of spoofing attacks, anti-spoofing techniques and databases used for anti-spoofing is done.

KEYWORDS**:** Biometrics, Spoofing, Anti-spoofing, Liveness Detection Countermeasures.

I. Introduction

Human characteristics are used as metrics in biometrics. Biometrics authentication is used in computer science as a form of identification and control. Challenges in many biometric recognition systems are to identify spoofing attacks. Spoofing attack occurs when a forged biometric is used to gain illegitimate access to secured resources which are protected by a biometric authentication system. Face recognition system is the high possibility of the system being deceived or spoofed by fake faces such as photograph, video clips or dummy faces. Our biometric information is widely available and extremely easy to sample so, to make face recognition system as a successful biometric identification technology, there is need for answering the spoofing attack problem. Spoofing is the ability to fool a biometric system into recognizing an invalid user as a valid user by means of presenting to the sensor a forged version of the original biometric trait. Recognition using facial information and identity verification has been an active research topic because of its non-intrusive interaction. Face spoof attacks can be classified as 2D which are successful against 2D face recognition systems and 3D attacks which may be used to attack 2D, 2.5D and 3D face recognition systems.

Anti-spoofing is a method used to automatically distinguish between real biometric traits presented to the sensor and forged one. Anti-spoofing is grouped into intrusive liveness detection and non-intrusive liveness detection. In the intrusive approach, the users to respond to a the actions specified by the system. Non-intrusive approach exploits the spontaneous physiological activities of face, such as properties of 3D geometry, eye blinking, skin texture, non-rigid deformation and thermogram. In non-intrusive systems, users are not aware of which clue of liveness is being used, tested and analysed in the face anti-spoofing system.

II. Related work

The first attempt towards spoofing detection based on texture analysis was made in [1], in which the authors argue that there is difference between the frequency distributions on the image of a live person and the image of an attack.

DOI: 10.15680/IJIRCCE.2017. 0506127

In [2], authors proposed a novel physics-based method which detects the images recaptured from printed material using only a single image. In [3], to extract the high frequency information from the face images, the algorithm uses multiple Difference of Gaussian (DoG) filters ,which is treated as the liveness clue. The filtered images are down-sampled to reduce the feature dimension. The achieved EER in [3] is 17%. In [4],a fast and memory efficient method of live face detection based on the analysis of the movement of the eyes for embedded face recognition system, is proposed. Here the achieved EER is 6.5%. System discussed in [5] assist in a biometric authentication framework, by adding liveness awareness in a non-intrusive manner. EER of this method is 0.5%.

III. Texture Analysis

Texture analysis exploits the texture patterns that provide detectable information between the texture of real and fake faces. In this approach, features are extracted from the face images or sequence of images showing certain texture patterns that do not exist in the real faces [6].Face images captured from printed photos may visually look very similar to the images captured from live faces. Consequently, all these images would be largely overlapping in the original input space. Therefore a suitable feature space is needed for separating the two classes (live vs. fake face images). This method focus at learning the fine differences between the images of real face and those of face prints, and then designing a feature space which emphasizes those differences. This method adopts the local binary patterns [7], which is a powerful texture operator, for describing the micro textures and their spatial information. The vectors in the feature space are then given to an SVM classifier which determines whether the micro-texture patterns characterize a live person or a fake image. Fig.1shows examples of images one is a live face and other is a face print in the original space and the corresponding LBP images using basic LBP as feature space. The printed photo looks similar to the image of the live face whereas the LBP images show some differences.

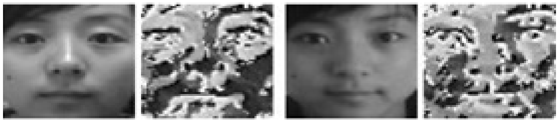


Fig 1: Examples of two images (a live face and a face print) in the original space and the corresponding LBP images using LBP as a feature space [7].

A. Discriminative Feature Space Using LBP

Ojala et al.in [8] introduced the LBP texture analysis operator, which is defined as a gray-scale invariant texture measure. LBP texture analysis is a powerful means of texture description and its properties in real-world applications are its discriminative power, simple to compute and tolerance against monotonic gray-scale changes.

