VOL. 11, NO. 13, JULY 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

VIDEO BASED FACIAL SPOOF ATTACKS DETECTION USING LOCAL BINARY PATTERN

Jeba J., Naga Visaradha Nalam and G. I. Shamini
Department of Electronics and Communication Engineering, Sathyabama University, Jeppiar Nagar, Rajiv Gandhi Salai, Chennai, India
E-Mail: jebajsk@gmail.com

ABSTRACT

The identification of video source is very important for video validation evidence, tracking down video piracy crimes and regulating individual video sources. User authentication is an important step to protect information and in this context, face biometrics has more advantage. Face biometrics are natural, intuitive, easy to use and less human invasive. Unfortunately, recent work has face biometrics vulnerable to spoofing attacks using cheap low-tech equipment. We have introduced a method for face spoofing detection using spatiotemporal (dynamic texture) extensions of highly popular local binary pattern operator. With wide deployment, face recognition systems has been used in applications from border control to mobile device unlocking and laptop device unlocking. The combat of video spoofing attacks requires increased attention. We address the problem of video spoofing detection against replay attacks by using the aliasing analysis in spoofed face videos. We analyse the texture pattern aliasing that commonly appears during recapture of video or photo replays on screen in different channels (R, G, B and grayscale) and regions. Multi-scale LBP and SIFT features determines the texture patterns characteristics which differentiate a replayed spoof face from a live video (face present). We have introduced effective approach in face spoof detection both cross-database, and intra-database testing scenarios(video) and shows better comparison since we compare the edge pixel values and depth of pixel values of the authenticated person with the image stored in the database.

Keywords: user authentication, video spoofing, GLCM, Multi-scale LBP, RADON, SIFT.

1. INTRODUCTION

Using various physiological characteristics of individuals humans distinguish each other. Identity verification occurs when user's information is to be already enrolled in system and presents an ID card or login name. In this case verification bio- metric data received from user is compared to user's data already stored in database. Identification (also known search) occurs when the identity of user is a priori unknown. In this case user's biometric data is matched against all records in database that can be anywhere in database. The user authentication requires the use of either passwords and user IDs or identification cards and PINs, which suffer from several limitations. Things like keys or cards can get stolen or misplaced, and by direct covert observation passwords and PINSs can be acquired. Once an intruder obtains user ID and the password, intruder has full access to user's resources. To achieve more reliable verification or identification we have to work on distinguishable features that characterize the person.

With the advancement of large-scale computer networks and extending applications of such networks, true authentication on bio-metrics has received more attention. Nowadays, we desire systems that deliver power to authenticate persons accurately, reliably, in a user-friendly manner without invading privacy issues. Behavioural features such as fingerprints, iris, hand geometry, signatures, video and voice recognition can be used for automated identity verification by many biometric technologies as shown in Figure-1. The characteristics shown can be measured and also unique. There is no possibility of losing or forgetting bio-metrics, as they are the most important and unique characteristics of each person, and this made an advantage over keys, passwords or codes. As a result the reliability of user authentication system increases. In commercial applications like as electronic data security, computer, mobile phones etc. Biometrics is used as primary source of authentication. Many multi-national companies have used swift way for the employee's authentication. Bio-metric technologies finds its application even in police departments and secret agencies all over the globe to identify the criminals based on evidences like; DNA, face and video verification obtained from the crime scenes, video footage and fingerprints. Electronic passport has two fingerprints in addition to a passport photograph and hence commonly used. Moreover, it speeds up border crossing through the use of scanners, which principle of recognition by comparison of the face or fingerprints. The same applies to visa applications and renewals.

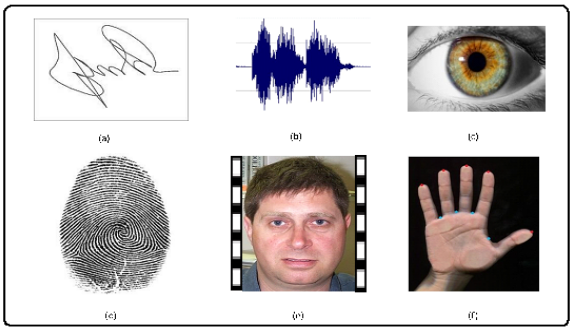


Figure-1. Sample bio-metrics: (a) signature, (b) voice recognition, (c) iris, (d) fingerprint, (e) video based facial attack, (f)hand geometry.

