Invited Paper

Efficient live face detection to counter spoof attack in face recognition systems

Bikram Kumar Biswas and Mohammad S. Alam

Department of Electrical & Computer Engineering, University of South Alabama,
Mobile, AL, USA, 36688

ABSTRACT

Face recognition is a critical tool used in almost all major biometrics based security systems. But recognition, authentication and liveness detection of the face of an actual user is a major challenge because an imposter or a non-live face of the actual user can be used to spoof the security system. In this paper, a robust technique is proposed which detects liveness of faces in order to counter spoof attacks. The proposed technique uses a three-dimensional (3D) fast Fourier transform (FFT) to compare spectral energies of a live face and a fake face in a mathematically selective manner. The mathematical model involves evaluation of energies of selective high frequency bands of average power spectra of both live and non-live faces. It also carries out proper recognition and authentication of the face of the actual user using the fringe-adjusted joint transform correlation technique, which has been found to yield the highest correlation output for a match. Experimental tests using real life datasets show that the proposed technique yields excellent results for identifying live faces.

KEYWORDS: Biometric Tools, Liveness Detection, Face Recognition, Spoof Attack, Joint Transform Correlator

1. INTRODUCTION

Biometrics is extensively used in many security applications such as surveillance systems, identity verification systems, and multimedia environments in order to identify individuals so that a wrong person cannot spoof the system. To prevent spoofing attacks, face recognition of the right person is essential. But face recognition alone cannot full-proof the system from being abused by unauthorized users, because a copy of the biometric trait can be used as an imposter to enter and break the security system. For that reason, liveness detection is crucial to ensure whether the biometric trait is from a live user or not. Common biometric properties are fingerprint, iris, face, voice, and palm. These properties can be sensed and measured by appropriate sensor equipment. Biometrics traits of individuals are stored in a database to verify them for particular applications. Among the various biometric features face recognition is used in almost all security and surveillance systems in order to identify a person for a given application or in a crowded place.

A spoof attack is a condition where one person pretends to be another person in order to access a system to steal, crack or damage information. A facial image can be used more than any other biometric modalities in security systems because other biometric traits need user help to complete the authentication process. For example, a user has to put his/her finger on a scanner to be identified by the system. But a face can be used without user help to recognize individuals by capturing photos or videos using cameras. At the same time, spoof attack conducted by using a print image of an individual is also easy and may be used to break into a face recognition based security system. It is very difficult for the face recognition system to differentiate between a real user and a fake user. To counter such types of attacks, researchers in recent times, put their efforts to detect liveness of faces or other biometric traits in their recognition systems [1]. Three common types of face spoof attacks are print photo attack, print mask attack and replay-video attack.

Face recognition is based on the detection and extraction of facial features of individual's. If an intruder wears a three-dimensional (3D) mask of a person, it is difficult for the face recognition system to detect it because the mask has all biometric properties like the original person. What is absent in the mask is liveness. Liveness corresponds to the change

Optical Pattern Recognition XXVI, edited by David Casasent, Mohammad S. Alam,
Proc. of SPIE Vol. 9477, 947703 · © 2015 SPIE · CCC code: 0277-786X/15/$18
doi: 10.1117/12.2177975

of a person's physiological or behavioral characteristics. A 3D mask or 2D print photograph does not carry as much detail as the live face. The task of a liveness detection system is to extract the difference between biometric properties of a live individual and its copy. Liveness detection of face can be performed by using software, hardware or a combination of both. Existing liveness detection methods are based on different approaches, ranging from frequency and texture based analysis to movement of facial features. Fourier transform based methods can play an important role in these contexts, which utilize Fourier spectra of both live face images and non-live face images into account for discrimination purposes. The focus of this paper is to develop a robust and efficient way to detect the liveness of a facial image by efficiently utilizing the Fourier spectra.

Face detection methods fall into two broad categories: image based and facial feature based [2]. The aim of face detection is to detect the location of facial features such as eyes, nose, ears, mouth, lips etc. During the last few decades researchers have made important progress in the field of face recognition [2-9]. Portland et al. [4] proposed a technique based on facial feature detector generated from Eigen features. Meng and Nguyen [5] developed an algorithm based on principal component analysis (PCA) which was used to make face images and background clutter. Several segmentation based algorithm using skin color information and composition was reported [6-9]. Face detection from a video sequence was done by motion analysis and segmentation [10].

Effective face recognition task is a challenging problem due to change in facial expression, aging, geometrical change during image acquisition, image rotation, illumination variations, use of mask and glasses etc. No particular technique is proven to be capable of combating all these challenges. Over the past thirty years, many techniques for face recognition have been devised by researchers [11, 12,13]. Face recognition methods can be broadly classified into two categories: Holistic based methods and Feature-based methods. Holistic based methods use the whole image region as a subject rather than local features like eyes, nose, and ears. Feature-based methods use local facial features like eyes, nose, lips, ears, and mouth into account and extract their characteristics, locations and statistical data to fit with standard pattern recognition techniques.

