ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.1

Techniques and Implementation of Face Spoof Recognition: Perspectives and Prospects

Priyanka P. Raut[1], Namrata R. Borkar[2]
ME Student[1], Assistant Professsor[2]
Department of Computer Science and Engineering
Dr. Sau. Kamlatai Gawai Institute of Engineering and Technology, Darapur, MS, India

Abstract:
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). 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 is used to distinguish between genuine (live) and spoof faces. The proposed approach is extended to multiframe face spoof detection in videos using a voting-based scheme. We also collect a face spoof database, MSU mobile face spoofing database (MSU MFSD).

Keywords: Face recognition, spoof detection, image distortion analysis, ensemble classifier, cross-database, cross-device.

I. INTRODUCTION

As face recognition applications progress from constrained imaging and cooperative subjects (e.g., identity card reduplication) to unconstrained imaging scenarios with uncooperative subjects (e.g., watch list monitoring), a lack of guidance exists with respect to optimal approaches for integrating face recognition algorithms into large-scale applications of interest. In this work we explore the problem of identifying a person of interest given a variety of information source about the person (face image, surveillance video, face sketch, 3D face model and demographic information) in both closed set and open set identification modes. Spoofing attacks upon face recognition systems involve presenting artificial facial replicas of authorized users to falsely infer their presence in order to bypass the biometric security measures. Such attacks can be carried out easily by means of printed photographs or digital images displayed on tablet, smart phones, etc. In order to distinguish real face features from fake faces, face liveness detection is a commonly used countermeasure approach. 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 finger print 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 [1], [2], we need to address concerns about face spoof attacks on face recognition systems, particularly in unconstrained sensing and uncooperative subject scenarios [3]. 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 (see Fig. 1). State of the art Commercial Off-The-Shelf (COTS) face recognition systems are not well designed to differentiate spoof faces from genuine live faces. Identification performance of a COTS face recognition system (COTS11) when spoof faces as probe are matched to genuine faces in the gallery. In this experiment, more than 70% of probe videos (spoof faces) were successfully matched to the gallery mates by COTS1 at rank-1, indicating that COTS1 cannot effectively distinguish between genuine and spoof faces.

Figure.1. A genuine face image (a) of a subject in the Idiap databases [4], [5]and three examples of spoofs of the same subject using a (b) printed photo,(c) displayed photo (on a tablet screen).

The fragility of face recognition systems to face spoof attacks has motivated a number of studies on face spoof detection [4], [7]–[12]. 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.

II. FACE SPOOFING

Biometrics alludes to technologies that measure and analyze human body characteristics. Biometrics traits will be

categorized into 2 categories, specifically physical characteristics, for instance, fingerprints, faces or iris patterns and activity characteristics, for instance, voice, signature or strolling patterns (step). Be that because it might, a standout amongst the foremost predominant challenges in varied biometric recognition systems is that the chance of fraud, that is fairly referred to as spoofing attack. Some purloined stolen data will be effectively exploited and mimicked by impostors to realize unauthorized access to the biometric system, while not the consent of the real user. Examine endeavors on identification of spoofing attack are created mistreatment totally different views [9]. The progressive spoofing identification technique for facial statistics in lightweight of physiological property detection is bestowed during a portion of the work. Generally, false faces will be categorized into 2 classes: positive and negative. The positive category, otherwise referred to as the real face, has restricted variation, although the negative category incorporates the spoof faces on pictures, dummy or recorded videos.

III. LITERATURE REVIEW & RELATED WORK

To our knowledge, one of the earliest studies on face spoof detection was reported in 2004 by Li et al. [13]. With the growing popularity of using face recognition for access control, this topic has attracted significant attention over the past five years [4], [7]–[12]. One of the major focus of the FP7 EU funded project, TABULA RASA [14], 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) real-time response and usability. According to different types of cues used in face spoof detection, published methods can be categorized into four groups: (i) *motion based methods*, (iii) *texture based methods*, (iii) *method based on image quality analysis*, and (iv) *methods based on other cues*.

(i) *Motion Based Methods:*

These methods, designed primarily to counter printed photo attacks, capture a very important cue for vitality: the subconscious motion of organs and muscles in a live face, such as eye blink [10], mouth movement [15] and head rotation [11]. Given that 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. However, the limitations of motion based methods are apparent. The frequency of facial motion is restricted by the human physiological rhythm, which ranges from 0.2 to 0.5 Hz [12]. Therefore, it takes a relatively long time (usually >3s) to accumulate stable vitality features for face spoof detection. Additionally, motion based methods can be easily circumvented or confused by other motions, e.g., background motion, that are irrelevant to facial liveness or replayed motion in the video attacks.