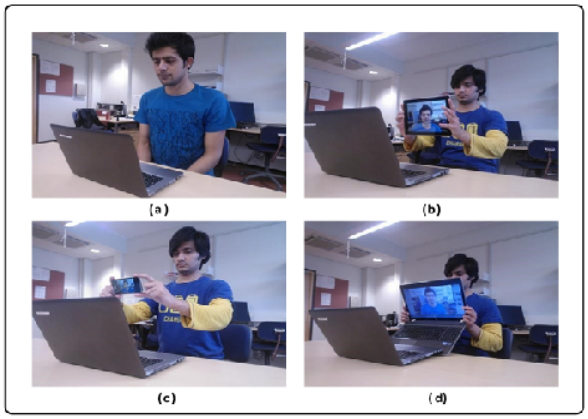


Figure-2. Sample biometric attacks (a) real, (b) video attack (c) mobile attacks,(d) laptop attack.

2. RELATED WORK

The user authentication is the basic requirement in any security system. To design such systems efforts have been made by most of the researchers. The literatures available for these are summarized below; [1] Introduced a spatio-temporal method to detect video-based face spoofing by analysing noise signatures generated by the video acquisition process which can be used to distinguish between valid and fake access videos. Noise properties are captured using Fourier spectrum for each frame of the video. A compact representation, called visual rhythm, is employed to detect temporal information in the Fourier spectrum. To form the visual rhythms, three different video traversal strategies were considered, of which horizontal and vertical combined was shown to be the most effective. Features were extracted from the visual rhythms through GLCM, LBP and HOG descriptors to allow a proper distinction between fake and real biometric data. [2] Proposed a remedy for by-passing 2-D face recognition systems with the usage of photographs of spoofed identities.[3]This paper uses general image quality features extracted from an image to differentiate between constructed and legitimate samples. It not only determines the multi attack but also the multi biometric.[4] introduced REPLAY ATTACK spoofing attack database comprising of three types of all the possible attacks by using two different recording conditions andthree different media. [5] presents a framework for spoofing detection using motion magnification. It proposes that motion magnification will improve the performance and configuration of LBP features. It further proposes a technique using optical flow descriptor (HOOF). It provides performance on the Print Attack and Replay Attack databases on accuracy and computational efficiency. [6] Introduced a robust method for face live detection which provides high security for mobile devices. It mainly models the differences in the illumination characteristics of live and fake faces by diffusion method. [7] Proposed an algorithm that considers noise added to the biometric samples when manufactured. This method uses as low-level descriptors. [8] Present video face verifications algorithms based on BNCA database. It is mainly divided into the following categories: part based versus holistic approach and frame-based image-set approach. It shows the importance of images based on their quality. [9] Proposed a method on 3D mask attacks. It evaluates spoofing performances on 2.5D and 3D systems by analysing each mask separately with LOOCV. [10] Introduced a method for several types of scenic fake face attacks from the study of fusion of motion and texture based counter measures.

3. METHODOLOGY USED

The main algorithm used here is Local binary pattern and Radon Transform to characterize whether the input video given to the camera is real or not.

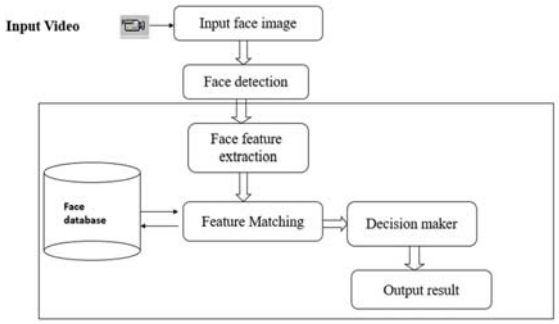


Figure-3. Algorithm flow of simplified block diagram.

3.1 Face detection

The localization of the face in an image is the main aim of face detection. For any video input, we must track the face in between the multiple frames of the video, to reduce computational time and the identity of a face of the person between frames must be preserved. Methods for face detection includes: Active appearance mode (AAM) and Shape templates.

3.2 Face preprocessing

The main aim of the face pre-processing step is to normalize the face detection in order to obtain robust feature extraction. Depending on the application, face pre-processing includes: light normalization/correlation and Alignment (translation, scaling, rotation).

3.3 Feature extraction

Extraction of a compact set of interpersonal differentiating geometrical and photometrical features of the face is the main aim of feature extraction. Methods for feature extraction includes: GLCM, SIFT, Radon Transform.

