



# Find Pretend Biometric Mistreatment Image Distortion Analysis for Spoofing Detection

Devi.P<sup>1</sup>, Keerthika.N<sup>2</sup>

PG Scholar, Department of CSE, Vandayar Engineering College, Thanjavur, India<sup>1</sup>

Assistant Professor, Department of CSE, Vandayar Engineering College, Thanjavur, India<sup>2</sup>

**Abstract**— 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. Current face biometric systems are vulnerable to spoofing attacks. A spoofing attack occurs when a person tries to masquerade as someone else by falsifying data and thereby gaining illegitimate access. Inspired by image quality assessment, characterization of printing artifacts, and differences in light reflection, we propose to approach the problem of spoofing detection from texture analysis point of view. Hence, we present a novel approach based on analyzing facial image quality or detecting whether there is a live person in front of the camera or a face print. The proposed approach analyzes 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. This face provides a unique feature space for coupling spoofing detection and face recognition. Extensive experimental analysis on a publicly available database showed excellent results compared to existing works.

**Index Terms**— Face recognition, spoof detection, image distortion analysis, cross database.

## I. INTRODUCTION

Computer forensics (sometimes known as computer forensic science) is a branch of science pertaining to legal evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the information. Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail. Face recognition systems to face spoof attacks have motivated a number of studies on face spoof detection. However, published studies are limited in their scope because the

training and testing images used were captured under the same imaging conditions. It is essential to develop face spoof

detection algorithms generalize well to new imaging conditions and environments. The cross database face spoof detection problem and propose a face spoof detection approach based on IDA. A face spoof algorithm based on IDA, which is effective in grasping the intrinsic distortions of spoof face images with respect to the genuine face images.

### A. Application of Information Forensics and Security

The china's continuous improvement in the degree of information regions of the country have been covered by network and a great deal of information network security issues. Information security emergency response procedures and disposal system are proposed according to the comprehensive analysis of weak links. Audio, video using the anti forensics technique for authentication and data security. Automated user transparent approach to log web URLs for Forensic analysis. An automated approach to record web activity as the user connects to Internet. It includes monitoring and logging of Web URLs visited by the user.

The distinctive features of this approach are a) it starts automatically, b) it is transparent to users, c) it is robust against intentional or un-intentional process kill, and d) it is robust against intentional or un-intentional. As the physical and cyber we live in worlds converge, public security and forensics increasingly become problems of the information and communication network infrastructure that supports our society. Wireless communications, traditional telephony, the Internet, broadcast communication networks.

Digital forensics and information security applications successful across a wide variety of types; however, there are mixed results regarding the utility of unigrams and bigrams as inputs independently.

### B. Project Description

Face recognition systems to face spoof attacks have motivated a number of studies on face spoof detection. However, published studies are limited in their scope because the training and testing images used were captured under the same imaging conditions. It is essential to develop face spoof detection algorithms generalize well to new imaging conditions and environments. The cross database



face spoof detection problem and propose a face spoof detection approach based on IDA. A face spoof algorithm based on IDA, which is effective in grasping the intrinsic distortions of spoof face images with respect to the genuine face images. A face spoof database, named the MSU Mobile Face Spoof Database (MSU MFSD), using the cameras of a laptop and a mobile phone. The results for both intra database and cross database scenarios using two public domain face spoof databases. According to different types of cues used in face spoof detection published methods can be categorized into four groups. It is essential to develop face spoof detection algorithms generalize well to new imaging conditions and environments. The cross database face spoof detection problem and propose a face spoof detection approach based on IDA.

**1. Motion based method:** These methods designed primarily to counter printed photo attacks capture a very important cue for vitality the subconscious motion of organs muscles in a live face, such as eye blink mouth movement and head rotation motion is a relative feature across video frames. These methods are expected to have better generalization ability than the texture based methods that will be discussed below. The motion based methods are apparent. The frequency of facial motion is restricted by the human physiological rhythm, which ranges from 0.2-0.5 HZ.

**2. Texture based methods:** To counter the printed photo and replayed video attacks, texture based methods were proposed to extract image artifacts in spoof face images. The authors argued that texture features are capable of differentiating artifacts in spoof faces from the genuine faces. Texture based methods have achieved significant success on the Idea and CASIA databases. The Half Total Error Rate on the Idea database was reduced from 13.87% in 4 and 7.60% in 16 to 6.62% in by incorporating texture cues. The motion based methods, texture based methods need only a single image to detect a spoof. The generalization ability of many texture based methods has been found to be poor. Due to the intrinsic data driven nature of texture based methods they can be easily over fitted to one particular illumination and imagery condition and hence do not generalize well to databases collected under different conditions.