(ii) *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. In [18], the authors argued that texture features (like LBP, DoG, or HOG) are capable of differentiating artifacts in spoof faces from the genuine faces. Texture based methods have achieved significant success on the Idiap and CASIA databases. The Half Total Error Rate (HTER)5 on the Idiap database was reduced from 13.87% in [4] and 7.60% in [16] to 6.62% in [12] by incorporating texture cues. Unlike motion based methods, texture based methods need only a single image to detect a spoof. However, the generalization ability of many texture based methods has been found to be poor. A study reported in [17] showed that for two of the texture based methods (proposed in [4] and [16]), the HTER increased dramatically under the cross-database scenarios (where the training and testing sets came from different face spoof databases). 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.

Table. 1. A Comparison of Different Face Spoof Detection Methods

Method	Strengths	Limitations	State-of-the-art performance
Motion based methods [10]–[12], [15]	• Good generalization ability	• Low robustness (can be circumvented by fake motion) • Slow response (> 3s) • High computational complexity (image registration needed)	*Intra-DB* [12]: HTER = 1.25% for Idiap REPLAY-ATTACK
Texture based methods [4], [8], [12], [16]–[18]	• Fast response (< 1s) • Low computational complexity	• Poor generalization ability (vulnerable to the variations in acquisition conditions)	*Intra-DB* [16]: HTER = 7.60% for Idiap REPLAY-ATTACK *Intra-DB* [18]: EER = 11.8% for CASIA FASD *Intra-DB* [12]: HTER = 6.62% for Idiap REPLAY-ATTACK
Methods based on other cues [6], [19]–[21]	• High robustness	• Additional sensing or processing technique needed (IR, audio, 3D, etc.) • Slow response (> 3s) when using audio and 3D cues	Intra-DB [21]: EER = 8.06% for VidTIMIT EER = 9.23% for DaFEx
Image quality analysis based methods [22], and the proposed method	• Good generalization ability • Fast response (< 1s) • Low computational complexity	• Different classifiers needed for different spoof attacks	*Intra-DB*: TPR = 92.2% @ FAR = 10% for Idiap REPLAY-ATTACK *Cross-DB*: TPR = 75.5% @ FAR = 10% for MSU MFSD

(iii) *Image Quality Analysis Based Methods:*

A recent work [22] 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 [22], our work is different in the following aspects: (1) While 25 features are required in [22] to get good results, no face-specific information has been considered in designing informative features for face spoof detection. On the contrary, four features are designed specifically for face feature representation in our method, and we demonstrate the effectiveness of these features for spoof face detection. (2) While the authors of [22] evaluated their method on *only* the Idiap-Replay database, we have used both the Idiap and CASIA databases, which are two important public-domain databases. (3) While the work in [22] 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 scenarios (same database for training and testing, even though cross-validation is used). By contrast, the proposed approach aims to improve the generalization ability under cross-database scenarios, which has seldom been explored in the biometrics community.

(iv) *Methods Based on Other Cues:*

Face spoof countermeasures using cues derived from sources other than 2D intensity image, such as 3D depth [19], IR image [6], spoofing context [20], and voice [21] have also been proposed. However, these methods impose extra requirements on the user or the face recognition system, and hence have a narrower application range. For example, an IR sensor was required in [6], a microphone and speech analyzer was required in [21], and multiple face images taken from different viewpoints were required in [19]. Additionally, the spoofing context method proposed in [20] can be circumvented by concealing the spoofing medium. Table I compares these four

types of spoof detection methods. These four types of methods can also be combined to utilize multiple cues for face spoof detection. For example, in [12], the authors showed that appropriately magnified motion cue [23] improves the performance of texture based approaches (HTER = 6.62% on the Idiap database with motion magnification compared to HTER = 11.75% without motion magnification, both using LBP features). The authors also showed that combining the Histogram of Oriented Optical Flow (HOOF) feature with motion magnification achieved the best performance on the Idiap database (HTER = 1.25%). However, motion magnification, limited by human physiological rhythm, cannot reach the reported performance [12] without accumulating a large number of video frames (>200 frames), making these methods unsuitable for real-time response. Though a number of face spoof detection methods have been reported, to our knowledge, none of them generalizes well to cross-database scenarios [17]. In particular, there is a lack of investigation on how face spoof detection methods perform in cross-database scenarios. The fundamental differences between intra-database and cross-database scenarios are as follows:

i) In an intra-database scenario, it is assumed that the spoof media (e.g., photo and screen display), camera, environmental factors, and even the subjects are known to a face liveness detection system. This assumption does not hold in most of the real scenarios. The intra-database performance of a face liveness detection system is only the upper bound in terms of performance that cannot be expected in real applications.

ii) In cross-database scenario, we permit differences of spoof media, cameras, environments, and subjects during the system development stage and the system deployment stage. Hence this cross-database performance better reflects the actual performance of a system that can be expected in real applications.

iii) 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.