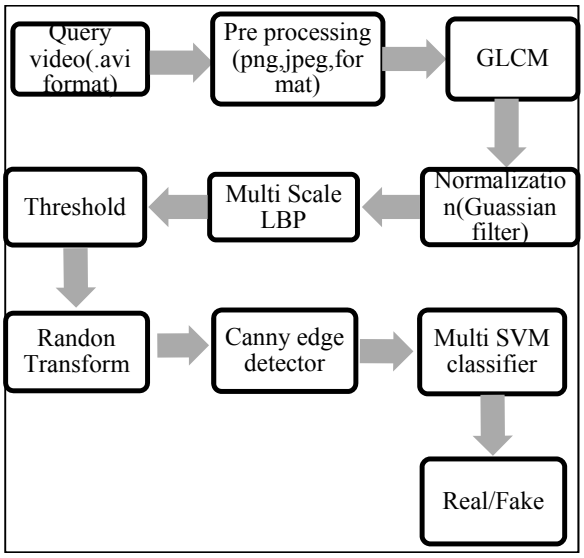


Figure-4. Detailed block diagram for the methodology used to determine the Feature Extraction.

3.4 Gray level co-occurrence matrix (GLCM)

The use of co-occurrence probabilities (GLCM) is used to extract various features of texture obtained estimating image properties obtaining many combinations of gray levels in an image. Each entry (i, j) is the number of occurrences of each pair of gray levels i and j which are separated by distance d in original image. Suppose an image has$N_x$columns, N_y rows and N_g is the quantised gray level appearing at each pixel. Let the columns and rows be $L_x = \{1, 2,..N_x\}$and $L_y=\{1,2,..N_y\}$ respectively and $G_x=\{0,1,2,..N_{g-1}\}$ be the set of quantized gray levels. The set $L_x \times L_y$ gives the set of pixels of the ordered image by row column indices. We used twenty three textural features in our study. Let $p(i, j)$ be the (i, j)th entry of the normalized GLCM. The mean and standard deviation for all the given rows and columns of the matrix are

$$\mu_x = \sum_i \sum_j i.\, p(i,j)\,, \mu_y = \sum_i \sum_j j.\, p(i,j)$$

$$\sigma_x = \sum_i \sum_j (i-\mu_x)^2.\, p(i,j),\ \sigma_y = \sum_i \sum_j (i-\mu_y)^2.\, p(i,j)$$

Some of the basic GLCM features are described below.

3.4.1 Energy

Angular second moment commonly known as Energy gives uniformity in texture of an image. When distribution of gray level has a constant or a periodic form, the energy reaches its highest value. If the p matrix contains many small entries, the energy feature has smaller value and vice versa.

$$f_1 = \sum_i \sum_j p(i,j)^2$$

3.4.2 Contrast

Contrast determines the difference value of the highest and the lowest measure of a set of pixels to find the amount of local variation.

$$f_2 = \sum_{n=0}^{N_g-1} n^2 \left\{ \sum_{i=1}^{N_g} \sum_{j=1}^{N_g} p(i,j) \right\}$$

3.4.3 Maximum probability

$$f_3 = \max_{i,j} p(i,j)$$

3.4.4 Correlation

The Correlation is the measure of linear dependencies of gray tone in an image at a specified position relative to each other.

$$f_4 = \frac{\sum_i \sum_j (ij) p(i,j) - \mu_x \mu_y}{\sigma_x \sigma_y}$$

3.4.5 Homogeneity

The image homogeneity is measured since it assumes larger values for smaller gray tone differences in paired elements. This GLCM statistic is also called as Inverse Difference Moment.

$$f_5 = \sum_i \sum_j \frac{1}{1+(i-j)^2}\, p(i,j)$$

3.4.6 Entropy

Entropy measure the disorderness of an image. When all theelements P matrix are equal, then entropy value is the highest. When the image is not uniform texturally, many of the GLCM elements have a very small value implying that entropy is very large.

