IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
nCORETech
LBS College of Engineering, Kasaragod
Vol. 3, Special Issue 1, February 2016

Real Time Face Liveness Detection

Sreenath Narayanan K[1], Mary Reena K.E[2]

PG Scholar (M Tech in VLSI Design and Signal Processing), LBS College of Engineering, Kasaragod, India[1]

Associate Professor, ECE, LBS College of Engineering, Kasaragod, India[2]

Abstract: Face recognition is a widely used biometric approach. But face recognition systems are vulnerable to spoof attacks made by non-real faces, where a photo or video of an authorized person's face could be used to gain access to facilities or services. A secure system needs liveness detection in order to guard against such spoofing attacks. Here an efficient real time face liveness detection algorithm based on image distortion analysis (IDA) is proposed. Two different features such as blurriness and chromatic moment are extracted from the image. A fuzzy classifier is used to distinguish between live and spoof faces. The proposed approach is implemented in MATLAB 2013a tool box.

Keywords: Face recognition, liveness detection, spoofing, image distortion analysis, fuzzy classifier.

I. INTRODUCTION

Now a days many people deal with personal business, using portable devices such as mobile phones etc. From unlocking mobile phones to financial business transactions, people can easily conduct their individual business tasks through such a device. Due to this trend, personal authentication has become a significant issue. Instead of using a simple PIN code, industries have developed stronger security systems with biometric authorization technology. Biometric traits, such as face, iris and fingerprint, are very powerful factors to protect one's private information. As there are more and more applications, where face recognition is used, this act of stealing an identity is becoming more serious. Face recognition systems are vulnerable to spoof attacks made by non-real faces, where a photo or video of an authorized person's face could be used to gain access to facilities or services. If this problem remains unsolved, anyone will be able to easily obtain others' personal information in order to commit identity-related crimes. For this reason, technological defence against spoofing attacks is necessary, so as to protect personal systems and users' private data.

The only way of preventing from this type of scams is liveness detection.
Liveness Detection is a highly desirable, yet rather unexplored anti-spoofing measure in biometric identity authentication. In this paper an efficient real time face liveness detection algorithm based on image distortion analysis (IDA) is proposed. Here mainly the parameters value of two features such as blurriness and chromatic moment are extracted from a single image. A fuzzy classifier is used to distinguish between live and spoof faces. The proposed approach is implemented in MATLAB 2013a tool.

II. LITERATURE SURVEY

The anti-spoofing methods for face recognition may be roughly classified in two categories: algorithms making use of motion or texture and image quality based methods. First, motion-based approaches are most commonly employed for anti-spoofing. They aim at detecting the natural responses of the face, which include eye blinking [1], [2], mouth movement [3], and head rotation [4]. Specifically, Pan et al. [1] detected eye blinking based on the undirected conditional graphical framework, in which a discriminative measure of eye states is incorporated. In [3], the authors proposed utilizing the optical flow line of the mouth region. They projected velocity vectors onto their intuitive stick-mouth model and extracted the statistics of the lip motion for face liveness detection. Anjos et al. [5] proposed utilizing correlations between the foreground and background regions obtained from the optical flow. Specifically, they attempted to detect motion correlations between the head of the user and the background that indicate a spoofing attack. Although these approaches are conceptually simple, multiple frames are required to track face components, which leads to an increase in the detection time, and highly cooperative user actions are also required.

The texture information is taken as, the images taken from the 2-D objects (especially, the illumination components) tend to suffer from the loss of texture information compared to the images taken from the 3-D objects. For texture-based feature extraction, they used Local Binary Pattern (LBP) which is one of the most popular techniques for describing the texture information of the images. Texture based methods are very popular in face anti-spoofing possibly because of its relationship with our own discrimination capabilities on reprinted photographs. An advantage of texture-analysis is it relaxes requirements on anti-spoofing databases. Sets can be constructed using single shots of spoofing attacks.

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
nCORETech
LBS College of Engineering, Kasaragod
Vol. 3, Special Issue 1, February 2016

Inspired by image quality assessment, characterization of printing artifacts and by differences in light reflection, Maatta et al. [6] proposed an anti-spoofing solution based on micro texture analysis. The authors use the Local Binary Patterns (LBP) texture analysis operator for describing the micro-textures and use the feature vectors in a Support Vector Machine classifier which determines whether an extracted micro-texture pattern belongs to a fake person (non-live) or a live person The image quality based approaches assume that fake faces tend to be more seriously distorted by the imaging system and thus yield a lower quality image under the same capturing condition. A recent work [7] proposed a biometric liveness detection method for iris, fingerprint and face images using 25 image quality measures, including 21 full-reference measures and 4 non-reference measures. In [7] the author uses 25 features to get good results. The authors evaluated their method on the Idiap-Replay Attack database.