1) Features Derived From Image Distortion Analysis

The classifier outputs are fused to give the final binary decision (ensemble classification): genuine or spoof face.

A. Specular Reflection Features

Specular reflection component image has been widely used for specular reflection removal [27] and face illumination normalization [28]. In this paper, we separate the specular reflection component *Is* from an input face image or video frame utilizing an iterative method (with 6 iterations) proposed in [29], which assumes that the illumination is i) from a single source, ii) of uniform color, and iii) not over-saturated. Given that most of the face images (in the Idiap, CASIA, and MSU databases) are captured indoors under relatively controlled illumination, these three assumptions are reasonable. Figures 2 (a, b) illustrate the difference between the specular reflection components extracted from a genuine face and the corresponding spoof face. After calculating the specular reflection component image *Is*, we represent the specularity intensity distribution with three dimensional features: i) specular pixel percentage *r*, ii) mean intensity of specular pixels μ, and iii) variance of specular pixel intensities σ. However, as argued in [32], the method in [29] extracts specular components based on chromatic difference analysis, which often incorrectly classifies the mono-chromatic regions as specular components. To correct such errors, we exclude the high-intensity mono-chromatic pixels in *Is*from specular components (as in [32]). Specifically, only pixels in the intensity range $(1.5\mu, 4\mu)$ are counted as specular pixels. Figures 2 (a-d) show the three dimensional specular reflection features calculated for a genuine and a spoof face of a subject in the MSU database. Figures 2 (e-g) visualize the 3D distributions of the specular reflection features of genuine and spoof faces in the Idiap training, Idiap testing and MSU testing datasets. These distributions suggest that using the specular reflection feature, a classifier trained on the Idiap training set can achieve good performance on both the Idiap and MSU testing sets.

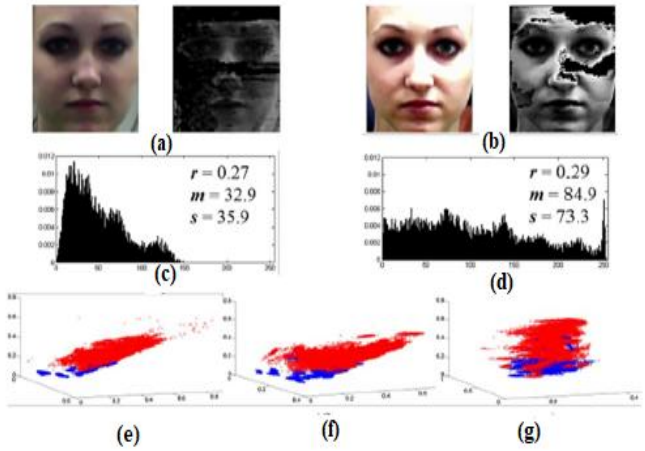


Figure.2. Illustration of specular reflection features. (a) A genuine face image and the detected specular reflection component; (b) A spoof face (replayed video) and the detected specular reflection component;(c-d) histograms and specific feature values of the specular reflection components in (a) and (b), respectively; (e-g) distributions of the three specula reflection features (blue: genuine samples, red: spoof samples) in the Idiap training, Idiap testing, and MSU testing sets, respectively.

B. 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 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. We utilize two types of blurriness features (denoted as *b*1 and *b*2) that were proposed in [33] and [34], respectively. In [33], blurriness is measured based on the difference between the original input image and its blurred version. The larger the difference, the lower the blurriness in the original image. In [34], blurriness is measured

based on the average edge width in the input image. Both these two methods output non-reference (without a clear image as reference) blurriness score between 0 ~1, but emphasizing different measures of blurriness.

C. Chromatic Moment Features

Recaptured face images tend to show a different color distribution compared to colors in the genuine face images. This is caused by the imperfect color reproduction property of printing and display media. This chromatic degradation was explored in [35] 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. 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 5 × 3 = 15. Figure 3 illustrates the presence of color distortion in a spoof face.

