3D Anti Face Spoofing Coupled With Face Recognition Through A Parallel Approach

Submiited as part of CSE507 Advanced Computer architecture Final Report

To

Dr M Rajasekhara Babu

By

Team Members:

15MCS0066 GOUTAM GHOSH,

15MCS0082 WALKE AMEY SHYAM,

15MCS0098 SHASHIKANT DEWANGAN

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING

VIT UNIVERSITY
(Estd. u/s 3 of UGC Act 1956)
VELLORE ▪ CHENNAI
www.vit.ac.in

***Abstract*- Biometric authentication is most important part in security system. Universally used Biometric fingerprint scanner can be bypassed quite easily. Biometric face recognition has been introduced to improve the security of a system. Methods such as Motion based and texture based are used for biometric face recognition. But these methods have less robust, poor generalization ability and high computational complexity. This paper presents a new approach for spoofing detection in face videos using motion magnification. A 3D method is used for checking the liveliness of image to increase accuracy and reliability of the system. In addition, the texture features that are used for spoofing detection time can be improved through a parallel approach. The implementation of this method can be achieved by Parallel MATLAB, stands for Matrix Laboratory, and is a parallel computing platform which uses multicore processor. This provides a unique feature space for coupling spoofing detection and face recognition.**

Index Terms: Biometric (access control), Three dimensional anti spoofing, Three dimensional face recognition, Local binary patterns (LBP), Image processing, Motion based method, Texture based method, Improved Time Complexity

1.INTRODUCTION:

Face acknowledgment frameworks, notwithstanding, depend on level pictures in request to identify individuals, with the goal that they can be effectively ridiculed by printed photos and versatile presentations. A few face parodying recognition techniques have been proposed[1]. A portion of the methodologies incorporate picture quality examination, movement investigation, surface examination, or a blend of these. Among the picture quality methodologies, Li et. al. characterize a high-recurrence descriptor and a lower edge to separate standard and face-satirizing picture.Identify printed and showed face-using so as to satirize pictures a bolster vector machine (SVM) to look for an absence of high-recurrence data.Tan. et. al. scan for unrealistic enlightenment changes and for low picture quality in the recognized face picture[2]-[19]. Peixoto et. al. likewise hunt down low picture quality, additionally adjust data pictures subject to terrible enlightenment conditions, in light of differentiation restricted versatile histogram adjustment. Galbally et. al. hunt down low picture quality utilizing 25 general picture quality components separated from one picture, for example, top sign to-commotion proportion furthermore, the basic likeness reco. cell telephones, [4]like unique mark validation (Touch ID) in the iOS framework. Dissimilar to unique mark validation, face acknowledgment does not require any extra sensor since all advanced mobile phones come outfitted with a front confronting camera. On the other hand, like other biometric modalities we need to address worries about face parody assaults on face acknowledgment frameworks, [5] especially in unconstrained detecting and uncooperative subject situations [6]. It is generally simpler to procure a man's face picture or video (e.g., with an advanced camera or from online networking) than it is to procure other biometric attributes, for example, unique finger impression, palm print, and iris. Further, the expense of propelling a face parody assault, for example, a printed photograph, showed photograph, or replayed video is generally low. Best in class Commercial Off-The-Shelf (COTS) face acknowledgment frameworks are most certainly not all around intended to separate farce faces from veritable live faces[1]. demonstrates the face recognizable proof execution of a COTS face acknowledgment framework (COTS11) when parody faces as test are coordinated to honest to goodness faces in the exhibition. In this trial, more than 70% of test recordings (satire appearances) were effectively coordinated to the exhibition mates by COTS1 at rank-1,showing that COTS1 can't viably recognize honest to goodness and parody faces. In this paper we don't address 3D face veil assaults, which are more costly to launch.2

Rather,[2],[3] we concentrate on printed photograph and replayed video assaults. The delicacy of face acknowledgment frameworks to face parody assaults has propelled various studies on face parody identification In any case, distributed studies are constrained in their extension in light of the fact that the preparation and testing pictures (recordings) utilized were caught under the same imaging conditions[4],[7]-[12] It is fundamental to create powerful and proficient face parody recognition (on the other hand against parodying) calculations that sum up well to new imaging conditions and situations. In this paper, we consider the cross-database face parody discovery issue and propose a face parody discovery methodology in view of Image Distortion Investigation (IDA).

i) A face parody discovery calculation taking into account IDA, which is compelling in getting a handle on the characteristic bends of farce face pictures as for the honest to goodness face pictures.
ii) We build a face parody database, named the MSU Portable Face Spoof Database (MSU MFSD), utilizing the cameras of a portable workstation (MacBook Air3) and a cell telephone (Google Nexus 54) and three sorts of assault medium (iPad, iPhone, and printed photograph). The MSU MFSD database permits us to assess the speculation capacity of face farce location calculations crosswise over diverse cameras also, light conditions with cell phones. For a subset of the MSU MFSD database (35 subjects), we have the subjects' consent to make their information freely accessible.
iii) We present results for both intra-database and cross-database situations utilizing two open space face parody databases (Idiap REPLAY-ATTACK and CASIA FASD), and our own particular database (MSU MFSD).

