International Journal of Advances in Engineering & Scientific Research, Vol.4, Issue 1, Jan-2017,
pp 40-48 ISSN: 2349 –3607 (Online) , ISSN: 2349 –4824 (Print)

www.arseam.com
Impact Factor: 2.48

Cite this paper as : *Dilna E.P et. al .(2017). Fake Face Identification, International Journal of Advances in Engineering & Scientific Research, Volume 4,(Issue 1, Jan-2017), pp 40–48. ISSN: 2349 –3607 (Online) , ISSN: 2349 –4824 (Print),*

FAKE FACE IDENTIFICATION

Ms. Dilna e p[1], Ms. Maneesha Manoj[2], Ms. Jiji c j[3], Ms. Jeena c j [4]
Ms. Hrudhya k p[5]
[1,2,3,4] UG Students, Department of Computer Science and Engineering,
[5]Assistant Professor, Department of Computer Science and Engineering,
IES College of Engineering, Chittilappilly, Thrissur.

Abstract:

Objective- Automatic face recognition is now widely used in applications ranging from de-duplication of identity to authentication of mobile payment. This popularity of face recognition has raised concerns about face spoof attacks (also known as biometric sensor presentation attacks), where a photo or video of an authorized person's face could be used to gain access to facilities or services. While a number of face spoof detection techniques have been proposed, their generalization ability has not been adequately addressed. We propose an efficient and rather robust face spoof detection algorithm based on *Image Distortion Analysis (IDA)*.

Design/Methodology/Approach- Four different features (specular reflection, blurriness, chromatic moment, and color diversity) are extracted to form the IDA feature vector. An ensemble classifier, consisting of multiple SVM classifiers trained for different face spoof attacks (e.g., printed photo and replayed video), is used to distinguish between genuine and spoof faces. The proposed approach is extended to multi-frame face spoof detection in videos using a voting based scheme. We also collect a face spoof database, MSU Mobile Face Spoofing Database (MSU MFSD),using two mobile devices (Google Nexus 5 and MacBook Air) with three types of spoof attacks (printed photo, replayed video with iPhone 5S and iPad Air).

Limitations- It is difficulty in separating genuine and spoof faces, especially in cross-database and cross device scenarios.

Practical implications- The system ensures user privacy and provides better security.

Originality- Two public-domain face spoof databases (Idiap REPLAY-ATTACK and CASIA FASD), and the MSU MFSD database show that the proposed approach outperforms state-of-the-art methods in spoof detection.

Keywords- Face Recognition, Spoof Detection, Image Distortion Analysis, Ensemble Classifier, Cross-Database, Cross-Device

1.INTRODUCTION

AS a convenient user authentication technique, automatic face recognition has attracted increasing attention in various access control applications, especially for mobile phone unlocking. With the release of face unlocking functionality in the Android mobile operating system, face recognition becomes another biometric authentication technique for mobile phones similar to fingerprint authentication (Touch ID) in the iOS system. Unlike fingerprint authentication, face recognition does not require any additional sensor since all smart phones come equipped with a front facing camera. However, similar to other biometric modalities, we need to address concerns about face spoof

attacks on face recognition systems, particularly in unconstrained sensing and uncooperative subject scenarios . It is relatively easier to acquire a person's face image or video (e.g., with a digital camera or from social media) than it is to acquire other biometric traits such as fingerprint, palm print, and iris. Further, the cost of launching a face spoof attack, such as a printed photo, displayed photo, or replayed video is relatively low . In this experiment, more than 70% of probe videos (spoof faces) were *successfully* matched to the gallery . In this paper we do not address 3D facemask attacks2, which are more expensive to launch. Instead, we focus on printed photo and replayed video attacks.