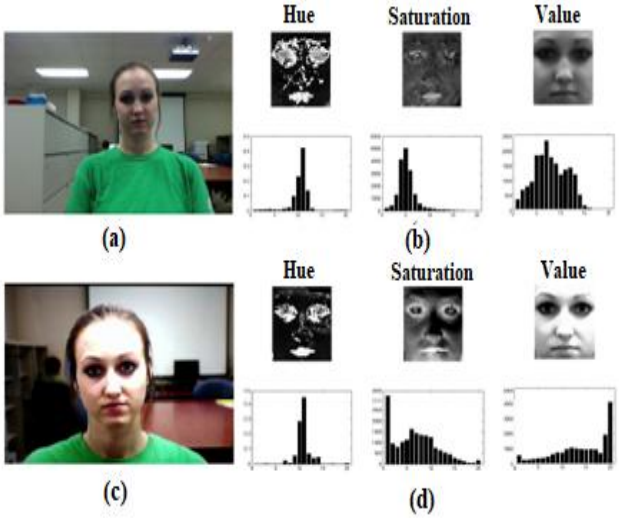


Figure.3. Examples of chromatic difference between a genuine face and a spoof face. (A) and (c): The genuine face and spoof face images; (b) and (d): Hue, Saturation, and Value component images (top row) and their histograms (bottom row). The abnormality of the histogram for the spoof face can be measured by the three chromatic moments.

D. Color Diversity Features

Another important difference between genuine and spoof faces is the color diversity. In particular, genuine faces tend to have richer colors. This diversity tends to fade out in spoof faces due to the color reproduction loss during image/video recapture. In this paper, we follow the method used in [35] to measure the image color diversity. First, color quantization (with 32 steps in the red, green and blue channels, respectively) is performed on the normalized face image. Two measurements are then pooled from the color distribution: i) the histogram bin counts of the top 100 most frequently appearing colors, and ii) the number of distinct colors appearing in the normalized face image. The dimensionality of the color diversity feature vector is 101. The above four types of feature (specular reflection, blurriness, chromatic moment, and color diversity) are finally concatenated together, resulting in an IDA feature vector with 121 dimensions. Although the IDA feature vector is extracted from the facial region, it contains only image distortion information, and not any characterization of facial appearance. Therefore, we expect that the IDA feature can alleviate the problem of training bias encountered in the commonly used texture features.

2) Classification Method

A. Ensemble Classifier

Given that our aim is to design an efficient face spoof detection system with good generalization ability and quick response, it is desirable to have an efficient classifier for the extracted IDA features. Following the success of SVM [36] in signal processing [37], pattern recognition and classification applications [38], [39], we choose to use SVM via the Lib SVM Library [40]. There are also a number of variations of SVM for handling large-scale classification problems, such as LIBLINEAR [41] and ALM-SVM [42]; however, most of the public-domain face spoof databases (including the databases used in our experiments) are of limited size in terms of the number of still images, video tracks, and subjects. A SVM classifier with RBF kernel is trained for each group of training data, with parameters optimized by cross-validation. On the other hand, it is understood that different spoof attacks will have different sample distributions in the IDA feature space. For example, while the printed attack samples tend to have lower contrast than the genuine samples, the replay attack samples tend to have higher contrast. Different types of attacks might also have different chromatic distortion characteristics. Therefore, instead of training a single binary classifier, an ensemble classifier is more appropriate to cover various spoof attacks. For a specific spoof database, we construct separate groups of training samples as follows: First, the spoof samples are divided into *K* groups according to the attack type. Second, a specific training set is constructed by combining all genuine samples and a single group of spoof samples, resulting in *K* training sets. In our experiments, we find that by training two constituent classifiers (K = 2) on two groups of spoof attacks separately, i.e., printed attack and replay attack, the ensemble classifier performs better than training a single classifier on the whole database.

B. Multi-Frame Fusion

Given the face spoof detection classifier working on a single image, a multi-frame fusion scheme is proposed to achieve a more stable face spoof detection performance for a video. The classification results from individual frames are combined by a voting scheme to obtain the spoof detection score for a video. A face video is determined to be genuine if over 50% of its frames are classified as genuine face images. Since some published methods report per video face spoof detection performance using *N* frames, the multi-frame fusion extension allows us to compare the proposed method's performance with state-of-the-art given the same length of testing videos.