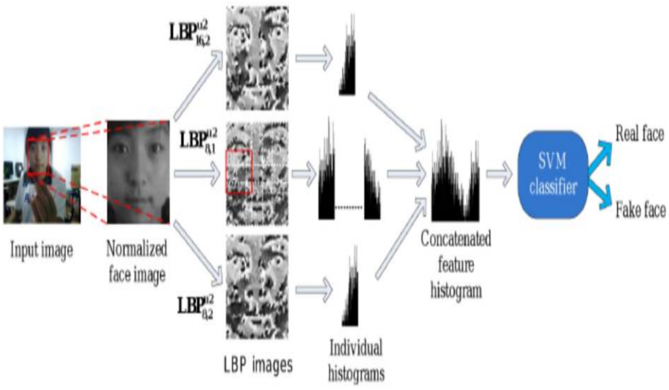


Fig 2: Approach used in [7].

As illustrated in Fig. 2, the approach represented in [7] computes LBP features from 3 × 3 overlapping regions from which the spatial information are captured and the holistic description are enhanced by including global LBP histograms computed over the whole face image. The face is first detected, cropped and normalized into a 64 × 64 pixel image. Then, apply LBP $^{u2}_{8,1}$ operator on the normalized face image and divide the resulting LBP face image into 3×3 overlapping regions. From each region the local 59-bin histograms are computed and collected into a single 531-bin histogram. Then other two histograms from the whole face image are computed using LBP $^{u2}_{8,2}$ and LBP $^{u2}_{16,2}$ operators, yielding 59-bin and 243-bin histograms which are added to the 531-bin histogram computed previously. Hence, the length of the final enhanced feature histogram is 833 (i.e. 531+59+243).Finally, nonlinear SVM classifier with radial basis function kernel is used for determining whether the input image is a live face or not.

B. Classification

A nonlinear SVM classifier is used when the enhanced histograms are computed, with radial basis function kernel to detect whether the input image is a live face or not. The SVM classifier is first trained using a set of positive (real faces) and negative (fake faces) samples.

C. Experimental Analysis

Publicly available NUAA Photograph Imposter Database is considered for performance evaluation which contains images of both real client accesses and photo attacks. The experimental results of [7] showed that LBP has the best performance with equal error rate (EER) of 2.9% compared with other texture operators like Local Phase Quantization (LPQ) and Gabor Wavelets with EER of 4.6% and 9.5% respectively.

IV. MOTION ANALYSIS

The input to motion-based algorithms for anti-spoofing is a sequence of images as perceived by the 2D face recognition input sensor together with the output of a prefixed face detector. Fig 3 shows the setup. Before being fed to the face output of the face detector, the video is first converted to gray-scale and the estimated flows are fed to the counter-measure that outputs scores on which it is finally evaluated [9].

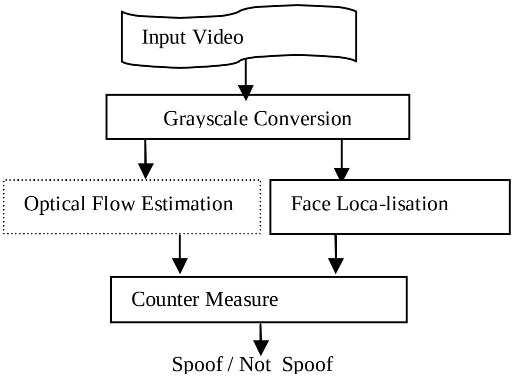


Fig 3: Common setup for all counter measures [9].

This countermeasure explained in [9] is based on foreground/background motion correlation using Optical Flow. Optical Flow Correlation (OFC) algorithm tries to detect motion correlations between the head of the user trying to authenticate and the background of the scene, which indicates the presence of a spoofing attack. Instead of working with averaged intensities, it uses fine-grained motion direction for deriving the correlation between these two regions. The direction of objects in the scene is estimated using Optical Flow (OF) techniques. The use of OFC is expected to grant more precise estimation of motion parameters between the regions of interest in the scene, assuring that motion cues are related in direction and do not come from unrelated phenomena. Instead of lump-summing intensities, OFC quantizes histograms, normalizes and motion direction vectors from the two regions of interest are compared in order to provide a correlation score, for every analyzed frame. OFC also introduces a new hyper-parameter that controls the amount of specific or global information that is considered while performing discrimination. The number of directions

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Q used by the algorithm determines if the detector will observe motion patterns which may be related to specific acquisition conditions or application independent.