2. ANALYSIS

In the early 90's, a novel pattern technique called fringe-adjusted joint transform correlation (JTC) [14] was introduced which has been found to yield the highest correlation output and relatively effective to changes in illumination conditions. In the fringe-adjusted JTC technique, a reference image,$r(x, y + y')$, and an input image, $t(x, y - y')$, are introduced in the input plane separated by a distance $2y'$ along the y axis. Then the input joint image $f(x, y)$ can be expressed as

$$f(x, y) = r(x, y + y') + t(x, y - y') \quad (1)$$

The corresponding joint power spectrum (JPS) is given by

$$|F(u, v)|^2 = |R(u, v)|^2 + |T(u, v)|^2 + 2|R(u, v)||T(u, v)| \times \cos[\varphi_r(u, v) - \varphi_t(u, v) + 2vy'] \quad (2)$$

where$|R(u, v)|$ and $|T(u, v)|$are the amplitudes, and $\varphi_r(u, v)$ and$\varphi_t(u, v)$ are the phases of the Fourier transforms of , $r(x, y)$, and $t(x, y)$, respectively.

To avoid the pole and gain problems associated with the above mentioned method, the joint power spectrum is multiplied by a real-valued fringe-adjusted filter (FAF), defined as

$$H_{faf}(u, v) = \frac{B(u,v)}{A(u,v)+|R(u,v)|^2} \quad (3)$$

where, $A(u, v)$ and $B(u, v)$ are either constants or functions.

The fringe-adjusted filter is then multiplied by the JPS yielding

$$G(u,v) = \frac{B(u,v)}{A(u,v)+|R(u,v)|^2}\{|R(u,v)|^2 + |T(u,v)|^2 + 2|R(u,v)||T(u,v)| \times \cos[\varphi_r(u,v) - \varphi_t(u,v) + 2vy']\} \quad (4)$$

If the reference image matches the input image, the autocorrelation output will consist of two delta-functions-like outputs located at $\pm 2y'$ and a zero order term. The zero order term can be suppressed by additional further processing such as the Fourier plane image subtraction technique [15].

Liveness detection approaches can be broadly classified into three categories: motion based, texture based and life sign based. Movement of the eye based analysis was introduced for embedded face recognition system [16], which takes variation of each eye-region of input images into account to differentiate between live images and non-live or fake images. A similar approach was taken by Liting, et al. [17] for liveness detection, which is based on physiological motion detected by estimating eye blinks from a video sequence and an eye contour extraction algorithm. Spoofing attacks on a security system can be done mostly by using a print image, a photograph image, or a video frame [18] which may be combated only by detecting the liveness of these media. An efficient liveness detection approach for prevention of a spoof attack in a face recognition system was proposed by Nalinaksh et al. [19], which is based on the localization of eyes, lips, forehead, chin and their variations. A 3D face shape based analysis was proposed by Lagorio et al. [20], which exploits the 3D structure of the face to detect liveness. Another approach proposed by Socolindky et al. [21] to detect spoof attack by determining vein map of face using a thermal infra-red sensor.

A binary classification based anti-spoofing technique was proposed by Tan et al. [22] which used the structure difference between a real human face and a photo face. For detecting face spoof, Maatta et al. [23] proposed an approach which used multi-scale local binary patterns to analyze the texture of the facial images. Chingovska et al. [24] proposed a face anti-spoofing method based on local binary pattern (LBP) which examined effectiveness of the method against three types of spoofing attacks: print photographs, photos, and video attacks. Reference [25] provides a summary of anti-spoofing criteria in terms of their data quality and other characteristics.

The basic difference between a live face and a print image is that a live face has 3D shape variance while a 2D print image or a photograph has a flat surface. Also, a 2D print image does not carry much detail like a 3D live face image. Moreover, live images contain more high frequency components than that of print or photograph images. According to Lambertian surface model, image intensity of a live image due to a point source is more focused than that of a fake image [26]. A frequency domain approach was proposed to evaluate the 2D Fourier spectra of live and non live images. Li et al. [27] proposed a live face detection method based on the analysis of Fourier spectra. A 2D Fourier transform $F(u,v)$ of an image $f(x,y)$ can be expressed as

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)e^{-j2\pi(\frac{ux}{M}+\frac{vy}{N})} \quad (5)$$

where M represents the number of pixels in x-direction, N represents number of pixels in y-direction, and $f(x,y)$ represents the image.

In [27], a high frequency descriptor (HFD), is defined as the ratio of the energy of high frequency components to that of all frequency components. The HFD parameters can be effectively used to differentiate between live and fake faces, and is given by

$$HFD = \frac{\iint_{\Omega=\{(u,v)|\sqrt{u^2+v^2}>\frac{2}{3}f_{\max} \text{ and } |F(u,v)|>T_f\}} |F(u,v)|dudv}{\iint |F(u,v)|dudv - F(0,0)} \times 1000 \quad (6)$$

where f_{max} is the highest radial frequency, and T_f is a predefined threshold.
But to determine the Fourier transform of an image from a live video sequence, Fourier transform must be applied in 3D planes so that the time dimension can be incorporated besides the spatial dimensions.

The 3D Fourier transform of an image $f(x,y,t)$ can be expressed as

$$F(u,v,w) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\sum_{t=0}^{L-1} f(x,y,t)\, e^{-j2\pi(\frac{ux}{M}+\frac{uy}{N}+\frac{wt}{L})} \tag{7}$$

where L represents the total frames recorded from a video sequence for a prescribed duration.