$$f_6 = \sum_i \sum_j p(i,j) \log(p(i,j))$$

3.4.7 Autocorrelation

$$f_7 = \sum_i \sum_j (i,j) p(i,j)$$

3.4.8 Cluster prominence

$$f_8 = \sum_i \sum_j (i+j-\mu_x-\mu_y)^4 p(i,j)$$

3.4.9 Sum average

$$f_9 = \sum_{i=2}^{2N_g} i.\, p_{x+y}(i)$$

3.4.10 Dissimilarity

$$f_{10} = \sum_i \sum_j |i-j|.\, p(i,j)$$

3.4.11 Sum variance

$$f_{11} = \sum_{i=2}^{2N_g} (i-f_{13})^2.\, p_{x+y}(i)$$

3.4.12 Cluster shade

$$f_{12} = \sum_i \sum_j (i + j - \mu_x - \mu_y)^3 p(i,j)$$

3.4.13 Sum entropy

$$f_{13} = \sum_{i=2}^{2N_g} p_{x+y}(i) \log\{p_{x+y}(i)\}$$

3.5 Local binary pattern

Local Binary Patterns (LBP) which has been proved to be robust against illumination variations and effective for capturing the hidden textural information of an image. Since the development of LBP, its many variants have been proposed in the literature such as Rotation invariant-LBP, Extended-LBP, Improved LBP, MB-LBP etc.The functionality of the operator is a local neighbourhood that is obtained by thresholding the gray value present in the centre pixel transforming it to a binary pattern that is determined by the LBP. The basic LBP operates on a 3x3 kernel to encode the local spatial structure of image by comparing pixel intensity of the centre pixel with its eight neighbours. The pixels in this block are then thresholded by obtaining the product of centre pixel value and the powers of two and then added to get a label for the centre pixel. Since the neighbourhood consists of 8 pixels, a total of $2^8 = 256$ different labels is obtained based on the relative gray values of the centre pixel and the neighbourhood pixels. An example of an LBP image is shown in Figure

$$\mathrm{LBP}_{P,R} = \sum_{p=0}^{P-1} s(g_p - g_c) 2^p$$

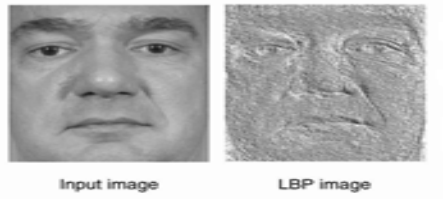


Figure-5. Example of LBP image.

Where g_c and g_p denote the gray values of the central pixel and its neighbour, respectively, and P is the index of the neighbour. P is the number of the neighbours, and R is the radius of the circularly neighbouring set. Supposing that the coordinate g_c of is (0,0), the coordinate of each neighbouring pixel $g_c$is then determined according to its index p and parameter (P, R) as $(R\cos(2\pi p/P)),(R\sin(2\pi p/P))$. Three circularly symmetric neighbouring sets with different (P, R)

Corresponds to the spatial transitions (bitwise 0/1 changes) number in the pattern. Based on the uniformity measure, the LBP descriptions of a texture image are defined as follows

$$\mathrm{LBP}^{riu2}_{P,R} = \begin{cases} \sum_{p=0}^{P-1} s(g_p - g_c), & \text{if } U(\mathrm{LBP}_{P,R}) \le 2 \\ P+1 & \text{otherwise} \end{cases}$$

LBPs with the U till 2 are defined as the uniform patterns labelling corresponds to the number of "1" bit in the pattern. $(P + 1)$.

3.6 Radon transform

Generally an image is denoted as a function of two spatial variables f(x,y). The value of function determines intensity of the image at the point (x,y),thus representing the spatial domain. The Radon transform is commonly a function of Rho and θ which are calculated for each matching points calculated whereas in Hough Transform, Rho and θ are calculated for every pixel value.

The radon transform of an image is given by the sum of radon transform of each pixel of the image. The projection of an image matrix along particular direction is performed by radon transform and it also computes the line integrals from multiple sources or beams in a certain direction or along parallel paths.The spacing of the beams is one pixel unit apart. The radon function takes several parallel-beam paths of the image from different angles by moving the source around the centre of the image. The skew angle is calculated depending upon the maximum value of radon function.

$$R\theta(x') = \int_{-\infty}^{+\infty} f(x'\cos\theta - y' sin\theta, x' sin\theta + y' cos\theta)\, dy'$$

3.7 Classification techniques

Choosing of the most suitable category from the given set of known classes, for an unknown object, is the main aim of classification. Since perfect classification has been often impossible, the classification may also be done by specifying the probability for each of the known categories.