A. *Feature Extraction*

The feature extraction has 4 steps as depicted in Fig 4. The input consists of the OF horizontal and vertical velocity estimates and uses the face bounding boxes available in the database to separate features from the face and background regions.

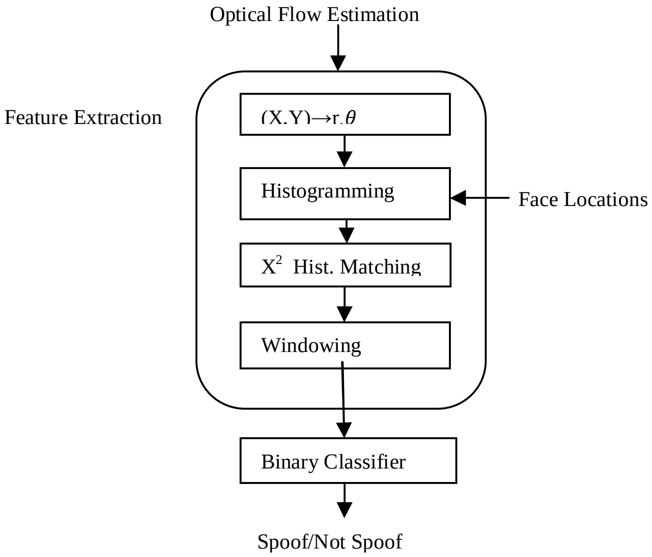


Fig 4: Block diagram of counter-measures to spoofing attacks using correlation with optical flow [9].