3. PROPOSED METHOD

As discussed in previous section that the result obtained by using HFD cannot differentiate between live and fake faces for motion images. It is less efficient for a very clear and large sized print image. It will not give better result for the frame taken from a live face video sequence. It is not feasible to take only two-third of the maximum radial frequency to differentiate between them. Small illumination change will bring a bigger change in HFD although illumination is assumed invariant.To overcome these limitations, the following algorithm is proposed in this paper which efficiently performs face recognition as well as liveness detection of the recognized face.
The proposed model is shown in figure 1, which may be divided into two phases:

a) Face recognition and authentication and b) Liveness detection

The main steps involved in the face recognition and authentication stage are:
Step 1: Record frames from a live face video (reference) and a fake face video (input).
Step 2: Record Fourier transform and joint power spectra of selected frames.
Step 3: Subtract input scene only power spectrum and reference image only power spectrum from the joint power spectrum.
Step 4: Multiply the modified JPS from step 3 with the fringe-adjusted filter.
Step 4: Apply inverse Fourier transform to obtain the correlation output.
Step 5: If the reference matches with the unknown input scene, initiate the liveness detection. If the images do not match, stop the process.

The main steps involved in the liveness detection stage are:
Step 1: Apply 3D FFT to the input and reference frames as shown in Figs.2 (a) and 2(b).
Step 2: Evaluate the average power spectra of the selected input and reference image frames.
Step 3: Design a band pass filter with a suitable cut off frequency and filter out low frequency (or illumination) components from the average power spectra of the input and reference image frames as shown in Figs 2(c).
Step 4: Divide the rest of the power spectrum by using a few circular bands and calculate the corresponding energies i.e., energies of high frequency components as shown in Fig. 2(d).
Step 5: Calculate the energy of each band for both input and reference images.
Step 6: Evaluate the maximum energy values of input and reference images and calculate their differences.
Step 7: If the normalized maximum energy value of average energy spectrum of reference images (P_R)is higher than the normalized maximum energy value of average energy spectrum of input images ($P_{I)}$,and the difference is higher than a threshold value (here is 100), liveness of a reference image is confirmed.

The proposed liveness index, η, may be defined as

$$\eta = \max\left(\max\left(\sum_{0}^{L_R}\frac{P_R(u,v,w)}{L_R}\right)\right) - \max\left(\max\left(\sum_{0}^{L_I}\frac{P_I(u,v,w)}{L_I}\right)\right) \tag{8}$$

where$L_R$and L_I are the numbers of tested frames corresponding to the of reference and input video frames.