2.Related Work:

Face acknowledgment frameworks can be effortlessly satirize by pictures of trusted clients on printed photos or on portable presentations. Be that as it may, as these caricaturing methods depend on computerized media, rather than the simple reality of the trusted client, the advanced framework of the face-acknowledgment framework camera covers with the network of the computerized media. On account of printed photos, the picture network of the camera covers with the printing halftoning specks, and on account of portable showcases, it covers with the pixel matrix. Figure 1 demonstrates to a standout amongst the most widely recognized antiquities of this kind: Moiré designs [21]–[24]. Figure 1(a) demonstrates a segment of test picture Lena, and Fig. 1(b) is a photo of (a), caught from a 13-inch presentation of a Macbook Pro utilizing an iPhone 4 camera, with no pressure antiques. Figures 1(c) and (d) show subtle elements of Figs. 1(a) and (b), separately, outlining the examples that happen after a picture is recovered from a screen. Note that these examples are most certainly not present in the first picture in Fig. 1(c). The location of Moiré examples at the spatial space can be extremely intricate, since there is no from the earlier technique to recognize this sort of example from whatever other. In the recurrence area, be that as it may, the examination can be further improved. Figures 1(e) and (f) demonstrate the supreme estimations of the discrete Fourier changes (DFT) of Figs. 1(a) and (b), separately, after a logarithmic scaling for review purposes. Figure 1(f) demonstrates extremely unmistakable crests at mid and high frequencies. Such crests are because of the covering of pixel frameworks between the camera and the screen.

Moiré examples have been altogether concentrated on [22]–[24]. Keeping in mind the end goal to disentangle the investigation, let us take a gander at the one-dimensional case. Consider a constant space low-pass capacity f (t), which is to be inspected with period T_1,, rendering $f_s(nT_1)$.The Fourier changes of f (t) and $f_s(nT_1)$. are F(ω) and $F_s(\omega) = \sum_k F(\omega - 2\pi k / T_1)$., separately. Whenever $f_s(nT_1)$. is shown on screen, $f_s d(t)$ is rendered, which is comparable to the convolution of $f_s(nT_1)$. with a freight car capacity, or to the augmentation of $F_s(\omega)$ with a sink capacity. Figure 2 represents this on will fall out of the frequency range of the recaptured image. It is important to point out that prior to resampling, low-pass filtering may take place, due to motion blur, lens defocus, diffraction and pixel response, among others, reducing the strength of the spectral repetitions and of the Moiré patterns. The sampling interval T2 depends on two factors: thesize of the camera's pixels and the distance between the screen and the camera. As the distance from the camera to the screen increases, the sampling interval T2 increases proportionally, reducing the capture resolution. The relation between T1 and T2 indicates if Moiré patterns are bound to occur, but it turns out to be very hard to directly measure. The sampling interval ratio S R = T1/T2, however, can be approximated by the pixel ratio P R:

$$P\ R = N2/N1, \quad (1)$$

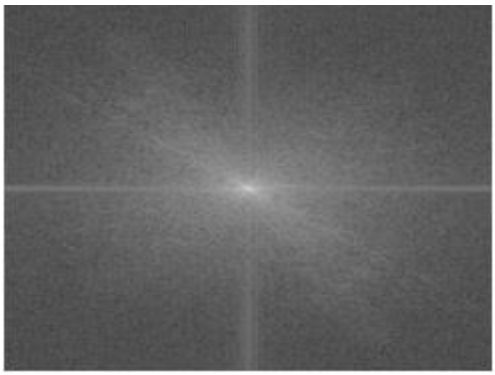
Where N1 and N2 represent the pixel lengths of a given feature on the screen and on the camera, respectively. As the distance from the camera to the screen increases, T2 also increases, decreasing S R. The pixel length N2 of the given feature on the camera will decrease proportionally, and so will P R. Since it is vital that T1 > T2 for the Moiré examples to develop, and accepting S R ≈ P R, it quickly takes after that: P R > 1. (2) Figure 3 shows the reliance of the catch determination on the separation from camera to screen Here, g is one of the n + 1 conceivable dim estimations of A(u, v) and p(g) is the likelihood of the dark level g. p(g) is approximated by the histogram of A(u, v). μ0(t) what's more, μ1(t) are the underneath or more limit means, such that μ0(t) = (t g=0 g p(g))/(t g=0 p(g)) and μ1(t) = (n g=t+1 g p(g))/(n g=t+1 p(g)) . In the event that there are crests on |F{IB P}| (the outright estimations of the DFT of any of the band-pass-separated variants of I), maximum correlation thresholding of this picture will underscore those tops, and not very many of its pixels will have a higher worth than the edge t. On the off chance that |F{IB P}| does not contain tops, a greater amount of its pixels will have a higher quality than t. In this way, the crest indicator calculation comprises in thresholding |F{IB P}| and tallying the rate p of pixels with a higher quality than the limit. where W is the picture's width and L its stature. In the event that p < pmin, I is viewed as a face-satirizing picture. The worth pmin is a basic rate of the entire picture, and it should be little when crests are available in |F{IB P}|. The calculation is rehashed for diverse estimations of σ , and on the off chance that no top is found for all band-pass forms of I, it is considered a non-face-mocking picture.