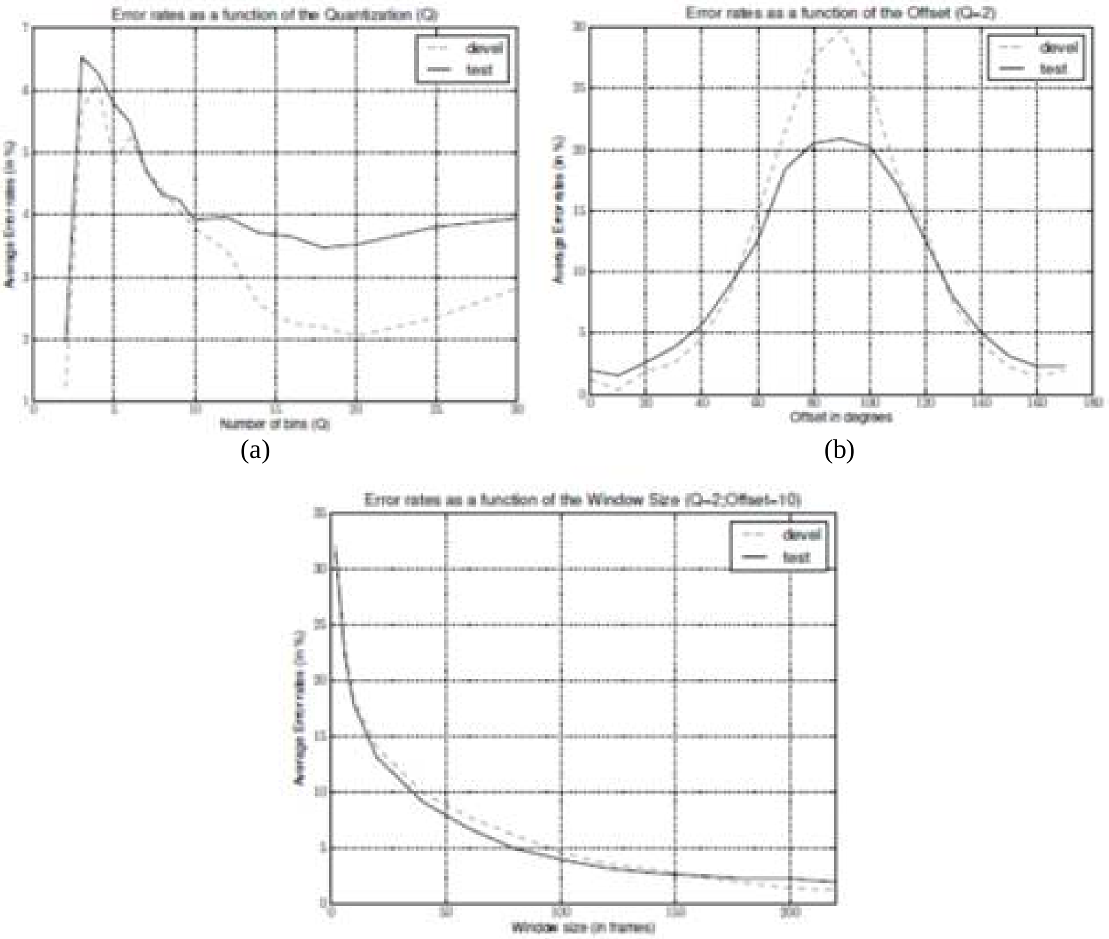
B. *Classification*

The binary classifier, which detects the spoofing attacks based on a threshold on the equal error rate (EER) tunned at the development set is fed with the scores computed from the windowing unit. Ideally, from above equation, attacks are expected to have scores close to 0 due to correlated motion between the face and the background areas. Scores of real accesses should be greater than 0 due to the fact that the face region moves independently from the background region [9].

C. *Experiment Analysis*

This algorithm measures motion correlation between face and background in [9] solely using the movement direction. To deploy it, one needs to tune 3 hyper-parameters: the number of bins Q used for the angle histograms, the amount of offset from the horizontal axis and the window-size used for the averaging processes, towards the end of the tool chain.

DOI: 10.15680/IJIRCCE.2017. 0506127



(a) (b)

(c)

Fig. 5: (a) Experimental results with varying number of bins Q on the PHOTO-ATTACK database for our contribution based on OFC. Fixed parameters are the Offset = 0o, Window-size (N) = 220 frames and the Overlap = 219 frames. (b) Experimental results varying the offset in steps of 10 o for OFC. Fixed parameters are the number of bins in the quantization step Q = 2, Window-size (N) = 220 frames and the Overlap O = 219 frames. (c) Experimental results varying the window-size for OFC. Fixed parameters are the number of bins in the quantization step Q = 2, the Offset = 10 o and the Overlap O = 219 frames [9].

V. Life Sign Detection Method

A human can distinguish a live face or a photograph without much effort, as a human can easily recognize many physiological clues of liveness, such as mouth movement, head rotation, eye change, facial expression variation. However, sensing these clues is very tough job for a computer, even under an unconstrained environment [10].

A. *Eyeblink for Liveness Detection*

Eyeblink is an activity of rapid closing and opening of the eyelid. The generic camera can easily capture the face video with not less than 15 fps i.e. the frame interval is not more than 70 milliseconds. Thus, it is easy for the generic camera to capture two or more frames for each blink when the face looks into the camera. Eyeblink is used easily as a measure for anti-spoofing. The advantages of eyeblink based approach are 1) it is completed in a non-intrusive manner without user collaboration, 2) no extra hardware is required, 3) the eyeblink behavior is the distinguishing character of a live face from a face photograph, which would be very helpful for liveness detection only from a generic camera.

The eyeblink behavior could be represented as a temporal image sequence after being digitally captured by the camera. One method to detect blink is to classify each image in the sequence independently as one state of either closed eye or opened eye. As the blink is a procedure of eye going from open to close and back to open, the neighboring images of blinking are dependent. The temporal information is ignored for this method, which may be helpful for recognition. This independence assumption can be relaxed by positioning the state variables in a linear chain. HMM assumes that each state depends only on its immediate predecessor, and that each observation variable depends only on the current state [10].