The fragility of face recognition systems to face spoof attacks has motivated a number of studies on face spoof detection . However, published studies are limited in their scope because the training and testing images (videos) used were captured under the same imaging conditions. It is essential to develop robust and efficient face spoof detection (or anti-spoofing) algorithms that generalize well to new imaging conditions and environments. In this paper, we study the cross-database face spoof detection problem and propose a face spoof detection approach based on *Image Distortion Analysis* (IDA). The contributions of this paper can be summarized as follows:
i) A face spoof detection algorithm based on IDA, which is effective in grasping the intrinsic distortions of spoof face images with respect to the genuine face images.
ii) We construct a face spoof database, named the MSU Mobile Face Spoof Database (MSU MFSD), using the cameras of a laptop (MacBook Air3) and a mobile phone and three types of attack medium (iPad, iPhone, and printed photo). The MSU MFSD database allows us to evaluate the generalization ability of face spoof detection algorithms across different cameras and illumination conditions with mobile devices. For a subset of the MSU MFSD database.
iii) We present results for both intra-database and cross database scenarios using two public-domain face spoof databases (Idiap REPLAY-ATTACK and CASIA FASD), and our own database (MSU MFSD).

II. RELATED WORKS

One of the earliest studies on face spoof detection was reported in 2004. The growing popularity of using face recognition for access control, this topic has attracted significant attention over the past five years.one of the major focus of the FP7 EU funded project, TABULA RASA, is "trusted biometrics under spoofing attacks". Here, we provide a brief summary of face spoof detection algorithms published in the literature along with their strengths and limitations in terms of (i) robustness and generalization ability, and (ii) realtime response and usability. According to different types of cues used in face spoof detection, published methods can be categorized into four groups: (1).face liveness detection using dynamic texture(2).classification of captured and recaptured images to detect photograph spoofing (3).spoofing in 2D recognition with 3D masks and anit-spoofing with Kinect (4).face anti-spoofing methods.

2.1 FACE LIVENESS DETECTION USING DYNAMIC TEXTURE:

User authentication is an important step to protect information, and in this context, face biometrics is potentially advantageous. Face biometrics is natural, intuitive, easy to use, and less human-invasive. Unfortunately, recent work has revealed that face biometrics is vulnerable to spoofing attacks using cheap low-tech equipment.A novel and appealing approach to detect face spoofing using the spatio temporal (dynamic texture) extensions of the highly popular local binary pattern operator. The key idea of the approach is to learn and detect the structure and the dynamics of the facial micro-textures that characterise real faces but not fake ones. We evaluated the approach with two publicly available databases (Replay-Attack Database and CASIA Face Anti-Spoofing Database). The results show that our approach performs better than state-of-the-art techniques following the provided evaluation protocols

of each database. Anti- spoofing ,liveness detection,counter measure,face recognition,biometrics are the keywords. Because of it ‘s natural and non-intrusive interaction, identify verification and recognition using facial information are among the most active and challenging areas in computer vision research .The issue of verifying if the face presented to a camera is indeed a face from a real person and not an attempt to deceive (spoof) the system has mostly been overlooked. It was not until very recently that the problem of spoofing attacks against face biometric system gained attention of the research community. This can be attested by the gradually increasing number of publicly available databases and the recently organized. A spoofing attack consists in the use of forged biometric traits to gain illegitimate access to secured resources protected by a biometric authentication system.

The lack of resistance to direct attacks is not exclusive to face biometrics. The findings indicate that finger print authentication systems suffer from a similar weakness. In authentication systems based on face biometrics , spoofing attacks are usually perpetrated using photographs ,videos or forged masks . while one can also use make-up or plastic surgery as means of spoofing, photographs and videos are probably the most common sources of spoofing attacks.

2.2 CLASSIFICATION OF CAPTURED AND RECAPTURED IMAGES TO DETECT PHOTOGRAPH SPOOFING:

A new face anti-spoofing approach, which is based on analysis of contrast and texture characteristics of captured and recaptured images, is proposed to detect photograph spoofing. Since photo image is a recaptured image, it may show quite different contrast and texture characteristics when compared to a real face image. In a spoofing attempt, image rotation is quite possible. Therefore, a rotation invariant local binary pattern variance (LBPV) based method is selected to be used. The approach is tested on the publicly available NUAA photo-impostor database, which is constructed under illumination and place change. The results show that the approach is competitive with other existing methods tested on the same database. It is especially useful for conditions when photos are held by hand to spoof the system. Since an LBPV based method is used, it is robust to illumination changes. It is non-intrusive and simple.

In a spoofing attempt, a person tries to masquerade as another person and thereby, tries to gain an access to the system. Numerous recognition approaches have been presented in face recognition topic, however the studies on face anti spoofing methods are still very limited. Therefore, nowadays anti-spoofing is a popular topic for researchers to fill this gap. Aim is to develop non-intrusive methods without extra devices and human involvement. In this way they can be integrated into existing face recognition systems. Also, methods which are robust to pose and illumination changes are preferable.