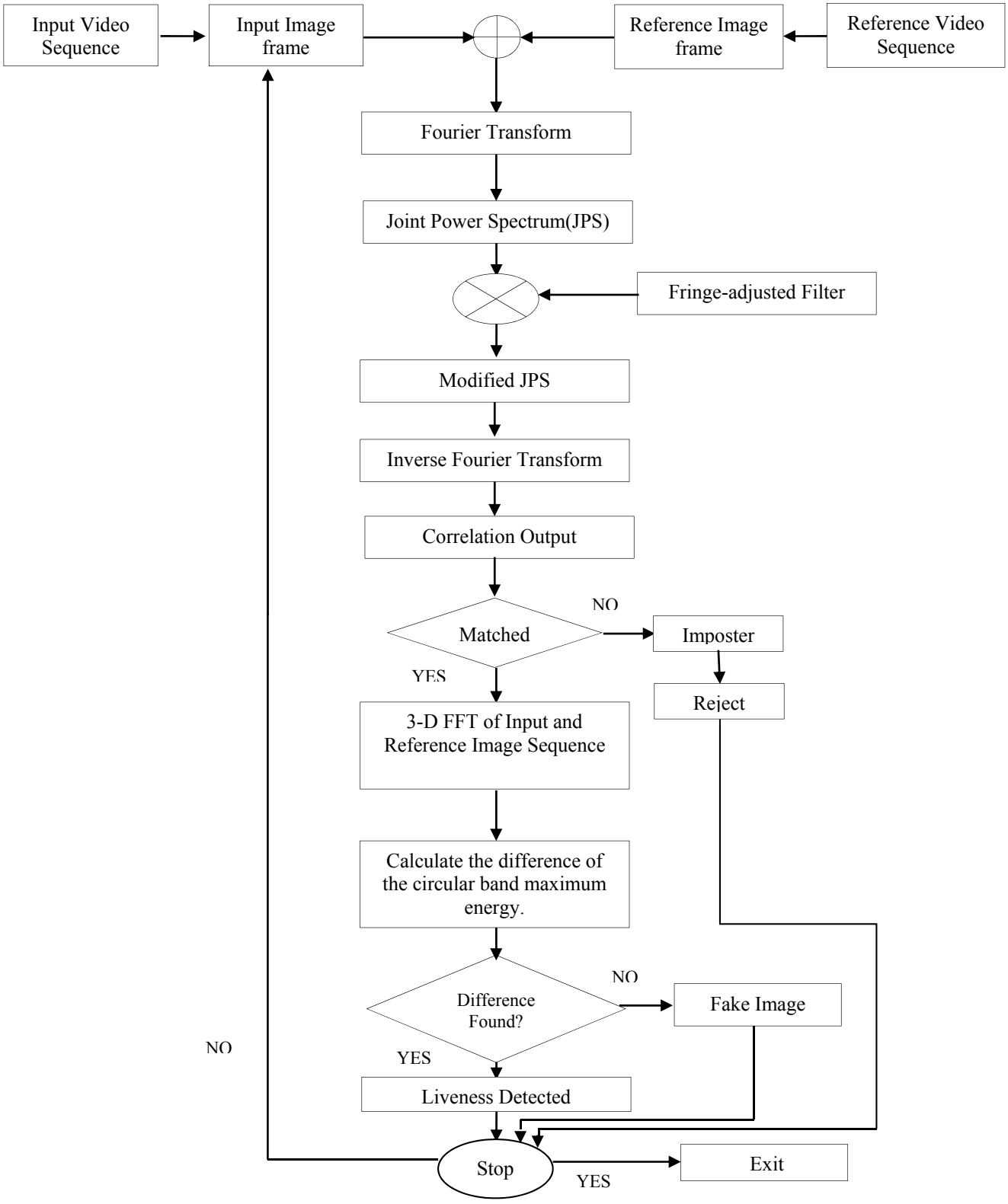

Figure 1: Flowchart of the proposed technique

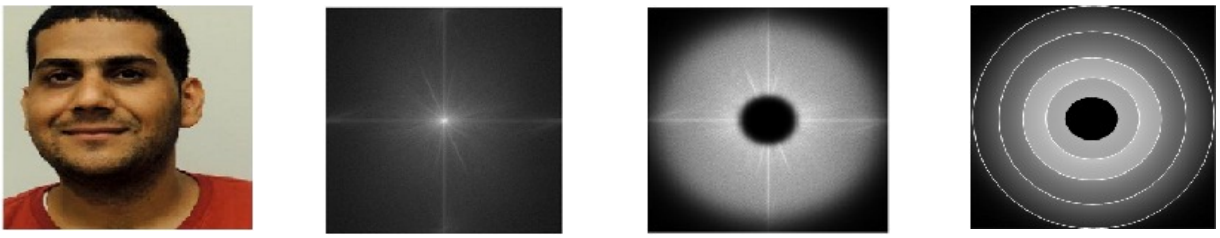

Figure: 2(a): An Image Frame, (b): 3-D FFT of (a), (c): Average power spectrum after passing through a band pass filter, (d): Formation of circular band from the power spectrum

If the normalized maximum energy value of average energy spectrum of the reference images (P_R) is lower than that of the normalized maximum energy value of average energy spectrum of the input images (P_I), by 100 or less, the algorithm will go trigger the single image frame analysis. If the normalized energy value of the energy spectrum of a single reference image frame is higher than the normalized energy value of energy spectrum of a single input image frame, then the liveness of a reference image will be confirmed.

4. EXPERIMENT

Experimental tasks were conducted in Vision, Image Processing, and Sensing (VIPS) laboratory involving twenty volunteers. For the database, videos of each individual were recorded using a digital camera. The images were printed using a laser printer on a paper of size 200×300 mm. The experimental task is divided into four phases:

a. Recording live videos of the persons.
b. Recording fake videos of the persons using their printed photographs.
c. Recording fake videos of the persons using their videos recorded in step a.
d. Liveness test using the Matlab software package.

All video recordings are performed under normal and low illumination conditions.
In addition, all video recordings included the following pose variations:

i) Subject in normal position, ii) Subject moving left, iii) Subject moving right,
iv) Subject moving upward, and v) Subject moving downward

Furthermore, live videos involving normal facial expression changes such as eye blinking, mouth movement, and smiling were also incorporated.

For experimental verification of the proposed liveness detection technique, a database was created with twenty individuals. The duration of each video was around ten seconds and each video contained twenty nine (29) frames per second. The input and reference image frames were taken from the video sequences using twenty (20) images at a given time and each frame includes 1920×1080 pixels. Facial pose variations of the aforementioned individuals were also taken into account. Then the proposed model was tested using the MATLAB software package. A few live image frame sequences of the volunteers recorded under normal illumination condition is shown in Fig. 3. Figure 4 shows some of the selected fake image sequences recorded from the video sequences which includes two scenarios when print image is in horizontal motion and print image is under normal illumination. It also includes a fake image sequence that was recorded from the original video sequence. Spoof attacks using video replay is called replay-video attack.