B. *Conditional Modeling of Blinking Behaviors*

An image sequence S consisting of T images represents an eyeblink activity, where S = {I i ,i =1,...,T}. Opening and closing are the basic eye states. Blinking from open state to close or from close state to open creates an ambiguous state. Three-state set for eyes are defined as, Q = {α : open, γ : close, β : ambiguous}. Thus, a blink activity is defined as a state change pattern of α → β → γ → β → α. Consider, that S is a random variable over observation sequences to be labeled, and Y is a random variable over the corresponding label sequences to be predicted, all of components yi of Y are assumed to range over a finite label set Q. Let G = (V,E) be a graph and Y is indexed by the vertices of G. Then (Y,S) is called a conditional random field (CRF), when conditioned on S, the random variables Y and S obey the Markov property[10].

C. *Eye Closity*

To measure the degree of eye's closeness, eye closityU(I) is used, which is constructed by a series of weak binary classifiers and computed by an iterative procedure. The eye closity can be considered as a sense of the ensemble of effective features. From insight into the training procedure of Adaboost algorithm, the positive value of closity indicates that the Adaboost classifier will classify the input as the close eye, and the negative value as the open eye. The bigger the value of closity, the higher the degree of eye closeness. The closity value of zero is exactly the threshold for the Adaboost classifier [10].

D. *Experiment Analysis*

An analysis is carried out with various windows size of W = {0,1,2,3,4} is carried out. The results are shown in Fig.6, the one-eye detection rate significantly increases when the windows size goes from zero to three, which shows that there is a strong dependency between the current state and the neighboring observations. One-eye detection rate or two-eye detection rate of performance is very near for W = 3 and W = 4, which shows the dependency becomes weak between the current state and the observations far from its corresponding observation. The window size of W = 3 means the contextual observations of 7 frames used for the conditional modeling. A blink activity average 7-8 frames shows that the observations out range of a blink activity have little contribution to the blink detection.

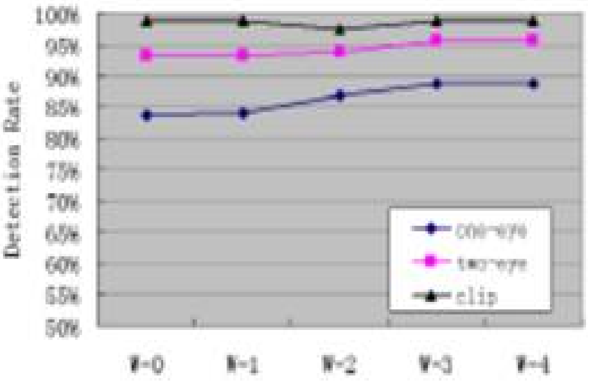


Fig 6. Results of various window size: W = {0,1,2,3,4}[10].

VI. Comparative Study

Texture analysis based approach is simple to implement and user collaboration is not required. The systems built on texture analysis must be robust to various texture patterns which require the presence of a very diverse dataset. It is possible that the attack which is performed by displaying a photo on a screen, which produces very low texture information. Motion analysis, differentiates the motion pattern between 3D and 2D faces as planar objects move in different way from real human faces which are 3-D objects. Motion analysis depends on optical flow calculated from video sequences. When using motion analysis, it is very difficult to spoof by 2D face image and is independent of texture and user collaboration is not required. Motion analysis requires video and it is difficult to use motion analysis when the video have low motion activity. When there is low motion information, motion analysis has to face problems. When spoof attacks is performed using more complicated methods, like 3D mask, motion analysis may fail. Detection of life signs can be of two types. First one assumes some known interaction from the user. Here, the user needs to perform a certain task to verify the liveness of face image. This task can be a certain movements. Users who will perform their task correctly are assumed to be real. Second one does not assume any interaction from the user, but focuses on certain movements of some parts of the face, such as eye blinking, and will consider those movements as a sign of life and therefore a real face. Life sign based liveness detection based approach is not easy to spoof by 2D face images and 3D sculptures. This approach is independent of textures but it may need user collaboration.

Table 1.shown below gives the advantages and disadvantages of liveness detection approaches.