The proposed approach relies on different contrast and texture characteristics of captured images and recaptured images to detect photograph spoofing. In the proposed approach, initially a DoG filter is used to obtain a special frequency band which gives considerable information to discriminate between real and photo images. DoG features are used for liveness detection and satisfactory results are reported. DoG filtering is used as the pre-processing step, and LBPV based method is used for feature extraction in the main part. The problem is simply a classification problem with two classes. First class is the real image class, which are in fact captured face images, and second class is the class of photograph images of real faces.

2.3 SPOOFING IN 2D RECOGNITION WITH 3D MASKS AND ANTI-SPOOFING WITH KINECT:

The problem of detecting face spoofing attacks (presentation attacks) has recently gained a well deserved popularity .Mainly focusing on 2D attacks forged by displaying printed photos or replaying recorded videos on mobile devices, a significant portion of these studies ground their arguments on the flatness of the spoofing material in front of the sensor. we inspect the spoofing potential of subject-specific 3D facial masks for2D face recognition .Local Binary Patterns based counter measures using both color and depth data, obtained by Kinect .This purpose, introduce the

3D Mask Attack Database (3DMAD), the first publicly available 3D spoofing database, recorded with a low-cost depth camera. Extensive experiments on 3DMAD.

Among many reliable biometric traits, face is a very popular one and it owes this reputation mainly to its accessibility .But unfortunately, this gift can also be acurse in malicious circumsances, enabling attackers to easily create copies and spoof face recognition systems. Spoofing is an attempt to gain authentication through a biometric system by presenting a counterfeit evidence of a valid user. Due to their convenience and low-cost, the most common types of spoofing methods being focused are photo and video attacks. Proposed anti-spoofing approaches against these attacks can be broadly classified into three groups liveness detection, motion analysis and texture analysis.

The first group aims to detect liveness of face, based on live-face specific movements such as eye blinking or lip movements .The second group of approaches analyze the motion in the scene and expose spoofing attacks by examining the way the objects move in front of the sensor. The movements of planar objects like papers or screens differ greatly from those of a real face. For this reason, in the trajectories of small regions in face images are analyzed and classified as real or fake. Similarly in, a set of facial points are located automatically and their geometric invariants are utilized to detect attacks.

In the third group of methods, the texture of the face image is examined to find spoofing clues like printing artifacts and/or blurring .Alternatively, micro-texture analysis is also applicable as proposed in a recent paper in which multi-scale local binary patterns (LBP) are utilized. A substantial portion of these approaches for 2D anti spoofing are rendered inoperative when 3D facial masks are introduced for attacks. For instance in , that a liveness detection system relying on eye-blinking and lip movements can be defeated by simply using photographic masks which are actually high resolution facial prints worn on face with eyes and mouth regions cut out. On the other side, motion based counter measures that depend on the shape difference between real and fake faces are not able to operate as intended .when the photos or screens are replaced by facial masks.

2.4 FACE ANTI-SPOOFING METHODS:

Facial biometric systems have received increased deployment in various application such as surveillance access control and forensic investigation .one of the limitations of face recognition system is the high possibility of the system being deceived or spoofed by non real faces such as photograph, video clips or dummy faces. to identify the spoofing attacks such as biometric system ,face liveness detection have been developed .it presents a review of state-of-the-art techniques in face liveness detection, which are classified into two groups, namely intrusive and non-intrusive approaches .each technique is in the term of its implementation, strengths and limitations.

Biometric traits can be categorized into two classes, namely physical characteristics, such as fingerprints, faces or iris patterns and behavioral characteristics such as voice, signature or walking patterns.one of the most predominant challenges in many biometric recognition systems the possibility of identity theft, which is conceptually known as spoofing attack. Some stolen biometrics data can be easily exploited and mimicked by impostors to gain unauthorized access to the biometric system, without the consent of the genuine user. Examples of spoofing attack son biometrics systems include the use of artificial fingers, contact lens with retinal patterns and recorded voice. Research efforts on identification of spoofing attack have been made from various perspectives. In this article, the state-of-the-art spoofing identification techniques for facial biometrics based on liveness detection are presented.