(a)

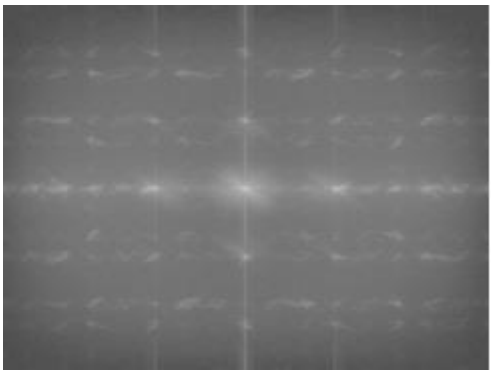
(b)

(c)

(d)



(e)



(f)

Figure 1. Moiré designs

3.Methodology:

3.1 Local Binary Pattern

The LBP administrator [11] is one of the best performing surface descriptors and it has been generally utilized as a part of different applications. It has turned out to be profoundly discriminative and its key favourable circumstances, specifically, its invariance to monotonic gray level changes and computational proficiency, make it suitable for requesting picture investigation assignments. The idea of using LBP for face description is motivated by the fact that faces can be seen as a composition of micro patterns which are well described by such operator. The LBP administrator was initially intended for texture portrayal. The administrator allocates a name to each pixel of a picture by thresholding the 3 x 3-neighborhood of every pixel with the center pixel esteem and considering the outcome as a binary number. At that point, the histogram of the names can be utilized as a texture descriptor. See Fig. 1 for an outline of the essential LBP administrator.

To have the capacity to manage textures at distinctive scales, the LBP administrator was later stretched out to utilize neighbourhoods of distinctive sizes [12]. Characterizing the nearby neighbourhood as an arrangement of sampling points equally divided on a circle focused at the pixel to be marked permits any range and number of sampling points. Bilinear interpolation is utilized when an sampling point does not fall in the focal point of a pixel. In the accompanying, the documentation ðP; Rþ will be utilized for pixel neighbourhoods which implies P sampling points on a circle of sweep of R. See Fig. 2 for a sample of roundabout neighbourhood.

Another expansion to the first administrator is the meaning of supposed uniform examples [12]. A local binary pattern is called uniform if the local binary pattern contains at most two bitwise moves from 0 to 1 or the other way around when the bit example is considered round. For instance, the examples 00000000 (0 moves), 01110000 (2 moves) and 11001111 (2 moves) are uniform while the examples 11001001 (4 moves) and 01010011 (6 moves) are most certainly not. In the calculation of the LBP histogram, uniform patterns are utilized so that the histogram has a separate container for each uniform patterns and every single non uniform patterns are appointed to a solitary container. Ojala et al. seen that in their explores different avenues regarding surface pictures, uniform patterns represent a bit under 90 percent of all examples when utilizing the (8,1) neighbourhood and for around 70 percent in the (16,2) neighbourhood. We have found that 90.6 percent of the patterns in the (8,1) neighbourhood .

.

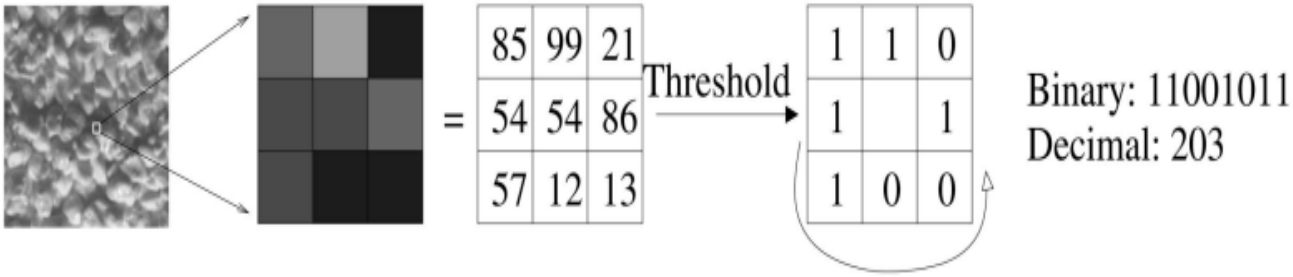


Figure 2. The basic LBP operator.

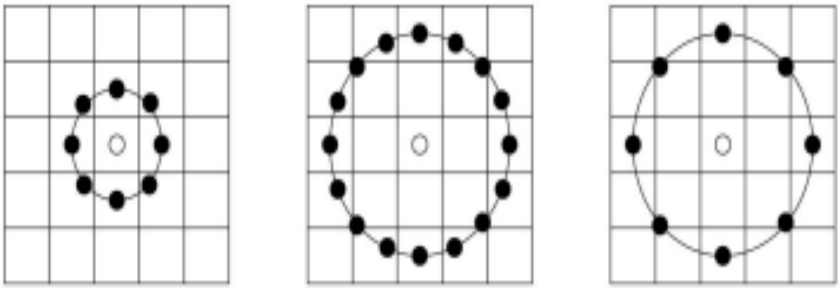


Figure 3. The circular (8,1), (16,2), and (8,2) neighbourhoods.

The pixel values are bilinear interpolated whenever the sampling point is not in the center of a pixel.

Figure 4. A facial image divided into 7 x 7, 5 x 5, and 3 x 3 rectangular regions.

3.2 Face Description with LBP:

In this work, the LBP technique displayed in the past segment is utilized for face depiction. The system comprises of utilizing the composition descriptor to assemble a few neighbourhood portrayals of the face and joining them into a worldwide depiction. These local feature-based and hybrid techniques appear to be stronger against varieties in posture or brightening than comprehensive strategies.

Another explanation behind selecting the nearby component based methodology is that attempting to fabricate a comprehensive depiction of a face utilizing surface systems is not sensible since surface descriptors tend to normal over the picture territory. This is an attractive property for normal surfaces, in light of the fact that composition portrayal ought to more often than not be invariant to interpretation or even turn of the surface and, particularly, for little dull surfaces, the little scale connections decide the presence of the composition and, consequently, the largescale relations don't contain helpful data. For countenances, on the other hand, the circumstance is distinctive: holding the data about spatial relations is vital.