The paper is organized as follows, Section 2 gives literature survey of related work, Section 3 deals with proposed framework, Section 4 gives the classification method, Section 5 represents the experimental result obtained by the proposed method and finally conclusion and future scope of the work is explained.

III.PROPOSED FRAMEWORK

It is our assertion that the performance of Liveness Detection techniques can be improved with Image Distortion Analysis.

A. Image Distortion Analysis

The proposed model provides the security to biometric system by authenticating the user with face modality along with liveness detection using variations. Here mainly Blurriness and Chromatic Moment are the two features extracted for the liveness detection. The proposed algorithm for face liveness detection is shown in figure 1.

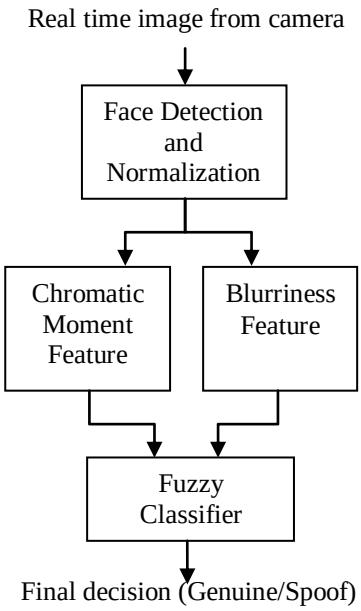


Fig. 1. The proposed real time face liveness detection

In the proposed algorithm the input is the given as a real time image captured from a camera. The face detection and normalization section detects the face from the input image. Here Voila Jones algorithm is used for face detection. The image is then normalized to 144 × 120 pixels. The face alignment and cropped face size are very important for spoof detection because they significantly reduce the influences of facial and background variations that are irrelevant to liveness detection. The blurriness and chromatic moment is measured for the normalized face image and these are referred as the features of image distortion analysis. This two feature values is then fed to fuzzy classifier. The classifier outputs are fused to give the final decision whether the face image is genuine or spoof face (e.g., printed photo attack)

(1) Blurriness Features

For short distance spoof attacks, spoof faces are often defocused in mobile phone cameras. The reason is that the spoofing medium (printed paper, tablet screen, and mobile phone screen) usually have limited size, and the attackers

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
nCORETech
LBS College of Engineering, Kasaragod
Vol. 3, Special Issue 1, February 2016

have to place them close to the camera in order to conceal the boundaries of the attack medium. As a result, spoof faces tend to be defocused, and the image blur due to defocus can be used as another cue for anti-spoofing.
According to [8], we are able to quantify the blur annoyance on a picture by blurring it and comparing the variations between neighbouring pixels before and after the low-pass filtering step. Consequently, the first step is to convert the normalized image to grayscale. On this same image, we apply a low-pass filter. Then compute the intensity variations between the neighbouring pixels of these two images. Then, the comparison result allows us to evaluate the blur annoyance. Thus, a high variation between the original and the blurred image means that the original image was sharp whereas a slight variation between the original and the blurred image means that the original image was already blurred.

(2) Chromatic moment
The spoof of face images shows a different colour distribution compared to genuine face images. This is caused by the imperfect colour reproduction property of printing and display media. This chromatic degradation was explored in [9] for detecting recaptured images, but its effectiveness in spoof face detection is unknown. Since the absolute colour distribution is dependent on illumination and camera variations, we propose to devise invariant features to detect abnormal chromaticity in spoof faces. That is, we first convert the normalized facial image from the RGB space into the HSV (Hue, Saturation, and Value) space and then compute the mean, deviation, and skewness of each channel as a chromatic feature. Since these three features are equivalent to the three statistical moments in each channel, they are also referred to as chromatic moment features. Besides these three features, the percentages of pixels in the minimal and maximal histogram bins of each channel are used as two additional features. So the dimensionality of the chromatic moment feature vector is 15.
The above two features are then given to the fuzzy classifier and checks whether the image is genuine or not.