**3. Methods based on image quality analysis:** A recent work 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. Compared to our work is different in the following aspects. While 25 features are required into get good results no face specific information has been considered in designing informative features for face spoof detection. The work in aims at designing a generic liveness detection method across different biometric modalities the training and testing of each modality were still performed under intra database. While the authors of evaluated their method on only the Idiap Reply database we have used both the Idiap and CASIA database which are two important public domain database.

**4. Methods based on other cues:** Face spoof counter measures using cues derived from sources other than 2D intensity image such as IR sensor was required in a

microphone and speech analyzer were required in multiple face images taken from different viewpoints were required additionally the spoofing context method proposed can be circumvented by concealing the spoofing medium.

## II. RELATED WORKS

### A. Analysis of user specific score characteristics for spoof biometric attacks

The vulnerability to spoof attacks standard performance evaluation strategies are likely to provide an optimistic estimate of the biometric system performance. The aim of this study is to analyze the score characteristics for spoof attacks such an analysis will 1) help improve our understanding of the zoo effect under spoof attacks and 2) allow us to design biometric classifiers that are more robust to the attacks analyze the correlation between user specific score characteristics The need for user specific matching and fusion schemes for increasing the robustness of the system against spoof attacks. It may also be used to decrease the robustness of the biometric system at the user level. The biometric systems analyze the correlation between the user characters. It detect the spoof attackers using the user specific score characteristics.

### B. Spoofing and countermeasures for automatic speaker verification

The use of prior knowledge is clearly unrepresentative of the practical scenario. The nature of the attack can never be known a public datasets of licit and spoofed speaker verification transactions to facilitate independent efforts in spoofing assessment and the development of countermeasures to provide the starting point for such an initiative. Promote the consideration of spoofing to encourage the development of countermeasures and to form a new community. It describes the selection of vulnerabilities studied previously presents a brief survey of recent work to develop spoofing countermeasures and discusses current approaches to evaluation. To encourage the development of countermeasures and form a new community. The speaker verification method is potential to detect spoofing attacks with manageable impacts on system usability. It trivial has the potential to detect the spoofing attacks with manageable impacts on system usability and the development of countermeasures and to form a new community. Improve the comparability of different countermeasures and their performance against varied spoofing attacks and identify the spoof attackers and improve the performance and easy to detect.

### C. Unconstrained face recognition: identifying a person of interest from a media collection

The use of commercial off the shelf faces recognition systems with respect to the aforementioned challenges in large scale unconstrained face recognition scenarios. First the efficiency of forensic identification is explored by combining two public domain unconstrained face databases. Labeled Faces in the Wild (LFW) and You Tube Faces (YTF) to create



sets of multiple probe images and videos to be matched against a gallery consisting of a single image for each subject. Present results for both open set and closed set identifications which are identifying the persons of interest in forensic and watch list scenarios.

To replicate forensic identification scenarios further populate our gallery with one million operational mug shot images from the Pinellas County Sheriff's Office (PCSO) database. To identify a "person of interest," often based on low quality face images and videos. To generate a single candidate list for the person of interest. Effective face quality measures to determine the fusion of information sources will help boost identification accuracy.

#### D. On the effectiveness of local binary patterns in face anti spoofing

Spoofing attack is the action of outwitting a biometric sensor by presenting a counterfeit biometric evidence of a valid user. It is a direct attack to the sensor input of a biometric system and the attacker does not need the previous knowledge about the recognition algorithm. Most of the biometric modalities are not resistant to spoofing attacks. The biometric systems are usually designed to only recognize identities without concern whether the identity is live or not. A novel publicly available database are called REPLAY ATTACK with three types of attacks and accompanied by a protocol and a baseline study of its effectiveness by passing biometric recognition systems. The limited number of identities is the provision of still images instead of videos which makes its unusable for motion based algorithms.

The strength of texture features based on Local Binary Patterns (LBP) to discriminate between real access and a spoof attack. The support of the idea for reproducible research the database is freely available for public use the method is simple and easy to re implement. Address the problem of detecting face spoofing attacks. Analyze the potential of texture features based on Local Binary Patterns.

#### E. Face liveness detection learning by multi spectral face reflectance distributions

A novel liveness detection method using multi spectral lighting and analyzing the fake faces multi spectrally based on the lambertian model when the user system distance is unlimited and variable. After measuring the curves of different materials two discriminative wave lengths are selected. A device is built to capture multi spectral data of the face to be recognized and classifier is trained on the multi distance reflectance data set for the final liveness detection.