This thinking prompts the fundamental procedure of this work. The facial picture is separated into neighbourhood locales and texture descriptors are extricated from every area freely. The descriptors are then connected to shape a worldwide depiction of the face. See Fig. 3 for a case of a facial picture partitioned into rectangular locales.

The fundamental histogram can be stretched out into a spatially upgraded histogram which encodes both the appearance and the spatial relations of facial locales. As the m facial regions R0; R1; . . . Rm1 have been resolved, a histogram is figured autonomously inside of each of the m locales. The subsequent m histograms are joined yielding the spatially improved histogram. The spatially upgraded histogram has size m n, where n is the length of a solitary LBP histogram. In the spatially upgraded histogram, we successfully have a depiction of the face on three distinct levels of territory: The LBP names for the histogram contain data about the examples on a pixel-level, the names are summed over a little district to produce data on a local level, and the local histograms are connected to construct a worldwide portrayal of the face It ought to be noticed that when utilizing the histogram-based techniques, notwithstanding the cases in Fig. 3, the districts R0; R1; . . . Rm don't should be rectangular. Neither do they should be of the same size or shape nor they don't as a matter of course need to cover the entire picture. For case, they could be roundabout locales situated at the fiducial focuses like in the EBGM system. It is likewise conceivable to have in part covering areas. On the off chance that acknowledgment of confronts pivoted top to bottom is thought of it as, may be helpful to take after the system of Heisele et al. [8] and naturally distinguish every locale in the picture rather than first recognizing the face and afterward utilizing a settled division into areas.

4.Working Example:

4.1 Working Example 1: An unauthorized user can create a three dimensional model of the authorized user to get the legitimate access of all the files, programs, personal mails, etc. In our Biometric Anti-face spoofing application we prevent this unauthorized access. We have built such a system which detects three dimensional fake models from getting the genuine access of the system. As our system check the liveliness of the object before the webcam.

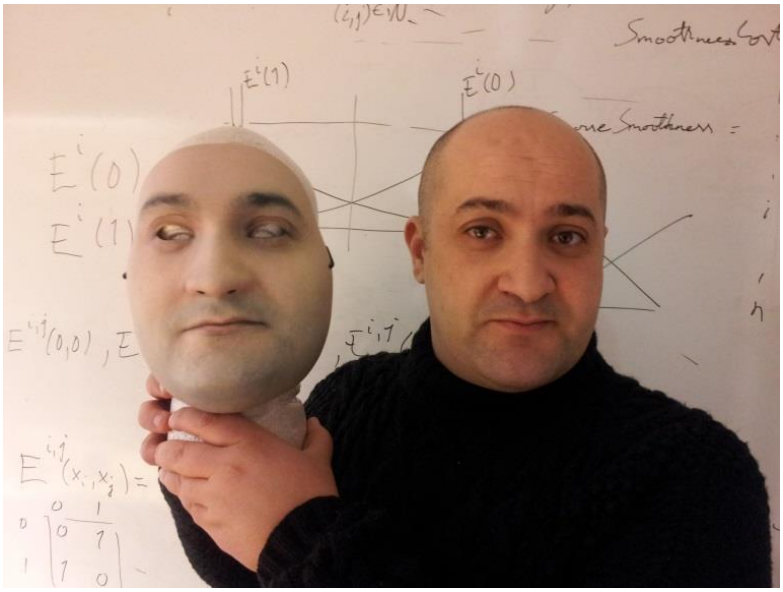


Figure 5. Working Example 1

4.2 Working Example 2: In here this person has taken the image of the authorized user. This unlicensed user uses this photograph to login the licensed users account. In such scenario, proposed system doesn't allow the access because our system checks the texture object. It prevents the spoofing.

Figure 6. Working Example 2

5.Results:

We have used MATLAB R2013a software for coding. Figure 7 depicts the interface of our application.