3. Face Spoof Databases

A. Public Domain Face Spoof Databases

To evaluate the effectiveness of spoof detection algorithms, many published papers designed and tested their algorithms on proprietary spoof databases [6], [10], [11], [19]. However, only a few authors have made their face spoof databases publicly available [4], [7]–[9], [44], [45]. In this section, we provide a brief summary of three public-domain face spoof databases: NUAA Photograph Imposter database [8], Idiap REPLAY-

ATTACK database [4] and CASIA Face Anti-Spoofing Database [9]. There are a couple of other public-domain databases for face spoof detection. For example, the VidTIMIT Audio-Video database (43 subjects) [44] and the DaFEx database (8 subjects) [45] have also been used for the purpose of face spoof detection, but their limited size and spoofing diversity makes them less attractive for use in experimental evaluations. The NUAA Photograph Imposter database [8], released in 2010, is one of the earliest public-domain spoof databases. It consists of 12,614 images (extracted from 143 videos) of genuine and attack attempts of only 15 subjects. Additionally, only hand-held printed photo attack is included in the NUAA database. The Idiap REPLAY-ATTACK database [4], released in 2012, consists of 1,300 video recordings of both real access and attack attempts of 50 different subjects.8 In the same acquisition condition (controlled and adverse illumination), the face spoof attacks were generated by forging live verification attempts of the same subjects via printed photos, displayed photos/videos on mobile phone's screen, and displayed photos/videos on HD screen. The CASIA Face Anti-Spoofing Database (FASD) [9], released in 2012, consists of 600 video recordings of genuine and attack attempts of 50 different identities. Although the size of the CASIA database is somewhat smaller than the Idiap database, it contains more diverse samples in terms of the acquisition devices (high resolution Sony NEX-5 camera and low-quality USB camera),face variations (pose and expression variations), and attack attempts (warp photo, cut photo, and HD displayed video).

Table.2. A Summary of Three Spoof Face Databases in Public-Domain and the MSU MFSD Database

Database	Year of release	# subjects	# videos	Acquisition camera device	Attack type	Subject race	Subject gender	Subject age
NUAA [8]	2010	15	• 24 genuine • 33 spoof	• Web-cam (640 × 480)	• Printed photo	• Asian 100%	• Male 80% • Female 20%	20 to 30 yrs
Idiap REPLAY-ATTACK [4]	2012	50	• 200 genuine • 1,000 spoof	• MacBook 13″ camera (320 × 240)	• Printed photo • Display photo (mobile/HD) • Replayed video (mobile/HD)	• White 76% • Asian 22% • Black 2%	• Male 86% • Female 14%	20 to 40 yrs
CASIA FASD [9]	2012	50	• 150 genuine • 450 spoof	• Low-quality camera (640 × 480) • Normal-quality camera (480 × 640) • Sony NEX-5 camera (1280 × 720)	• Printed photo • Cut photo‡ • Replayed video (HD)	• Asian 100%	• Male 86% • Female 14%	20 to 35 yrs
MSU MFSD	2014	55†	• 110 genuine • 330 spoof	• MacBook Air 13″ camera (640 × 480) • Google Nexus 5 camera (720 × 480)	• Printed photo • Replayed video (mobile/HD)	• White 70% • Asian 28% • Black 2%	• Male 63% • Female 37%	20 to 60 yrs

Table II provides a summary of the above three databases in terms of sample size, acquisition device, attack type, and age, gender and race distributions of subjects. A major drawback of these three spoof databases is that they were all captured by web cameras or high quality digital cameras. There is no public-domain face spoof database using mobile phone cameras as capturing devices. The mobile phone front facing cameras pose the following additional challenges for face spoof detection: i) They usually have lower resolution, narrow dynamic range, and in accurate metering and auto-focus capabilities. As a result, videos or images captured by these cameras typically have low quality due to defocus, under or over exposure. Since these image quality degradations appear in both genuine and spoof face images, they will diminish the differences between genuine and spoof face images in terms of facial detail and image distortion. ii) The purpose of building a mobile phone face spoof database is not simply to make the face spoof detection task more difficult, but to better replicate a realistic scenario. Another noticeable property of these databases is the standoff distance used in launching the spoof attacks. In the Idiap database, the attacker presented the spoof medium fairly close to the camera (short distance spoofing attack), resulting in a relatively large facial area in the spoof video. In the CASIA database, the spoof attacks were generated with a larger standoff [46] (long distance spoofing attack), resulting in a smaller facial area and lower contrast in the spoof attacks.