Generally, fake faces can be categorized into two classes: positive and negative. The positive class, also known as the genuine face, has limited variation, whereas the negative class includes the spoof faces on photographs, dummy

or recorded videos. examples of fake faces made of silica gel, rubber, photo and video replay. Facial biometrics spoofing techniques involve placing genuine photographs or dummies, playing video recording etc. In front of the camera. A human photograph represents planar objects with only one static facial expression. However, it lacks the three-dimensional (3D) information and provides less physiological clues than videos3. These limitations of still photographs are often exploited in liveness detection for facial biometrics. However, the challenges in facial detection increase for spoofing attacks that involve the use of video cameras. Nowadays, videos of a genuine user with facial expressions, eye blink and head movement can be easily captured using high quality cameras. As far as 3D structure is concerned, a 3D corporeal model of a user has detailed 3D information that photos and videos do not possess.

The biometric system can be spoofed by using a 3D corporeal model which is known as synthesis attack. Dummy models can usually reproduce rigid head movement by rotation but cannot imitate the lip movement, eye blink and facial expressions. On the face liveness detection have been widely explored in order to tackle the problem of spoofing attacks. Face liveness detection involves a process of verifying whether the face image presented to recognition system is real (i.e. alive) specimen or has been reproduced synthetically and is thus fraudulent. This article mainly describes the state-of-the-art techniques in face liveness detection, which covers both intrusive and non-intrusive methods.

III. SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

Existing methods, particularly methods using texture features, commonly used features (e.g., LBP) that are capable of capturing facial details and differentiating one subject from the other (for the purpose of face recognition). As a result, when the same features are used to differentiate a genuine face from a spoof face, they either contain some redundant information for liveness detection or information that is too person specific. These two factors limit the generalization ability of existing methods. To solve this problem, we have proposed a feature set based on Image Distortion Analysis (IDA) with real-time response (extracted from a single image with efficient computation) and better generalization performance in the cross-database scenario. Compared to the existing methods, the proposed method does not try to extract features that capture the facial details, but try to capture the face image quality differences due to the different reflection properties of different materials, e.g., facial skin, paper, and screen. As a result, experimental results show that the proposed method has better generalization ability.

3.1.1 DRAW BACKS

- Low robustness
- Slow response
- High computational complexity
- Additional sensing or processing technique needed
- Different classifiers needed for different spoof attacks

3.2 PROPOSED SYSTEM

In the proposed system ,the face spoof based image distortion analysis(IDA).Four types of IDA features(specular reflection,blurriness,color moment,color diversity).The four different features are concatenated together,resulting in a 121-dimensional IDA feature vector.An ensemble classifier consisting of two constituent SVM classifiers trained for different spoof attacks is used for the classification of genuine and spoof face. In mobile applications, the real-

time response of face spoof detection requires that a decision be made based on a limited. The proposed face spoof detection algorithm based on Image Distortion Analysis. Therefore, we aim to design discriminative features that are capable of differentiating between genuine and spoof faces based on a single frame. Given a scenario where a genuine face or a spoof face (such as a printed photo or replayed video on a screen) is presented to a camera in the same imaging environment, the main difference between genuine and spoof face images is due to the "shape" and characteristics of the facial surface in front of the camera. According to the Dichromatic Reflection Model [24], light reflectance I of an object at a specific location x can be decomposed into the following diffuse reflection (Id) and specular reflection (Is) components:

$$I(x)=Id + Is = wd(x)S(x)E(x)+ws(x)E(x) \quad (1)$$

where E(x) is the incident light intensity, wd(x) and ws(x) are the geometric factors for the diffuse and specular reflections, respectively, and S(x) is the local diffuse reflectance ratio. Since 2D spoof faces are recaptured from original genuine face images, the formation of spoof face image intensity I(x) can be modeled as follows:

$$I(x)=Id + Is = F(I(x)) + ws(x)E(x) \quad (2)$$

Note that equation (1) and (2) only model the reflectance difference between genuine and spoof faces and have not considered the final image quality after camera capture. In equation (2), we substitute the diffuse reflection of spoof face image Id by F(I(x)) because the diffuse reflection is determined by the distorted transformation of the original face image I(x). Therefore, the total distortion in I(x) compared to I(x) consists of two parts: i) distortion in the diffuse reflection component (Id), and ii) distortion in the specular reflection component (Is), both of which are related to the spoofing medium. In particular, Id is correlated with the original face image I(x), while Is is independent of I(x). Furthermore, the distortion function F(·) in the diffuse reflectance component can be modeled as