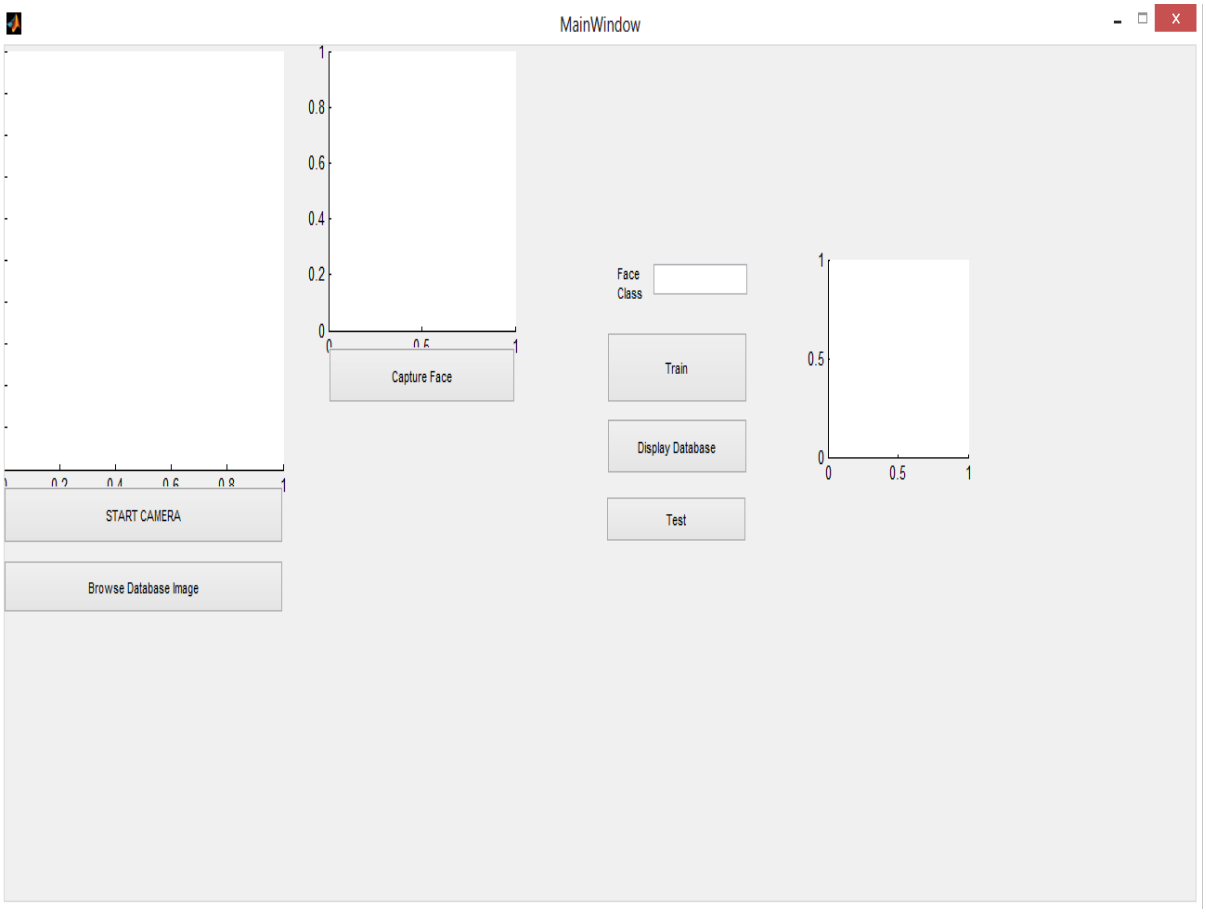


Figure 7. Interface of the Face Biometric Recognition System.

We have provided three camera view, first camera view is used to displays the view when click on the start camera button. Second view provides the user or object detected image. Capture face button is used to capture the user's image and the captured image is displayed in the third view. Face class number is given to a training data and added to the database shown in figure 8. Figure 9 determines how it adds the database. As shown in Figure 10, this is the database of all the valid users. Testing is performed by clicking on test button, determines in which the image falls in as shown in figure 11. We execute the application in parallel to reduce time, the time analysis is shown in the figure 12. Time comparison of the application in parallel execution compare to serial execution is shown in figure 13.

.

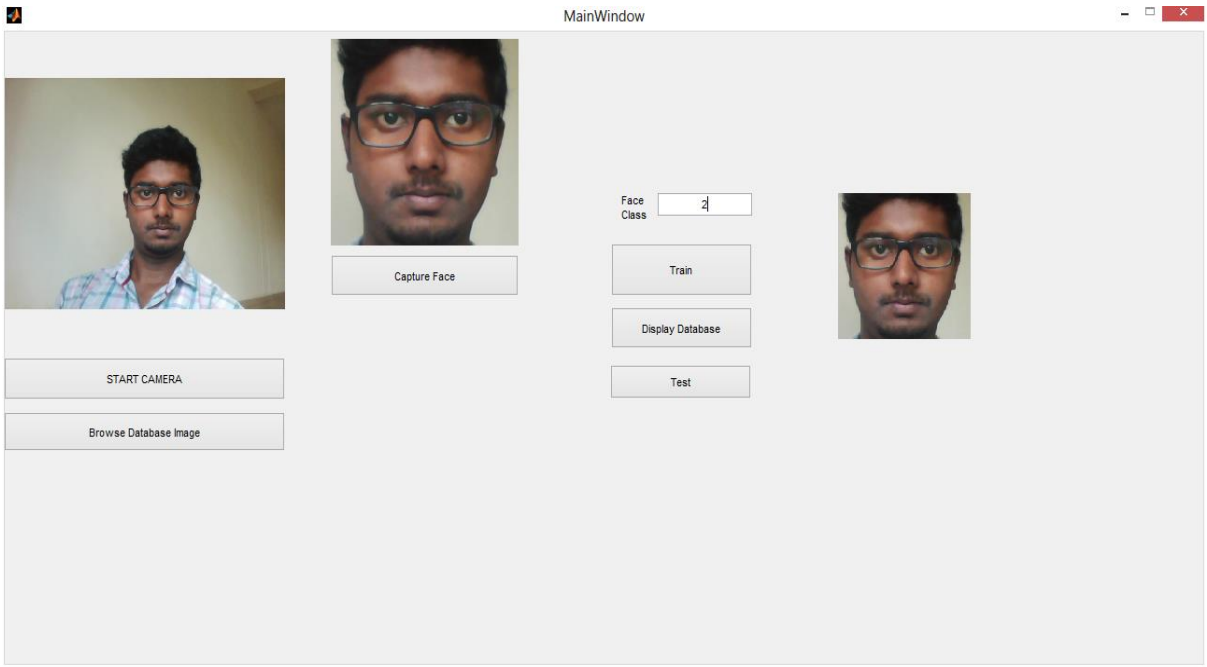


Figure 8. Authentic User's image storing in database.