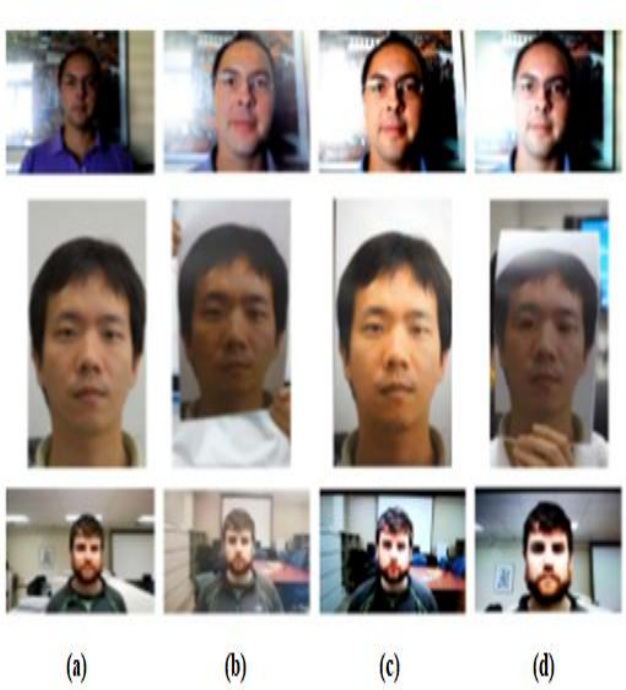


Figure. 4. Typical face samples from the Idiap (first row), CASIA H subset (second row) and MSU (third row) spoofing databases. (a) Genuine face images; (b) Spoof faces generated for printed photo attack; (c) Spoof faces generated by HD tablet screen; (d) Spoof faces generated by mobile phone screen (first and third row) or cut photo (second row).

Figure 04 shows the short distance spoofing attacks and gives MSU Mobile Face Spoofing Database (MSU MFSD) to facilitate spoof detection research on mobile phone applications.

B. MSU MFSD Database

The MSU MFSD database consists of 440 video clips of photo and video attack attempts of 55 subjects. Two types of cameras were used in collecting this database:

1) Built-in camera in laptop

2) Front-facing camera in the mobile phone. Both these devices are the state of the art models.

***1) Genuine Face*:** The (true) subject presents his face close to the camera, and a genuine face video is recorded using both the Android and laptop cameras. The average standoff distance between the face and the camera is ~50cm.

***2) Spoof Attack Video Replay*:** The video of the subject's Face is rest recorded using a camera. The camera also is used to capture a HD video (1920×1088), which is replayed on screen to generate the HD video replay attack. The mobile is used to capture another HD video (1920×1080) that is replayed on mobile screen to generate the mobile video replay

attack. The average standoff for the HDvideo replay attack is ~20cm. The average standoff for the mobile video replay attack is ~10cm. In table 03 various techniques of spoof detection has been reviewed in terms of description and outcome.

Table. 3. Table of Comparison [47]

Author	Year	Description	Outcomes
R.Tan	2005	Color chromaticity based method	Accurate, robust
K. Kollreider	2007	Motion based method	Good generalization ability
W.Bao	2009	To distinguish between 2d and 3d images for face detection	Feasible, effective
N.Kose	2012	To contrast between captured and recaptured images	Non intrusive and Simple
T. de Freitas Pereira	2012	Texture based method	Fast response (< 1s) Low computational Complexity
J.Yang	2013	Face Liveness Detection method	Best performance for liveness detection
J. Galbally	2014	Image quality analysis based methods to detect fake faces	Good generalization ability,Low degree of complexity
Di Wen, Hu Han	2015	Feature extraction based method	Good generalization ability Fast response (< 1s) Low computational complexity

IV. PROBLEMANALYSIS

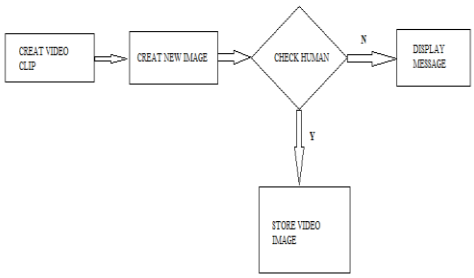
Traditional face matching methods take single media (i.e., a still face image, video track, or face sketch) as input, our work considers using the entire gamut of media collection as a probe to generate a single candidate list for the person of interest. Automatic face recognition is now widely used in applications ranging from deduplication 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.