IV. CLASSIFICATION METHOD

B. Fuzzy Inference System
As per [10] fuzzy inference system (FIS) essentially defines a nonlinear mapping of the input data vector into a scalar output, using fuzzy rules. The mapping process involves input/output membership functions, FL operators, fuzzy if–then rules, aggregation of output sets, and defuzzification. An FIS with multiple outputs can be considered as a collection of independent multi input, single-output systems. A general model of a fuzzy inference system (FIS) is shown in Figure 2.

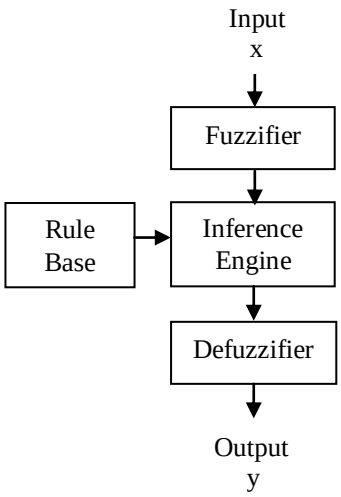


Fig. 2. Fuzzy Inference System

Here the fuzzifier is used to perform fuzzification. It is the process of making a crisp quantity. Fuzzy logic is a solution to complex problems in all fields of life, including medicine as it resembles human reasoning and decision making

V. EXPERIMENTAL RESULT

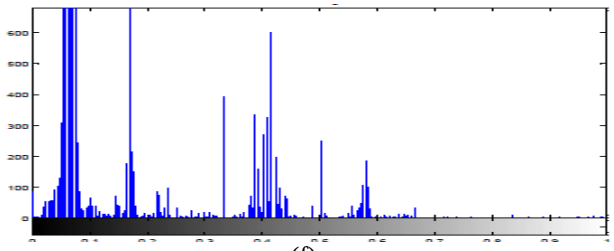
Here we evaluated the result from real time database. A high quality digital camera is used to capture the image. Seven data sets are used for experiment .The experiment is conducted by adding different amount of blur into the input image and analysed the performance among them. The chromatic moment feature include, mean, deviation, skewness,

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
nCORETech
LBS College of Engineering, Kasaragod
Vol. 3, Special Issue 1, February 2016

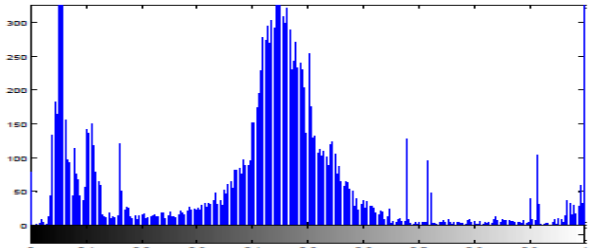
maximum and minimum bin parameters from a image. The analysis is done by taking each value separately also. We found that the mean, deviation and skew value of Hue channel is changing widely for live and spoof image. The Type I fuzzy classifier is used for the classification purpose. The numerical values from the extracted IDA features are directly loaded to the fuzzy classifier. The range of membership functions are defined in the fuzzy classifier after analysing different parameter values for different databases.

(a) (b)

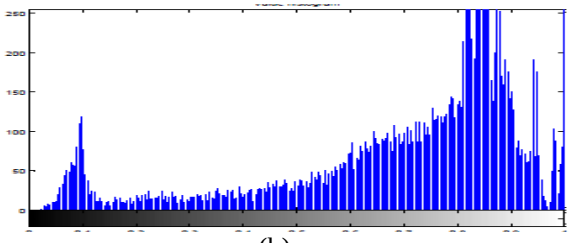
(c) (d) (e)



(f)



(g)



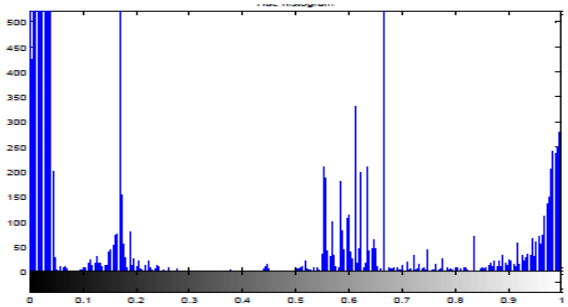
(h)

Fig. 3. Examples of chromatic moment. (a) and (b): The genuine image and normalized face; (c),(d),(e): Hue, Saturation, and Value component of normalized face respectively; (f),(g),(h): Histograms of Hue, Saturation, and Value