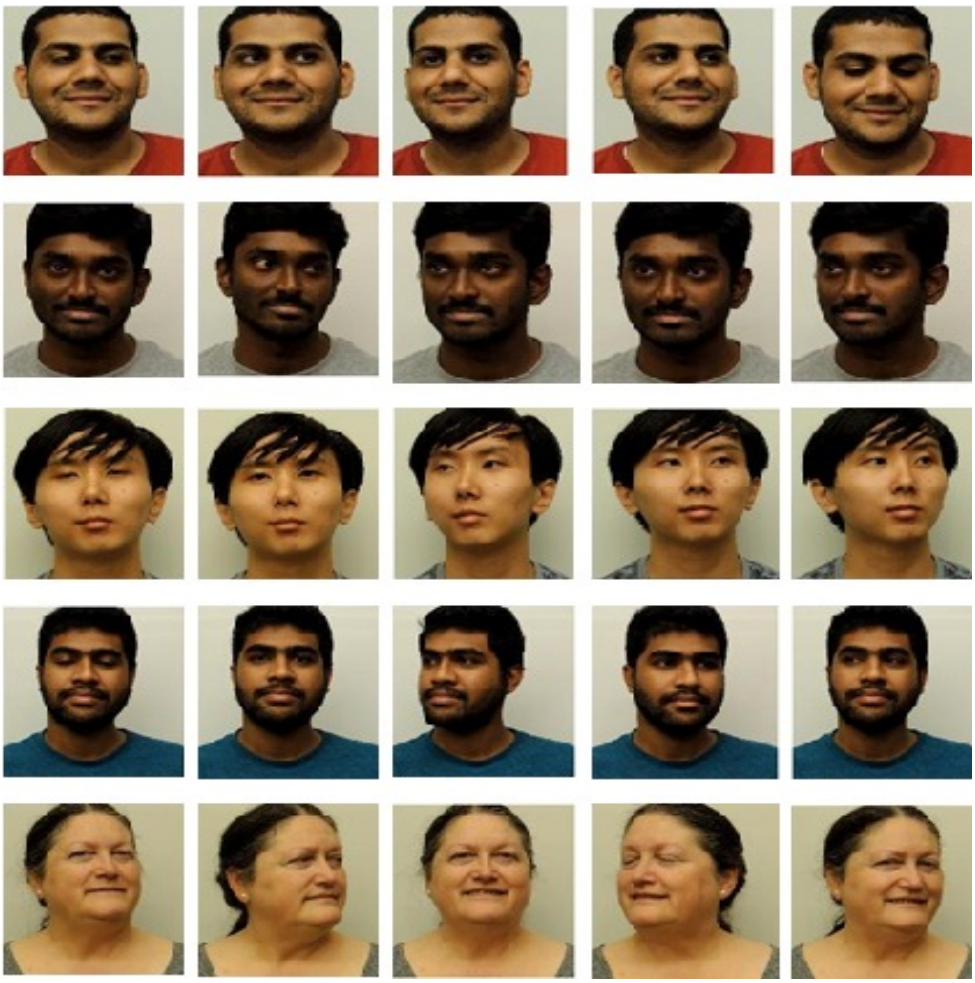

Figure 3: Live image frame sequences of different faces under normal illumination

Figure 4:Fake image sequences of different faces: Print images in horizontal motion[Top], Print image under normal illumination [Middle], and Replay-video attack[[Bottom]

5. RESULT

5.1 Input image under normal illumination

Four reference image frames were selected from a live video sequence and four input image frames were selected from a photograph video sequence at different instants of time and their Fourier spectra were calculated as shown in Figs. 5(a) and 5(b), respectively. In general, live image frames contain various pose variations and their Fourier spectra are also different.Due to the absence of pose variations the Fourier spectra of fake image frames are similar. Figure 6 shows a plot of the normalized energy as a function of the radial frequency for both reference and input images. It clearly depicts that maximum normalized energy of the reference image is higher than that of the input image. It occurs at the radial frequencies band lying between 2 and 3. So, one can infer that the input image is a fake or a non-live image.

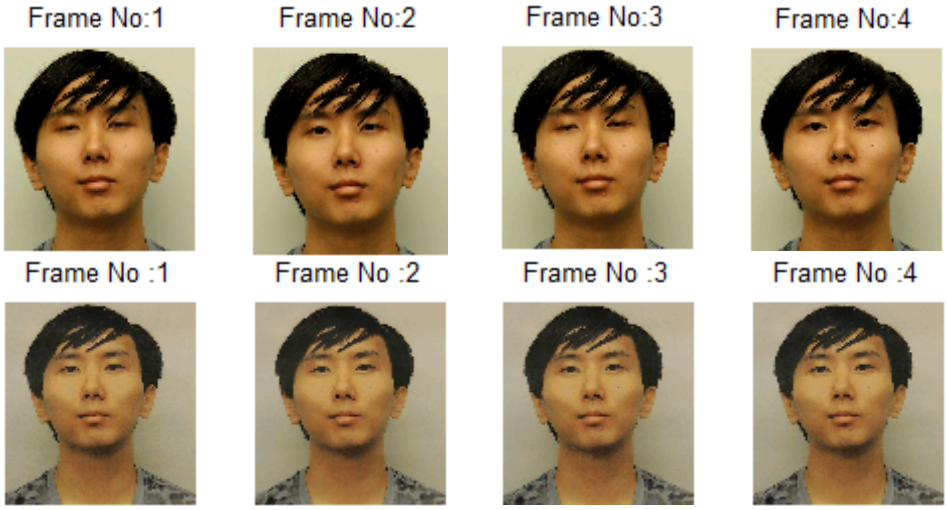

Figure 5(a) [Top]: Reference live frame sequences, and 5(b): Input print image frame sequences

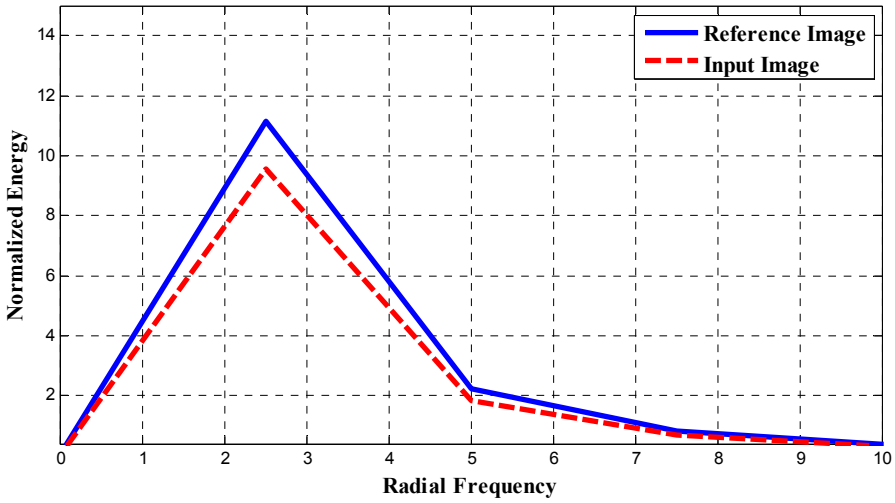

Figure 6: Plot of normalized energy vs. radial frequency for normal illumination

5.2 Input image under low illumination

Four reference image frames were selected from a live video sequence and four input image frames were selected