V. PROPOSED SYSTEM

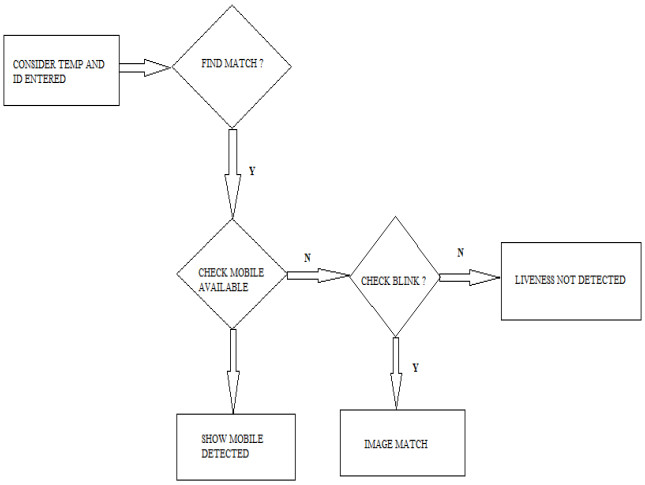
In this work proposed approach boosts the likelihood of correctly identifying the person of interest through the use of different schemes video frame selection. An efficient and rather robust face spoof detection algorithm proposed in this work is based on image distortion analysis (IDA). Four different features (specular reflection, blurriness, chromatic moment, and color diversity) are extracted to form the IDA feature vector. In this work also collect a face spoof database, MSU mobile face spoofing database (MSU MFSD), with spoof attacks for replayed video i. e. mobile. Our propose results also highlight the difficulty in separating genuine and spoof faces, especially in cross-database and cross-device scenarios. The proposed method has the ability to perform consistently at different biometric traits (multi biometric). The proposed methods provide a high level of protection from different types of attacks (multi attack). The error rates are very low when compared to other anti-spoofing attacks; Due to the multi biometrics and multi attack characteristics, the proposed method is fast, user-friendly and effective.

Flow chart of proposed system:

i) Check Temp ID Authentication:



ii) Check Authentication:



VI. RESULTS AND DISCUSSION

In this work collecting a face spoof database, MSU mobile face spoofing database (MSU MFSD), with spoof attacks for replayed video i. e. mobile. Most of the published methods use motion or texture based features, this work proposes to perform face spoof detection based on Image Distortion Analysis (IDA). Four different features (specular reflection, blurriness, chromatic moment, and color diversity) are extracted to form the IDA feature vector. This work proposed to use of Matlab as front end and back end to approach boosts the likelihood of correctly identifying the person of interest through the use of different fusion schemes incorporation ofquality measures for fusion and video frame selection.

VII. CONCLUSION

In this work, it is been concluded that face spoof detection is the technique which is been applied to improve security of the bio-metric system Anti-spoofing is becoming a vital issue in biometric authentication systems. It is highly critical for a system to correctly discover and prevent attackers especially with the diverse variation of attacks. In this work, a face spoof detection method based on Image Distortion Analysis (IDA) is proposed.

VIII. REFERENCES

[1]. A. Rattani, N. Poh, and A. Ross, "Analysis of user-specific score characteristics for spoof biometric attacks," in Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), Jun. 2012, pp. 124–129.

[2]. Z. Wu, N. Evans, T. Kinnunen, J. Yamagishi, F. Alegre, and H. Li, "Spoofing and countermeasures for speaker

verification: A survey," Speech Commun., vol. 66, pp. 130–153, Feb. 2015.

[3]. L. Best-Rowden, H. Han, C. Otto, B. F. 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, Sep. 2012, pp. 1–7.

[5]. N. Erdogmus and S. Marcel, "Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect," in Proc. IEEE BTAS, Sep./Oct. 2013, pp. 1–6.

[6]. Z. Zhang, D. Yi, Z. Lei, and S. Z. Li, "Face liveness detection by learning multispectral reflectance distributions," in Proc. FG, Mar. 2011, pp. 436–441.

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

[8]. 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. ECCV, Sep. 2010, pp. 504–517.

[9]. Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face antispoofing database with diverse attacks," in Proc. ICB, Mar./Apr. 2012, pp. 26–31.

[10]. L. Sun, G. Pan, Z. Wu, and S. Lao, "Blinking-based live face detection using conditional random fields," in Proc. AIB, 2007, pp. 252–260.

[11]. W. Bao, H. Li, N. Li, and W. Jiang, "A liveness detection method for face recognition based on optical flow field," in Proc. IASP, Apr. 2009, pp. 233–236.

[12]. 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 (CVPRW), Jun. 2013, pp. 105–110.

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

[14]. The TABULA RASA Project. [Online]. Available: http://www.tabularasa -euproject.org/, acccessed Sep. 2014.

[15]. 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. 2007.

[16]. T. de Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel, "LBP–TOP based countermeasure against face spoofing attacks," in Proc. ACCV Workshops, 2012, pp. 121–132.

[17] 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. ICB, Jun. 2013, pp. 1–8.

[18]. J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection with component dependent descriptor," in Proc. IJCB, Jun. 2013, pp. 1–6.

[19]. T. Wang, J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection using 3D structure recovered from a single camera," in Proc. ICB, Jun. 2013, pp. 1–6.

[20]. J. Komulainen, A. Hadid, and M. Pietikäinen, "Context based face antispoofing," in Proc. BTAS, Sep./Oct. 2013, pp. 1–8.

[21]. G. Chetty, "Biometric liveness checking using multimodal fuzzy fusion," in Proc. IEEE FUZZ, Jul. 2010, pp. 1–8.