The main disadvantage is user unfriendly. Propose a distance robust face liveness detection method, which performs better than previous works. Discriminative wavelengths are selected to build our multispectral system.

### III. PROPOSED DESIGN

Biometrics is an emerging technology that enables uniquely recognizing humans based upon one or more intrinsic physiological or behavioral characteristics. The spoofing attack is still a fatal threat for biometric

authentication systems. Liveness detection, which aims at recognition of human physiological activities as the liveness indicator to prevent spoofing attack is becoming a very active topic in field of face recognition. The human is able to distinguish a live face and a photograph without any effort since human can very easily recognize many physiological clues of liveness for example facial expression variation, mouth movement, head rotation, eye change. The tasks of computing these clues are often complicated for computer even impossible for some clues under the unconstrained environment. IDA includes specular reflection, blurriness, chromatic moment, and color diversity. Specular reflection features analyze illumination of the images. The blurriness is measured based on the difference between the original input image and its blurred version. It 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. Finally analyzed color reproduction loss in input images. Feature vectors are then fed into multiple SVM classifiers.

The proposed scheme is to achieve a more stable face spoof detection performance.

#### Advantages

- It is easy to find out real and fake users because fake identities always have some different features.
- Image distortion approaches which have been consistently tested showing good performance for different applications.

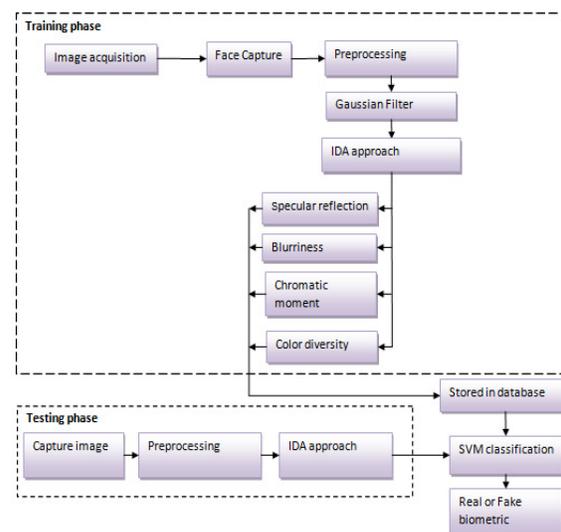


Fig 1 System Architecture

#### A. Module Description Modules

- Image acquisition
- Preprocessing
- Features construction
- Classification



- Alert system

### 1. IMAGE ACQUISITION

The upload images from users. Face images from user through web cameras and using face detection which is a computer technology that determines the locations and sizes of human faces in digital images. It detects face and ignores anything else, such as buildings, trees and bodies. Face detection can be regarded as more general case of face localization. Face localization, the task is to find the locations and sizes of a known number of faces (usually one). Face detection, face is processed and matched bitwise with the underlying face image in the database.

### 2. PREPROCESSING

Normalizing the intensity of the individual particles images removing reflections. Image preprocessing is the technique of enhancing data images prior to computational processing. The module implement Gaussian filter to remove noise from images. Gaussian filters have the properties of having no overshoot to a step function input while minimizing the rise and fall time. The behavior is closely connected to the fact that the Gaussian filter has the minimum possible group delay.

### 3. FEATURES CONSTRUCTION

Image distortion analysis can be implemented for extracting features like image features. These features are

- Specular reflection
- Blurriness
- Chromatic features
- Color diversity

**a. Specular Reflection Features:** Calculate diffusion component of image and subtract diffusion from original image to get specular reflection.

**b. Blurriness features:** Blurriness is measured based on the average edge width in the input image.

**c. Chromatic features:** 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

**d. Color diversity features:** The histogram bin counts of the top 100 most frequently appearing colors the number of distinct colors appearing in the normalized face image.

### 4. IMAGE CLASSIFICATION

It performs the face recognition. Face recognition is a K class problem where K is the number of known individuals and support vector machines (SVMs) are a binary classification method. By reformulating the face recognition problem and reinterpreting the output of the SVM classifier. The SVM based face recognition algorithm. The face recognition problem is formulated as a problem in difference space.

### 5. ALERT SYSTEM

Create the alert system for unauthorized access. The alert is

send to users through mobile phones. And we evaluate performance of the system using rate based on false rejection rate and false acceptance rate.