from a photograph video sequence at different instants of time and their Fourier spectra were calculated as shown in Figs. 7(a) and 7(b), respectively. The illumination is kept low while recording the print photograph video sequences. Due to absence of the pose variations the Fourier spectra of fake image frames are similar. Figure 8 clearly demonstrates the liveness of the reference image as its maximum average energy is higher than that of the input image which occurs at the radial frequencies band lying between 2 and 3.

Figure 7(a) [Top]: Reference live frame sequences, and 7(b): Input print image frame sequences

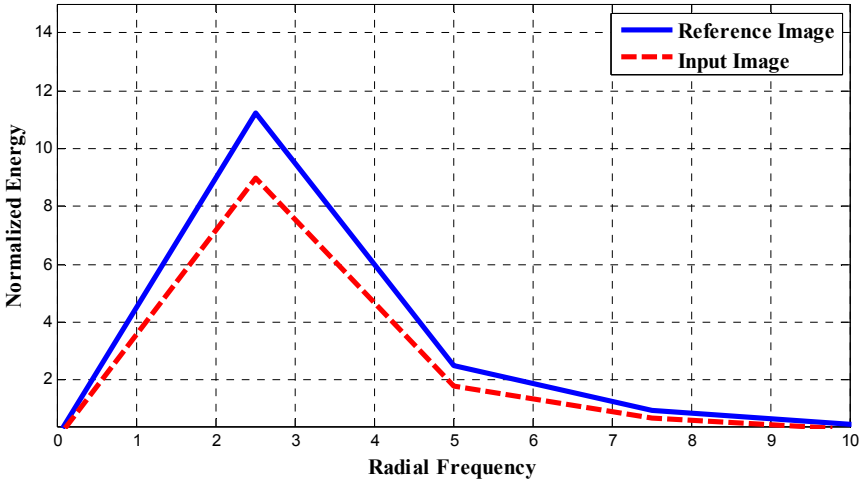

Figure 8: Plot of normalized energy vs. radial frequency for low illumination

5.3 Replay-video attack

Figure 9(a) shows four reference image frames selected from a live video sequence and Figure 9(b) shows four input image frames selected froma video sequence that was recorded from the original video sequence at different instants of time. This type of video spoofing attack can also be prevented by using the proposed algorithm. Figure 10 verifies the accuracy of the algorithm. Image frames contain pose variations as they were recorded from the original live video sequence. Live image frames still contain higher band selective energy than that of the input video attack image frames although theycontain more movement and variations than that of the print image attack. Again the maximum energy difference occurs at the radial frequencies band between 2 and 3.

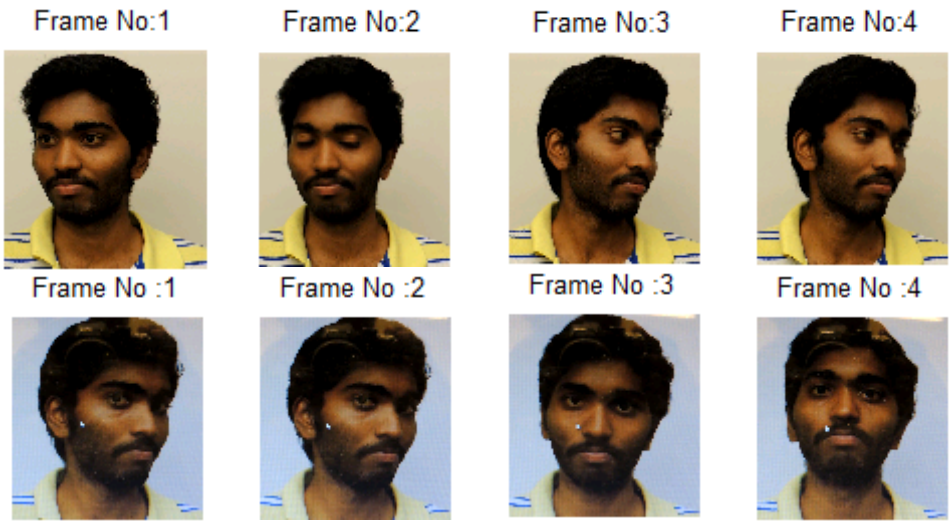

Figure 9(a) [Top]: Reference live frame sequences, and 9(b): Input replay-video frame sequences