[22]. 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.

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

[24]. S. A. Shafer, "Using color to separate reflection components," Color Res. Appl., vol. 10, no. 4, pp. 210–218, 1985.

[25]. O. Bimber and D. Iwai, "Superimposing dynamic range," in Proc. ACM SIGGRAPH Asia, 2008, pp. 1–8, no. 150.

[26]. PittPatt Software Developer Kit.Pittsburgh Pattern Recognition PittPatt.[Online]. Available: http://www.pittpatt.com/, accessed Jan. 2011.

[27]. Q. Yang, S. Wang, and N. Ahuja, "Real-time specular highlight removal using bilateral filtering," in Proc. ECCV, 2010, pp. 87–100.

[28]. V. Christlein, C. Riess, E. Angelopoulou, G. Evangelopoulos, and I. Kakadiaris, "The impact of specular highlights on 3D-2D face recognition," Proc. SPIE, vol. 8712, p. 87120T, May 2013.

[29]. R. T. Tan and K. Ikeuchi, "Separating reflection components of textured surfaces using a single image," IEEE Trans. Pattern Anal. Mach. Intell., vol. 27, no. 2, pp. 178–193, Feb. 2005.

[30]. J.-F.Lalonde, A. A. Efros, and S. G. Narasimhan, "Estimating the natural illumination conditions from a single outdoor image," Int. J. Comput. Vis., vol. 98, no. 2, pp. 123–145, Jun. 2011.

[31]. H. Han, S. Shan, X. Chen, S. Lao, and W. Gao, "Separability oriented preprocessing for illumination-insensitive face recognition," in Proc. ECCV, 2012, pp. 307–320.

[32] X. Gao, T.-T. Ng, B. Qiu, and S.-F. Chang, "Single-view recaptured image detection based on physics-based features," in Proc. ICME, Jul. 2010, pp. 1469–1474.

[33]. 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.

[34]. P. Marziliano, F. Dufaux, S. Winkler, and T. Ebrahimi, "A no-reference perceptual blur metric," in Proc. ICIP, vol. 3.2002, pp. III-57–III-60.

[35]. Y. Chen, Z. Li, M. Li, and W.-Y.Ma, "Automatic classification of photographs and graphics," in Proc. ICME, Jul. 2006, pp. 973–976.

[36]. B. E. Boser, I. M. Guyon, and V. N. Vapnik, "A training algorithm for optimal margin classifiers," in Proc. 5th ACM Workshop Comput. Learn. Theory, 1992, pp. 144–152.

[37]. A. Bashashati, M. Fatourechi, R. K. Ward, and G. E. Birch, "A survey of signal processing algorithms in brain–computer interfaces based on electrical brain signals," J. Neural Eng., vol. 4, no. 2, pp. R32–R57, Mar. 2007.

[38]. C. Hou, F. Nie, C. Zhang, D. Yi, and Y. Wu, "Multiple rank multi-linear SVM for matrix data classification," Pattern Recognit., vol. 47, no. 1, pp. 454–469, Jan. 2014.

[39]. Y. Lin et al., "Large-scale image classification: Fast feature extraction and SVM training," in Proc. IEEE CVPR, Jun. 2011, pp. 1689–1696.

[40]. C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines," ACM Trans. Intell. Syst. Technol., vol. 2, no. 3, pp. 27:1–27:27, May 2011.

[41]. R.-E. Fan, K.-W.Chang, C.-J.Hsieh, X.-R.Wang, and C.-J. Lin, "LIBLINEAR: A library for large linear classification," J. Mach. Learn. Res., vol. 9, pp. 1871–1874, Aug. 2008.

[42]. F. Nie, Y. Huang, X. Wang, and H. Huang, "New primal SVM solver with linear computational cost for big data classifications," in Proc. ICML, 2014, pp. 1–9.

[43]. A. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," Pattern Recognit., vol. 38, no. 12, pp. 2270–2285, Dec. 2005.

[44]. C. Sanderson, Biometric Person Recognition: Face, Speech and Fusion. Saarbrücken, Germany: VDM-Verlag, 2008.

[45]. A. Battocchi and F. Pianesi, "DaFEx: Un database dispersion if accialidinamiche," in Proc. SLI-GSCP Workshop, 2004, pp. 311–324.

[46]. T. de Freitas Pereira et al., "Face liveness detection using dynamic texture," EURASIP J. Image Video Process., vol. 2014, no. 1, p. 2, Jan. 2014.

[47]. RamandeepKaur, P.S. Mann. "Techniques of Face Spoof Detection: A Review" International Journal of Computer Applications (0975 – 8887) Volume 164 – No 1, April 2017.