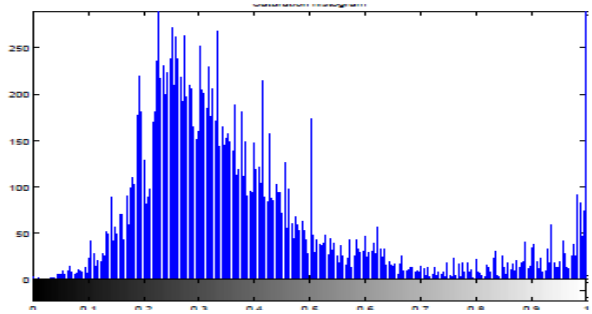
(a) (b)

(c) (d) (e)

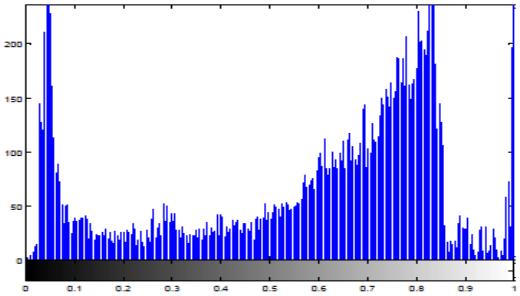
IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
nCORETech
LBS College of Engineering, Kasaragod
Vol. 3, Special Issue 1, February 2016



(f)



(g)



(h)

Fig. 4. Examples of chromatic moment. (a) and (b): The spoof image and normalized face; (c),(d),(e): Hue, Saturation, and Value component of normalized face respectively; (f),(g),(h): Histograms of Hue, Saturation, and Value

TABLE I VALUES OF THE EXTRACTED FEATURE

Image Name (genuine/spoof)	Blurriness	Chromatic Moment
g_1	0.6292	534.0342
s_1	0.419	280.0252
g_2	0.746	618.3543
s_2	0.6868	229.1476
g_3	0.5692	356.8875
s_3	0.554	157.865
g_4	0.6886	551.4531
s_4	0.5924	173.0827
g_5	0.8376	354.0419
s_5	0.7723	50.5503
g_6	0.8448	372.6217
s_6	0.8397	189.2703
g_7	0.8018	393.5283
s_7	0.6531	195.2011

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
nCORETech
LBS College of Engineering, Kasaragod
Vol. 3, Special Issue 1, February 2016