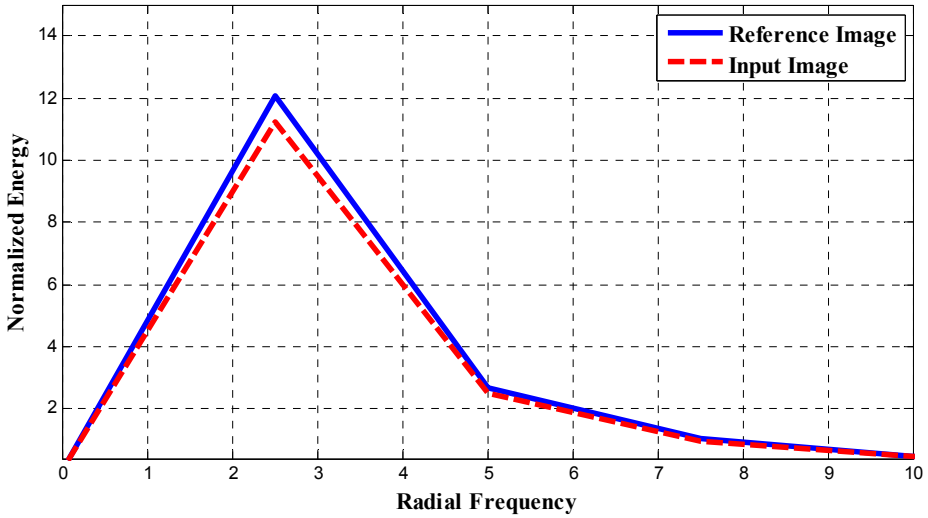

Figure 10: Plot of normalized energy vs. radial frequency for replay-video attack

5.4 Input image in horizontal motion

Figure 11 shows four input image frames selected from a video sequence at different instants of time when the print image is in horizontal motion. After determining the band selective energy contents of both types of image frames, it is seen that they have almost equal circular band energy. Figure 12 clearly depicts liveness of the reference image [Fig.7 (a)] as its maximum average energy value is higher than that of the input image which occurs at the radial frequencies band between 2 and 3. From experimental results, sometimes it is difficult for the algorithm to differentiate between live and fake image sequence as they have almost equal circular band energy. In that situation, the algorithm has to perform additional tasks before reaching a decision.

Figure 11: Input print image frame sequences in for print image in horizontal motion

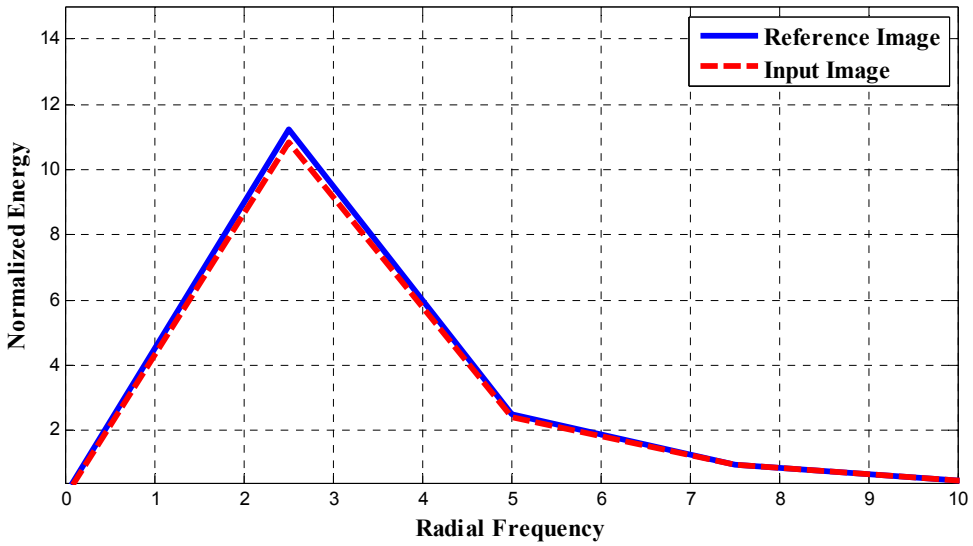

Figure 12: Plot of normalized energy vs. radial frequency for input image in horizontal motion

From experimental results, it is observed that for image sequences with normal illumination condition the method correctly identifies all input images and provides a perfect counter spoof attack function. For video replay attack and image sequences with low illumination condition, it gives correct identification rate of 95.23% and 95.56%, respectively which is better than that of the existing methods. In case of image sequences with horizontal motion, the correct identification rate becomes 88.88%, which is the lowest of all categories considered. This is due to the poor face recognition performed by FJTC. If we consider only the second phase, i.e. liveness detection part of the proposed method, the accuracy of liveness detection of all types of image sequences will be higher. On an average, the accuracy of the proposed method for liveness detection for preventing spoof attack is 95.88%. By reducing alignment error, maintaining correct distance between subjects and camera during experimental tasks, the performance and accuracy of the proposed method can be further improved. Further, different frame size of the image needs different threshold value of discrimination ratio in the face recognition phase and value of cut off frequency in band pass filter in liveness detection phase. As a result, liveness detection may occur at different radial frequency band rather than of the presently discussed frame size.

6. CONCLUSION AND FUTURE WORK

An efficient live face detection method is proposed in this paper to counter spoof attack in face recognition systems. In this research work, we developed our own face database because for this type of research, publicly available datasets are not available. This method exploits power spectra of the image sequences in different ways. It incorporates the task of face recognition as well, which is a new dimension compared to other liveness detection methods. Due to the incorporation of face recognition task, theoretical efficiency of the proposed method drops to 95.88% which is also very encouraging

performance. Test results obtained using real life datasets confirm that the proposed technique successfully counters spoof attacks. For future work, the proposed algorithm has to be tested with an efficient and widely accepted publicly available database. Further, the proposed method can also be tested with a 3D fake face or a sculpture which has more 3D depth information. Dynamic selection of the cut off frequency of the band pass filter for various types and sizes of images can also be a good future research topic.