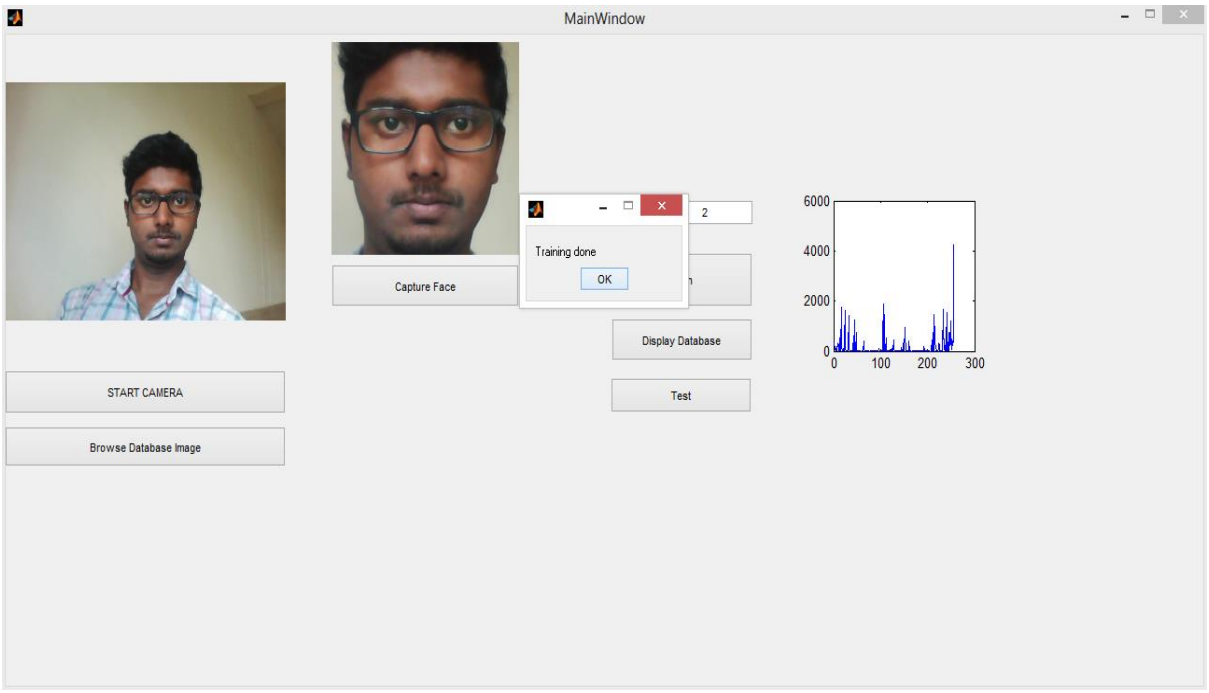


Figure 9. Added to the Database.