$$F(I(x)) = H(GI(x)), \quad (3)$$

where G(·) is a low pass point spread function (blurring the original face image) and H(·) is a histogram transformation function (distorting color intensity). Explanation of G(·) and H(·) in printed photo attack and replay video attack is detailed below. Based on this imaging model, we provide an analysis of the significant differences between genuine faces and two types of spoof faces (printed photo and replay video or photo attacks) studied in this paper. Printed photo attack: In printed photo attack, I(x) is first transformed to the printed ink intensity on the paper and then to the final image intensity through diffusion reflection from the paper surface. During this transformation, G(·) and H(·) are determined by the printer frequency and chromatic fidelity. For high resolution color printer, the distortion of G(·) can be neglected, but not for H(·), since it has been reported that the color printing process usually reduces the image contrast [25]. Therefore, image distortion in printed photo attack can be approximated by a contrast degrading transformation. Replay video attack: In replay video attack, I(x) is transformed to the radiating intensity of pixels on LCD screen. Therefore, G(·) is determined by the frequency band width of the LCD panel, the distortion of which can be neglected. H(·) is related to the LCD color distortion and intensity transformation properties. Besides the difference in diffuse reflectance, the specular reflectance of the spoof face also differentiates from that of the genuine face, which is caused by the spoof medium surface. Due to the glassy surface of tablet/mobile phone and the glossy ink layer on the printed paper, there is usually a specular reflection around the spoof face image. While for a genuine 3D face, specular reflection is only located in specific fiducial locations (such as nose tip, glasses, forehead, cheeks, etc.). Therefore, pooling the specular reflection from the entire face image can also capture the image distortion in spoof faces. Besides the above distortions in the reflecting process, there is also distortion introduced by the capturing process. Although the capturing distortion can apply to both genuine and spoof faces. The spoof faces are more vulnerable to such distortion because they are usually captured in close distance to conceal the discontinuity of spoof medium frame. For example, defocused blurriness is commonly seen in both printed photo and replayed video attacks. Based on the above analysis, the major distortions in a spoof face

image include: (1) specular reflection from the printed paper surface or LCD screen; (2) image blurriness due to camera defocus; (3) image chromaticity and contrast distortion due to imperfect color rendering of printer or LCD screen; and (4) color diversity distortion due to limited color resolution of printer or LCD screen. There might be some other distortions present in spoof face images such as geometric distortion (e.g., paper warping) and artificial texture patterns (e.g., Moir´e pattern); however, these distortions are camera and illumination dependent. For example, geometric distortion varies with illumination and the artificial texture pattern can only be discerned by a high quality camera. Hence, we focus only on the above four general sources of image distortion in spoof face images (specular reflection, blurriness, chromaticity, and color diversity), and design the corresponding features for face spoof detection. The system diagram of the proposed spoof detection algorithm based on IDA. The input face image is first aligned based on two eyes locations and normalized to 144 × 120 pixels with an inter pupillary distance (IPD) of 60 pixels. For face detection and eye localization, we use the PittPatt 5.2.2 SDK [26], which works successfully for about 99% of the faces in the Idiap, CASIA, and MSU face spoof databases. Our experiments show that face alignment and cropped face size are very important for spoof detection because they significantly reduces the influences of facial and background variations that are irrelevant to spoof detection. For each normalized face image, four different IDA features are extracted, constituting a 121-dimensional feature vector. This feature vector is then fed into multiple SVM classifiers, each trained on a different group of spoof training samples (e.g., printed photo attack and replayed video attack). The classifier outputs are fused to give the final binary decision (ensemble classification): genuine or spoof face.

3.2.1 ADVANTAGES OF PROPOSED SYSTEM

- Good generalization ability
- Fast response
- Low computational complexity
- High robustness

IV.SYSTEM DESIGN AND IMPLEMENTATION MODELS

4.1 IMPLEMENTATION MODULES

There are 2 modules:

- **Admin**
- **user**

4.1.1 ADMIN

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.

4.1.1.1 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.