REFERENCES

1. S. Chakraborty and D. Das, "An overview of face liveness detection," *International Journal on Information Theory,* Vol. 3, No.2, 2014.
2. E. Hjelmas, B. K. Low, "Face detection: A survey," *Computer Vision and Image Understanding,* Vol. 83**,** pp.236–274, 2001.
3. P. Viola and M. Jones, "Rapid object detection using boosted cascade of simple features," *Proceedings of IEEE computer society, on Computer vision and Pattern recognition,* Vol. 1, pp. 511-518, 2001.
4. M. Turk and A. Pentland, "Eigen faces for recognition," *Journal of Cognitive Neuroscience,* Vol. 3, pp. 71-86, 1991.
5. L. Meng and T. Nguyen, "Two subspace methods to discriminate faces and clutters," *Proceedings of the International Conference on Image Processing,* pp. TA07.03, 2000.
6. R. L. Hsu, M. Abdel-Mottaleb, and A.K. Jain, "Face detection in color images," *IEEE Transaction on Pattern Analysis and Machine Intelligence,* Vol. 24(5), pp. 696-706, 2002.
7. E. Saber and A. M. Tekalp, "Frontal-view face detection and facial feature extraction using color, shape and symmetry based cost functions," *Pattern Recognition Letters,* Vol. 19(8), pp. 669-680, 1998
8. M. J. Jones and J. M. Rehg, "Statistical color models with application to skin detection," *International Journal of Computer Vision,* Vol. 46(1), pp. 81-96, 2002.
9. C. Chen and S.P. Chiang, "Detection of human faces in color images," *IEEE Proceedings of Vision Image Signal Processing, Vol. 144, pp. 384-388, 1997.*
10. C.H. Lee, J.S. Kim and K. H. Park, "Automatic human face location in a complex background," *Pattern Recognition,* Vol. 29, pp. 1877-1889, 1996.
11. R. Jafri and H. R. Arabnia, "A survey of face recognition techniques," *Journal of Information Processing Systems*, Vol. 5, pp. 41-68, 2009.
12. B. Heisele, P. Ho, J. Wu and T. Poggio, "Face recognition: component-based versus global approaches," *Computer Vision and Image Understanding*, Vol. 91, pp. 6-21, 2003.
13. W. Zhao, R. Chellappa, P.J. Phillips and A. Rosenfeld, "Face Recognition: A Literature Survey," *ACM Computing Surveys,* Vol. 35, pp. 399-458, 2003.
14. M. S. Alam and M. A. Karim, "Fringe-adjusted joint transform correlation," Applied Optics, Vol. 32, pp. 4344-4350, 1993.
15. M. S. Alam, and M. M. Rahman, "Class-associative multiple target detection by use of fringe-adjusted joint transform correlation," *Applied Optics*, Vol. 41, pp. 7456-7463, 2002.
16. 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, pp. 235-238, 2006.
17. L. Wang, X. Ding, C. Fang, "Face live detection method based on physiological motion analysis," *Tsinghua Science and Technology,* Vol. 14, pp. 685-690., 2009.
18. C. Kant, and N. Sharma, " Fake face detection based on skin elasticity," *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 3, pp. 1048-1051, 2013.
19. B. G. Nalinakshi, S. M. Hatture, M. S.Gabasavalgi, R. P. Karchi, "Liveness detection technique for prevention of spoof attack in face recognition system," *International Journal of Emerging Technology and Advanced Engineering*, Vol. 3, pp. 1048-1051, 2013.
20. A. Lagorio, M. Tistarelli, M. Cadoni, "Liveness detection based on 3D face shape analysis," *International Workshop on Biometrics and Forensics* (IWBF), pp. 1-4, 2013.
21. D. A. Socolinsky, A. Selinger, and J. D. Neuheisel, "Face recognition with visible and thermal infrared imagery," *Computer Vision and Image Understanding,* Vol. 91, pp. 72-114, 2003.
22. X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," *Computer Vision- ECCV, ISBN: 978-3-642-15566-6*, Vol. 6316, pp. 504-517, 2010.

23. J. Maatta, A. Hadid, and M. Pietikainen, "Face spoofing detection from single images using micro-texture analysis," *IEEE International Joint Conference on Biometric Compendium,* pp. 1-7, 2011.
24. I. Chingovska, A. Anjos, and S. Marcel, "On the fffectiveness of local binary patterns in face anti-spoofing," *Proceedings of the International Conference Biometrics Special Interest Group,* ISBN: 978-1-4673-1010-9, pp. 1-7, 2012.
25. G. Pan, Z. Wu, and L. Sun, "Liveness detection for face recognition," *Recent Advances in Face Recognition,* KresimirDelac, MislavGrgic and Marian Stewart Barlett (Editors),ISBN: 978-953-7619-34-3, InTech, pp. 109-124, 2008.
26. R.T. Tan and K. Ikeuchi, "Separating reflection components for textured surfaces using a single image,"*IEEE Transactions on Pattern Analysis and Machine Intelligence,* 27:178-193, 2005.
27. J. Li, Y. Wang, T. Tan, and A. Jain, "Live face detection based on the analysis of Fourier spectra," *SPIE Biometric Technology for Human Identification*, Vol. 5404, pp. 296-303, 2004.