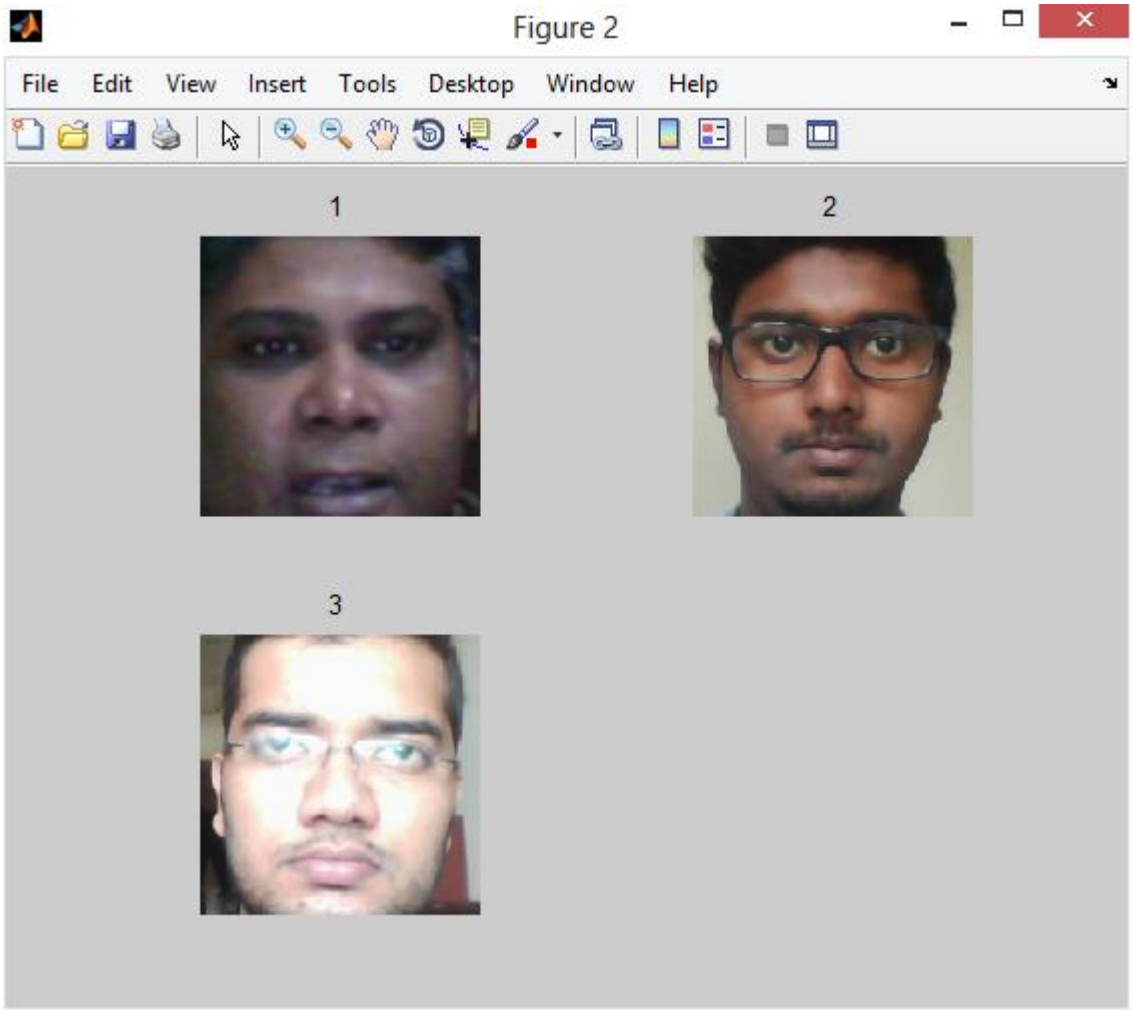


Figure 10. Displays the database of valid users.

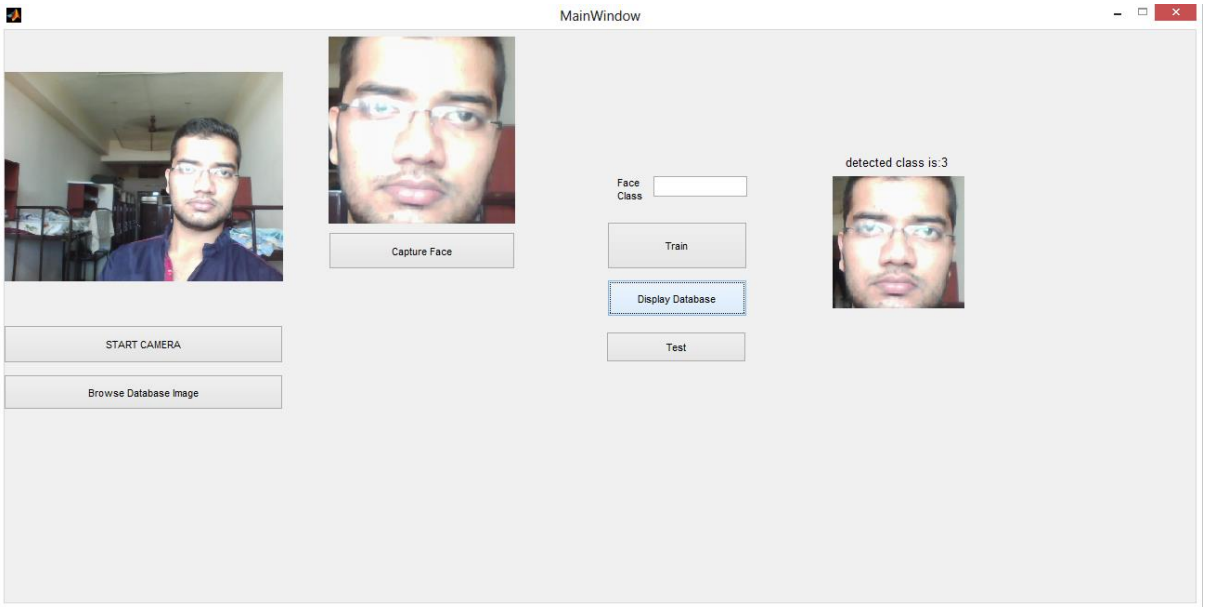


Figure 11. Testing is performed, determines the in which falls.

Profile Summary

Generated 05-Nov-2015 12:53:35 using cpu time.

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
MainWindow	2	23.296 s	0.016 s	
...'.hObject,eventdata,guidata(hObject))	1	22.842 s	0.000 s	
gcp	4	22.687 s	0.000 s	
...rayManager.getOrAutoCreateWithCleanup	2	22.672 s	-0.000 s	
parpool	1	22.641 s	0.016 s	
doParpool	1	22.625 s	-0.000 s	

Figure 12. Time analysis for running face biometric recognition.

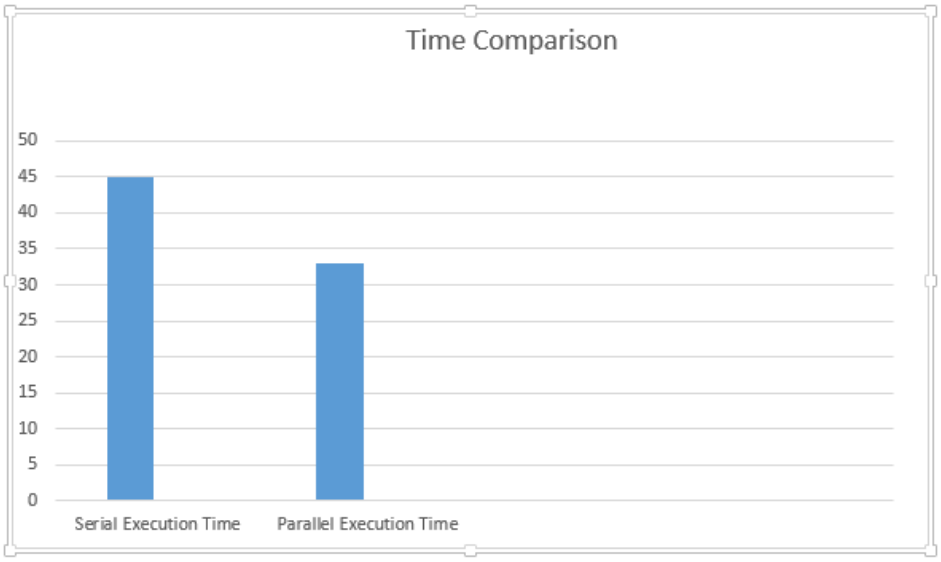


Figure 13. Time comparison

6.Conclusion:

We have presented an implementation of three dimensional coupled with anti-face spoofing technique for face liveness detection. This approach makes face recognition system secure to various types of spoof attacks liveness detection still remains a challenge for the face recognition systems. We have concluded that use of ordinary generic cameras we can protect from the different spoof attacks.

References:

[1] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security Privacy*, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003.

[2] J. Li, Y. Wang T. Tan, and A. Jain, "Live face detection based on the analysis of Fourier spectra," *Proc. SPIE, Biometric Technol. Human Identificat.*, vol. 5404, pp. 296–303, Aug. 2004.

[3] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face antispoofing database with diverse attacks," in *Proc. IEEE 5th IAPR Int. Conf. Biometrics Compendium*, Mar./Apr. 2012, pp. 26–31.

[4] 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. 11th Eur. Conf. Comput. Vis.*, Sep. 2010, pp. 504–517.

[5] B. Peixoto, C. Michelassi, and A. Rocha, "Face liveness detection under bad illumination conditions," in *Proc. IEEE 18th Int. Conf. Image Process.*, Sep. 2011, pp. 3557–3560.

[6] 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.

[7] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in *Proc. Int. Joint Conf. Biometrics*, Oct. 2011, pp. 1–7.

[8] M. De Marsico, M. Nappi, D. Riccio, and J. Dugelay, "Moving face spoofing detection via 3D projective invariants," in *Proc. 5th IAPR Int. Conf. Biometrics*, Mar./Apr. 2012, pp. 73–78.

[9] K. Kollreider, H. Fronthaler, and J. Bigun, "Non-intrusive liveness detection by face images," *Image Vis. Comput.*, vol. 27, no. 3, pp. 233–244, Feb. 2009.

[10] A. da Silva Pinto, H. Pedrini, W. Schwartz, and A. Rocha, "Video-based face spoofing detection through visual rhythm analysis," in *Proc. 25th SIBGRAPI Conf. Graph., Patterns, Images*, Aug. 2012, pp. 221–228.

[11] J. Määttä, A. Hadid, and M. Pietikäinen, "Face spoofing detection from single images using micro-texture analysis," in *Proc. Int. Joint Conf. Biometrics*, Oct. 2011, pp. 1–7.

[12] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in *Proc. Int. Conf. Biometrics Special Interest Group*, Sep. 2012, pp. 1–7.

[13] S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, "Computationally efficient face spoofing detection with motion magnification," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops*, Jun. 2013, pp. 105–110.

[14] H.-Y. Wu, M. Rubinstein, E. Shih, J. V. Guttag, F. Durand, and W. T. Freeman, "Eulerian video magnification for revealing subtle changes in the world," *ACM Trans. Graph.*, vol. 31, no. 4, p. 65, 2012.

[15] G. Kim, S. Eum, J. K. Suhr, D. I. Kim, K. R. Park, and J. Kim, "Face liveness detection based on texture and frequency analyses," in *Proc. IEEE 5th IAPR Int. Conf. Biometrics Compendium*, Mar./Apr. 2012, pp. 67–72.

[16] T. de Freitas Pereira *et al.*, "Face liveness detection using dynamic texture," *EURASIP J. Image Video Process.*, vol. 2014, no. 1, pp. 1–15, 2014.

[17] J. Bai, T.-T. Ng, X. Gao, and Y.-Q. Shi, "Is physics-based liveness detection truly possible with a single image?" in *Proc. IEEE Int. Symp. Circuits Syst.*, May 2010, pp. 3425–3428.

[18] W. R. Schwartz, A. Rocha, and H. Pedrini, "Face spoofing detection through partial least squares and low-level descriptors," in *Proc. IEEE Int. Conf. Biometrics Compendium*, Oct. 2011, pp. 1–8.

[19] 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 *Proc. IEEE Int. Conf. Biometrics Compendium*, Jun. 2013, pp. 1–8.

[20] R. Akbani, S. Kwek, and N. Japkowicz, "Applying support vector machines to imbalanced datasets," in *Proc. 15th Eur. Conf. Mach. Learn.*, 2004, pp. 39–50.

[21] I. Amidror, *The Theory of the Moiré Phenomenon: Periodic Layers*, vol. 1, 2nd ed. New York, NY, USA: Springer-Verlag, 2009.

[22] J. C. Krumm and S. A. Shafer, "Sampled-grating and crossed-grating models of Moiré patterns from digital imaging," *Opt. Eng.*, vol. 30, no. 2, pp. 195–206, 1991.

[23] J. P. Allebach and B. Liu, "Analysis of halftone dot profile and aliasing in the discrete binary representation of images," *J. Opt. Soc. Amer.*, vol. 67, no. 9, pp. 1147–1154, 1977.

[24] A. Steinbach and K. Y. Wong, "Moiré patterns in scanned halftone pictures," *J. Opt. Soc. Amer.*, vol. 72, no. 9, pp. 1190–1198, 1982.