## IV. EXPERIMENTAL ANALYSIS

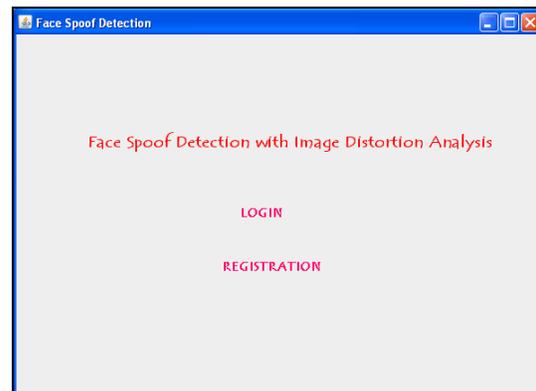


Fig 2 Face Spoof Detection

Fig 3 Registration

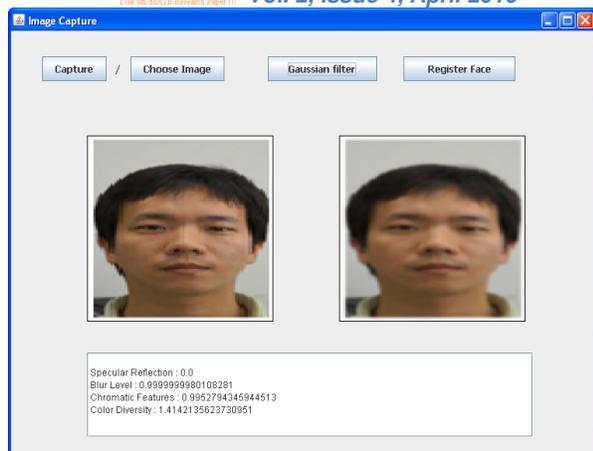


Fig 4 Image Capture

## V. CONCLUSION

To provide the anti spoofing approach for implements the IDA and SVM classification algorithms. To overcome the printed attacks with improved accuracy rate and extensive experiments on real time database containing several real and fake faces showed excellent results. Compared to many previous works, our proposed approach is robust, computationally fast and does not require user cooperation. In future extend our approach to implement this concept in multimodal biometrics that includes iris and finger print images with face images and implementation image quality assessments techniques to improve the performance of the system with efficient accuracy rate.

## REFERENCES

- [1] Anjos. A, Chingovska. I and Marcel. S, (2012), "On the effectiveness of local binary patterns in face anti spoofing" in Proc. IEEE BIOSIG, pp. 1–7.
- [2] Anjos. A, de Freitas Pereira. T, De Martino. J, Marcel. S, (2013), "Can face anti spoofing counter measures work in a real world scenario?" in Proc. ICB, pp. 1–8.
- [3] Angelopoulou. E, Christlein. V, Evangelopoulos. G, Kakadiaris. I, Riess. C, (2013), "The impact of specular highlights on 3D 2D face recognition" in Proc. SPIE.
- [4] Anjos. A, De Martino. J, de Freitas Pereira. T, Hadid. A, Komulainen. J, Marcel. S, Pietikäinen. M, (2014), "Face liveness detection using dynamic texture" EURASIP Journal on Image and Video Processing, vol. no. 2.
- [5] Bharadwaj. T, Dhamecha. I, Singh. R, Vatsa. M, (2013), "Computationally efficient facespoofing detection with motion magnification," in Proc. CVPR Workshops, pp. 105–110.
- [6] Chen. X, Gao. W, Han. H, Lao. S, Shan. S, (2012), "Separability oriented preprocessing for illumination insensitive face recognition" in Proc. ECCV, pp. 307–320.
- [7] Evans. N, Kinnunen. T and Yamagishi. J, (2013), "Spoofing and counter measures for automatic speaker verification," in Proc. Interspeech, pp. 925–929.
- [8] Erdogmus. N and Marcel. S, (2013), "Spoofing in 2D face recognition with 3D masks and anti spoofing with kinect," in Proc. IEEE Btas, pp. 1–6.
- [9] Fierrez. J, Galbally. J, Marcel. S, (2014), "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.
- [10] Hou. C., Nie. F, Wu. Y, Yi. D, Zhang. C, (2014), "Multiple rank multi linear SVM for matrix data classification" Pattern Recognition, vol. 47, no. 1, pp. 454–469.
- [11] Huang. H, Huang. Y, Nie. F, Wang. Y, (2014), "New primal SVM solver with linear computational cost for big data classifications" in Proc. ICML.
- [12] Hadid. A, Komulainen. J and Pietikäinen. M, (2013), "Context based Face Anti Spoofing" in Proc. BTAS, pp. 1–8.
- [13] Li. S, Yang. J, (2013), "Face Liveness Detection with Component Dependent Descriptor" in Proc. IJCB, pp. 1–6.