3.8 Support vector machines

Support vector machines (SVMs) proposed by Boser have been successfully used in many learning problems. When applied to classification, the desired optimal separating hyper plane between two classes, is found by using SVM, especially in a higher dimensional space. The aim of SVMs is to decide the parameters of a mapping function that can map all the training samples to some real valued functions which separates them efficiently. "Divide and conquer" algorithm is commonly used technique to determine multiclass problem in which a single multiclass problem is divided into binary pairs and then a SVM is trained for each pair.

4. EXPERIMENTAL RESULTS

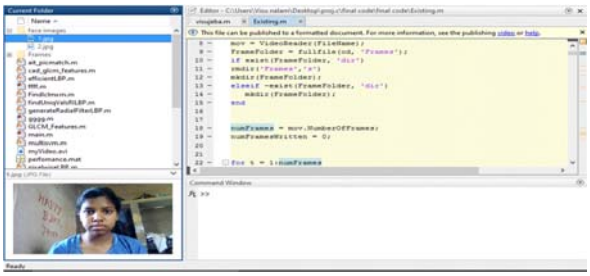


Figure-6. Image stored in the database.

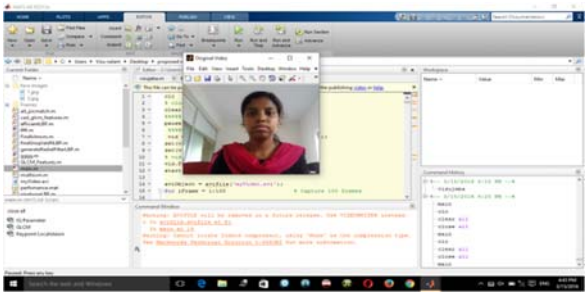
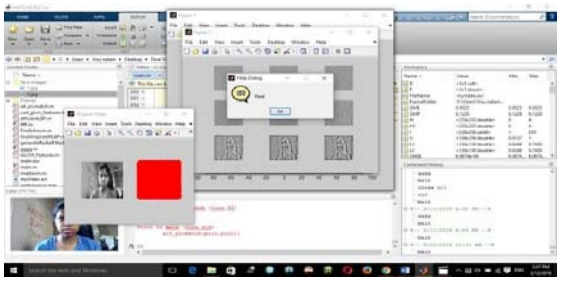


Figure-7. The input video is taken in .avi format.



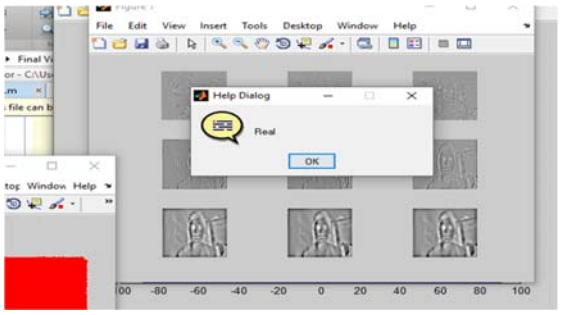


Figure-8. The edge pixels and the pixel depth are calculated and compared with the database image values, hence matching occurs.

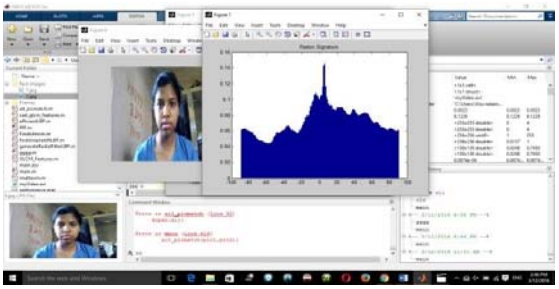


Figure-9. The Radon signature graph is plotted to determine the intensity of image for different orientations.

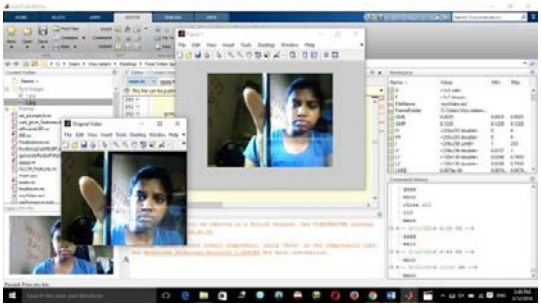
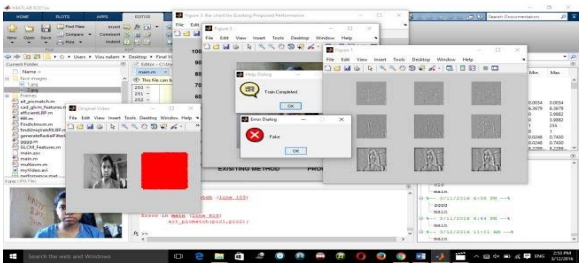


Figure-10. The input video is given from mobile phone.