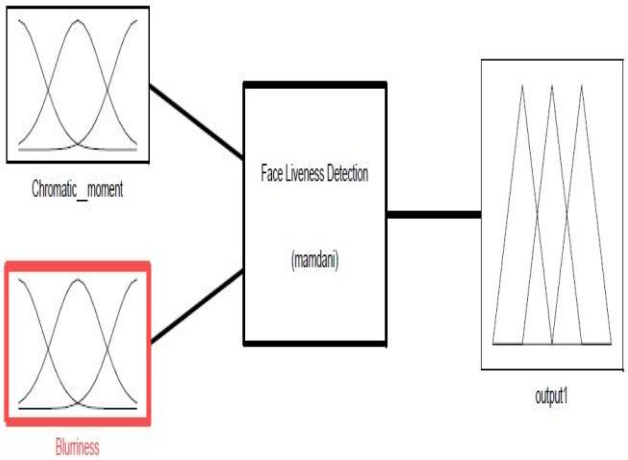


Fig. 5 Face liveness detection classifier

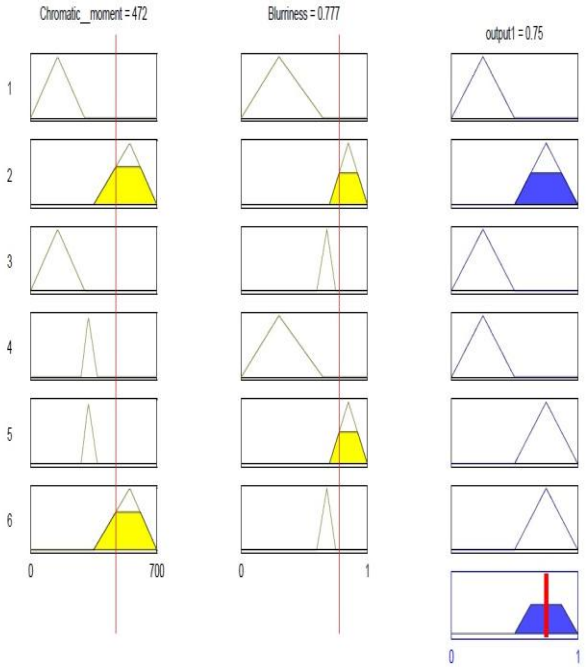


Fig. 6. Output Results from FIS

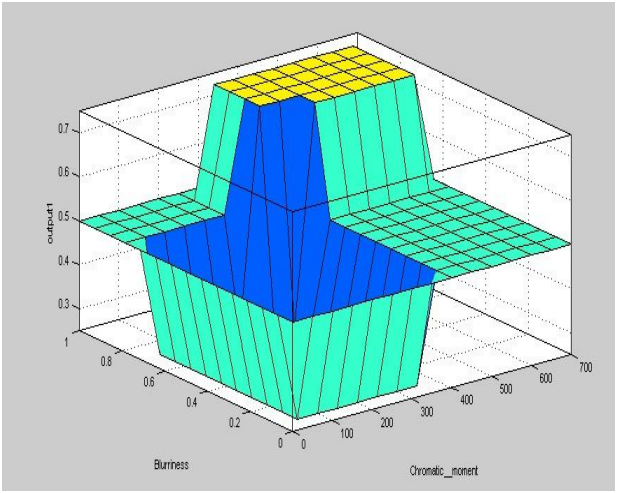


Fig.7 Surface view output Results

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
nCORETech
LBS College of Engineering, Kasaragod
Vol. 3, Special Issue 1, February 2016

VI. CONCLUSION AND FUTURE WORK

The developed system identifies the user being genuine or not with the help of single image, in contrast with the previous method where multiple images are used. The proposed system is implemented by extracting the IDA features, namely blurriness and chromatic moment. Fuzzy classifier is used for liveness detection. The result is obtained for real time database. In future the accuracy can be increased by including more features along with this two features. Thus the designed system can provides higher rate of performance in terms of security.

ACKNOWLEDGMENT

The authors would like to express special thanks to teachers for providing an excellent guidance and motivation for the research, parents and friends who helped a lot for finalizing the review work. Above all sincere thanks to god who is the power of strength in each step of progress towards its successful completion.

REFERENCES

[1] G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink-based anti-spoofing inface recognition from a generic webcamera," in Proc. IEEE 11th Int.Conf. Comput. Vis. (ICCV), Oct. 2007, pp. 1–8.
[2] L. Sun, G. Pan, Z. Wu, and S. Lao, "Blinking-based live face detection using conditional random fields," in Proc. Adv. Biometrics, Oct. 2007, pp. 252–260. [2]
[3] K. Kollreider, H. Fronthaler, M. I. Faraj, and J. Bigun, "Real-time face detection and motion analysis with application in 'liveness' assessment," IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 548–558, Sep. 2007BIOGRAPHY
[4] W. Bao, H. Li, N. Li, and W. Jiang, "A liveness detection method for face recognition based on optical flow field," in Proc. IEEE Int. Conf. Image Anal. Signal Process., Apr. 2009, pp. 233–236.
[5] A. Anjos, M. M. Chakka, and S. Marcel, "Motion-based counter-measures to photo attacks in face recognition," IET Biometrics, vol. 3, no. 3, pp. 147–158, Sep. 2014.
[6] J. Ma¨att ¨ a, A. Hadid, and M. Pietikainen, "Face Spoofing Detection from ¨ Single Images using Micro-texture Analysis," in Intl. Joint Conference on Biometrics, Oct. 2011, pp. 1–7.
[7] 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.
[8] F. Crete, T. Dolmiere, P. Ladret, and M. Nicolas, "The blur effect: Perception and estimation with a new no-reference perceptual blur metric," Proc. SPIE, vol. 6492, p. 64920I, Feb. 2007.
[9] Y. Chen, Z. Li, M. Li, and W.-Y. Ma, "Automatic classification of photographs and graphics," in Proc. ICME, Jul. 2006, pp. 973–976.
[10] Tomoham Nakashima, Gaku Nakai, **and** Hisao Ishibuchi "Constructing Fuzzy Ensembles for Pattern Classification Problems", in Systems, Man and Cybernetics, 2003. IEEE International Conference on (Volume:4)
[11] Di Wen, Member, IEEE, Hu Han, Member, IEEE, and Anil K. Jain, Life Fellow, IEEE "Face Spoof Detection With Image Distortion Analysis", IEEE Transactions on Information Forensics And Security, vol. 10, no. 4, April 2015
[12] Bezdek, J. C., 1993. Fuzzy models—what are they and why—editorial. IEEE Transactions on Fuzzy Systems, vol .1, pp. 1–5.