4.1.1.1.1 BLURRINESS FEATURE

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 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.

4.1.1.1.2 CHROMATIC MOMENT

The spoof of face images shows a different color distribution compared to genuine face images. This is caused by the imperfect color reproduction property of printing and display media. This chromatic degradation was explored in for detecting recaptured images, but its effectiveness in spoof face detection is unknown. Since the absolute color distribution is dependent on illumination and camera variations, we propose to devise invariant features to detect abnormal chromaticity in spoof faces.

4.1.1.2 FUZZY INFERENCE SYSTEM

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.

4.1.2 USER

User can login to this system using face authentication process with his original face. The system can identify whether the face is spoof or not.

4.2 SYSTEM ARCHITECTURE

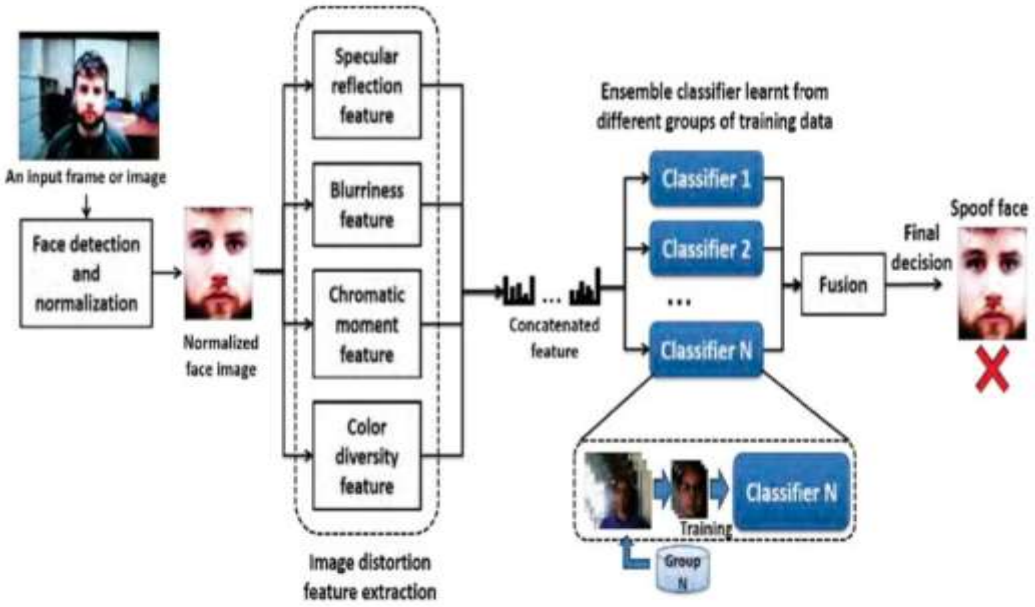

Fig.4.2.1 Architecture diagram

V. CONCLUSION

This face liveness detection system detects the spoof face where the face authentication system is used. The face recognition is a widely used biometric authentication mechanism which is used for login or accessing several data or digital areas. But the photo or video of an authorized person can also be used to enter in to the desired section, which is the main demerit of the face authentication system. So the liveness of the face is important in face recognition entry methods. we use an efficient real time face liveness detection algorithm based on image distortion analysis with the help of some features like blurriness and chromatic moment. There is a fuzzy classifier used to detect the liveness. we can make this system more accurate in future.

VI. REFERENCES

[1] A. Rattani, N. Poh, and A. Ross, "Analysis of user-specific score characteristics for spoof biometric attacks," in *Proc. CVPR Workshops*, 2012, pp. 124–129.
[2] N. Evans, T. Kinnunen, and J. Yamagishi, "Spoofing and countermeasures for automatic speaker verification," in *Proc. INTERSPEECH*, 2013, pp. 925–929.
[3] L. Best-Rowden, H. Han, C. Otto, B. Klare, and A. K. Jain, "Unconstrained face recognition: Identifying a person of interest from a media collection," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 12, pp. 2144– 2157, Dec 2014.
[4] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in *Proc. IEEE BIOSIG*, 2012, pp. 1–7.
[5] N. Erdogmus and S. Marcel, "Spoofing in 2D face recognition with 3D masks andanti-spoofing with kinect," in *Proc. IEEE BTAS*, 2013, Pp.1-6.