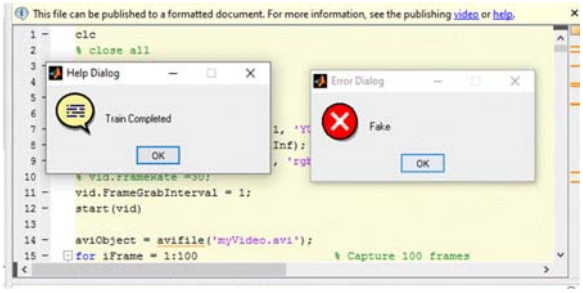


Figure-11. The edge pixels and the pixel depth are calculated and compared with the database image values hence mismatching occurs in this case.

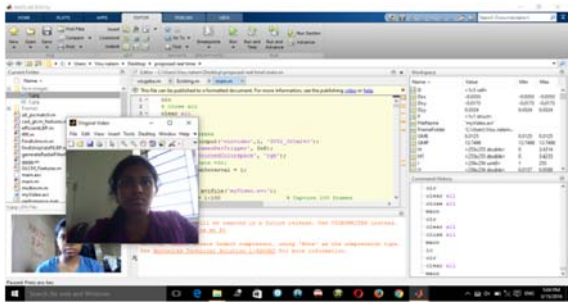


Figure-12. The video of unauthorised person whose image not in database is taken.

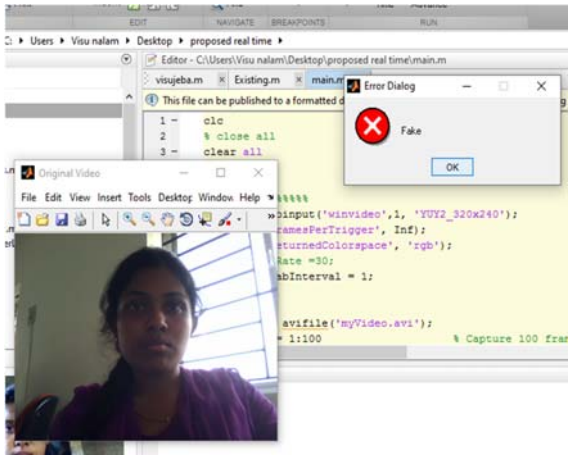


Figure-13. The edge pixels and the pixel depth are calculated and compared with the database image values hence mismatching occurs in this case also.

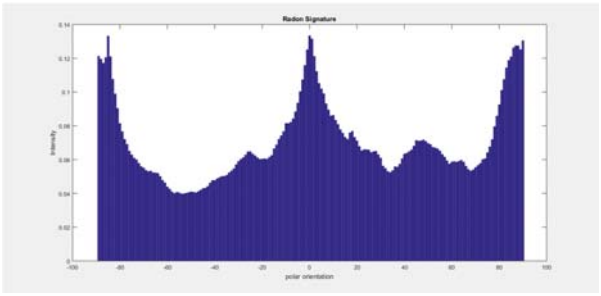


Figure-14. Radon Signature for real video.

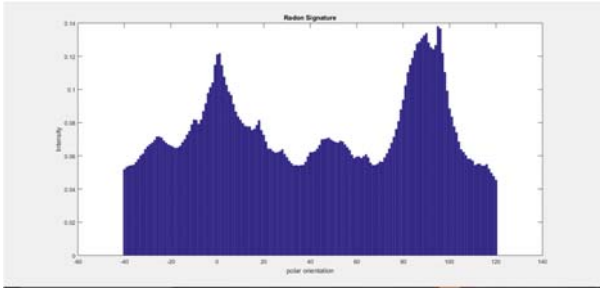


Figure-15. Radon Signature for fake video.

5. CONCLUSIONS

Video is generally used for authentication purpose nowadays. In this paper we have introduced a noble method to detect video spoofing using spatio-temporal extensions of highly popular Local Binary Pattern, SIFT features and also the usage of Radon transform to project the intensity of the appropriate image in 2D form. This method finds its application in laptop and mobile security and in surveillance camera.