Table 1. Advantages and Disadvantages of liveness detection approaches

Liveness detection approaches	Advantages	Disadvantages	Cost of system	Performance
Texture[7]	1. Easy implementation. 2. No user collaboration required. 3. Fast response.	1. Images with low texture information. 2. Dataset must be diverse.	Low level	EER=2.9%
Motion[9]	1. Independent of texture. 2. Hard to spoof. 3. No user collaboration required.	1. Needs video sequence. 2. Difficult to use when video has low motion activity. 3. Can be spoofed by 3D sculptures.	Medium level	HTER=10%
Life Sign[10]	1. Difficult to spoof using 2D image or 3D sculptures. 2. Independent of texture. 3. Good performance under bad illumination conditions.	1. User collaboration is may required. 2. Depends on face part detection. 3. Needs video sequence. 4. Slow response.	High level	Avg one-eye rate of 88.8% . Avg two-eye rate of 95.7%

VII. Conclusion

Security of biometric system should be in better way so more and more successful spoofing attempts are being implemented. Many authors are showing their efforts to make biometric devices more robust but every countermeasure can eventually be bypassed in some way. Thus, efforts of research and development should go on. This work provides an overview of different types of spoof attacks and different anti-spoofing techniques. A review of approaches for liveness detection was presented. Micro-texture based approach used multi-scale local binary patterns (LBP) to encode the micro-texture patterns into an enhanced feature histogram. Then the results are fed to a SVM classifier which determines whether there is a live person in front of the camera or not. This approach is robust, computationally fast and does not require user-cooperation. This approach is robust, computationally fast and doesn't require user-cooperation. This approach can be extended to detect spoofing attacks done by the use of masks or 3D models of the face because skin has a very particular texture and fake faces have seldom such a level of detail. Optical flow technique based on motion correlation, achieves perfect scoring with an EER of 1.52% on the available test data. The advantages of eye blink-based method are non-intrusion and no extra hardware requirement. To recognize the eye blink behavior, dependencies are modeled among the observations and states in an undirected conditional graphical framework, embedded a new-defined discriminative measure of eye state in order to fast response as well as convey the most effective discriminative information. Liveness detection methods based on eye blinking and movement of eyes, reflection caused by eyes glasses must be considered for future development of liveness detection solutions. Future attack datasets must consider attacks like 3D sculpture faces and improved texture information.

REFERENCES

[1] Jiangwei Li,Yunhong Wang, Tieniu Tan,A.K.Jain, “Live Face Detection Based On The Analysis Of Fourier Spectra,” Biometric Tecnology for Human Identification, 2004. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[2] Jiamin Bai,Tian-Tsong Ng,Xinting Gao,Yun-Qing Shi,“Is physics-based liveness detection truly possible with a single image?” in IEEE International Symposium on Circuits and Systems (ISCAS), May 2010. K. Elissa, “Title of paper if known,” unpublished.

[3] Zhiwei Zhang, Junjie Yan,Sifei Li,Zhen Lei,Dong Yi,Stan Z. Li, “A face antispoofing database with diverse attacks,” in Proceedings of the 5th IAPR International Conference on Biometrics (ICB’12), New Delhi, India, 2012. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[4] H. K. Jee, S. U.Jung, and J. H. Yoo, “Liveness detection for embedded face recognition system,” Engineering and Technology, 2006.

[5] K. Kollreider, H. Fronthaler, and J. Bigun, “Non-intrusive liveness detection by face images,” Image and Vision Computing, vol. 27, no. 3, 2009.

[6] SajidaParveen , SharifahMumtazah Syed Ahmad , MarsyitaHanafi and Wan Azizun Wan Adnan, “Face anti-spoofing methods” , Current Science, Vol. 108, No. 8, 25 April 2015.

[7] J. Maatta, A. Hadid, and M. Pietikainen, “Face spoofing detection from single images using micro-texture analysis,” in Proc. International Joint Conference on Biometrics (IJCB 2011),Washington, D.C., USA, 2011.

[8] T. Ojala, M. Pietikäinen, and T. Mäenpää.Multiresolution gray-scale and rotation invariant texture classification with local binary patterns” , IEEE Trans. Pattern Anal. Mach. Intell., 24:971–987, July 2002. 2, 3, 4

[9] André Anjos, Murali Mohan Chakka and Sébastien Marcel, ”Motion-Based Counter-Measures to Photo Attacks in Face Recognition”,

[10] Gang Pan , Lin Sun, Zhaohui Wu, Shihong Lao, “Eyeblink-based Anti-Spoofing in Face Recognition from a Generic Webcamera”.