REFERENCES

[1] Allan Pinto, William Robson Schwartz, HelioPedrini, and Anderson de Rezende Rocha. 2005. Using Visual Rhythms for Detecting Video-Based Facial Spoof Attacks. IEEE Transactions on Information Forensics and Security. 10(5).

[2] Andre Anjos and Sebastien Marcel. 2011. Counter-measures to photo attacks in face recognition: a public database and a baseline. In: Proceedings of IAPR IEEE International Joint Conference on Biometrics (IJCB), Washington DC, USA.

[3] Javier Galbally, Sebastien Marcel and Julian Fierrez. 2014. Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition. IEEE Transactions on Image Processing. 23(2).

[4] Ivana Chingovska, Andre Anjos and Sebastien Marcel Idiap, Suisse. 2012. On the Effectiveness of Local Binary Patterns in Face Anti-spoofing. IEEE Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG), ISSN-1617 5468.

[5] Samarth Bharadwaj, TejasI. Dhamecha, MayankVatsa and Richa Singh IIIT-Delhi, India. 2013. Computationally Efficient Face Spoofing Detection with Motion Magnification. IEEE Conference of computer Vision and Pattern Recognition Workshops (CVPRW), INSPEC Number-13767008.

[6] Wonjun Kim, Member, IEEE, Sungjoo Suh, Member, IEEE and Jae-Joon Han, Member, IEEE. 2015. Face Liveness Detection From a Single Image via Diffusion Speed Model. IEEE Transactions on Image Processing. 24(8).

[7] Allan Pinto, Student Member, IEEE, HelioPedrini, Senior Member, IEEE, William Robson Schwartz, Member, IEEE and Anderson Rocha, Senior Member, IEEE. 2015. Face Spoofing Detection Through Visual

Codebooks of Spectral Temporal Cubes. IEEE Transactions on Image Processing. 24(12).

[8] Norman Poh, Chi Ho Chan, Josef Kittler, Sébastien Marcel, Christopher Mc Cool, Enrique ArgonesRúa, José Luis AlbaCastro, Mauricio Villegas, Roberto Paredes, VitomirStruc, Nikola Pavesic, Albert Ali Salah, Hui Fang and Nicholas Costen. 2010. An Evaluation of Video-to-Video Face Verification. IEEE Transactions on Information Forensics and Security. 5(4).

[9] Nesli Erdogmus and Sebastien Marcel. 2014. Spoofing Face Recognition with 3D Masks. IEEE Transactions on Information Forensics and Security. 9(7).

[10] Jukka Komulainen, Abdenour Hadid, Matt Pietikainen. 2013. Complementary Counter measures for Detecting Scenic Face Spoofing Attacks. IEEE International Conference on Bio-metrics (ICB), INSPEC-13826755.

[11] A. K. Jain, P. Flynn, and A. A. Ross, Eds. 2008. Introduction to biometrics. In Handbook of Biometrics. New York, NY, USA: Springer-Verlag. pp. 1-22.

[12] I. R. Buhan and P. H. Hartel. 2005. The state of the art in abuse of biometrics. Centre Telematics Inf. Technol., Univ. Twente, Enschede, the Netherlands, Tech. Rep. TR-CTIT-05-41.

[13] X. Tan, Y. Li, J. Liu, and L. Jiang. 2010. Face liveness detection from a single image with sparse low rank bilinear discriminative model. In: Proc. 11thEur. Conf. Comput. Vis. pp. 504-517.

[14] J. Määttä, A. Hadid and M. Pietikäinen. 2011. Face spoofing detection from single images using micro-texture analysis. In: Proc. Int. Joint Conf. Biometrics. pp. 1-7.

[15] W. R. Schwartz, A. Rocha, and H. Pedrini. 2011. Face spoofing detection through partial least squares and low-level descriptors. In: Proc. Int. Joint Conf. Biometrics. pp. 1-8.

[16] G. Pan, L. Sun, Z. Wu, and S. Lao. 2007. Eyeblink-based anti-spoofing in face recognition from a generic webcamera. In: Proc. IEEE 11th Int. Conf. Comput. Vis. pp. 1-8.

[17] T. Ojala, M. Pietikäinen, T. Mäenpää. 2002. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. IEEE Transactions on Pattern Analysis and Machine Intelligence. Vol. 24.