

# Implementation of Face Spoof Recognition by Using Image Distortion Analysis

Priyanka P. Raut<sup>1</sup>, Namrata R. Borkar<sup>2</sup>, Virendra P. Nikam<sup>3</sup>

<sup>1</sup>ME Student, CSE Department, KGIET, Darapur, M.S., India

<sup>2,3</sup> Assistant Professor, CSE Department, KGIET, Darapur, M.S., India

\*\*\*

**Abstract** - 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. We proposed an efficient and rather robust face spoof detection algorithm based on image distortion analysis (IDA). In this work we proposed Template matching algorithm for face recognition. Here we perform Face recognition by live streaming to improve the performance of the system. Here the image is given as input and facial features like eyes, nose, and mouth are extracted from the image. The proposed algorithm compares input images with stored patterns of face or features and collects the database. In this work we also implemented the detection medium for spoofing which detects the medium used for face spoofing like mobile, printed photo. The Experimental result shows that proposed algorithm gives better result than the existing methods use for face spoof recognition.

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

## 1. INTRODUCTION

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.

Spoof detection (or anti-spoofing) algorithms that generalize well to new imaging conditions and environments.

## 2. LITERATURE REVIEW

According to different types of cues used in face spoof detection, published methods can be categorized into four groups:

### 2.1 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 [3], mouth movement [5] and head rotation [4]. 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 [5]. 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.

### 2.2 Texture Based Methods

To counter both the printed photo and replayed video attacks, texture based methods were proposed to extract image artifacts in spoof face images. In [7], 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) on the Idiap database was reduced from 13.87% in [4] and 7.60% in [6] to 6.62% in [4] 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 [6] showed that for two of the texture based methods (proposed in [1] and [7]), 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.

### 2.3 Image Quality Analysis Based Methods

A recent work [11] 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 [11], our work is different in the following aspects: (1) While 25 features are required in [11] 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 [11] 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 [11] 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.

### 2.4 Methods Based on Other Cues

Face spoof countermeasures using cues derived from sources other than 2D intensity image, such as 3D depth [8], IR image [2], spoofing context [9], and voice [13] 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 [2], a microphone and speech analyzer were required in [10], and multiple face images taken from different viewpoints were required in [8]. Additionally, the spoofing context method proposed in [9] can be circumvented by concealing the spoofing medium. A study reported in [4], the authors showed that appropriately magnified motion cue 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 [4] 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 [6]. In particular, there is a lack of investigation on

how face spoof detection methods perform in cross-database scenarios.

In this [12] the strategy relies exclusively on colors, significantly hue, while not requiring any geometrical parameter information. One in all the fundamental concepts is to match the intensity power differentiation of specular-free pictures and input pictures iteratively. The specular-free image may be a pseudo-code of diffuse elements which will be generated by shifting a pixel's intensity and hue nonlinearly whereas holding its hue. All processes within the methodology square measure done regionally, involving a most of solely 2 pixels. The experimental results on natural pictures show that the planned methodology is correct and robust below renowned scene illumination hue. In contrast to the prevailing ways that use one image, our methodology is effective for rough-textured objects with advanced multicolor scenes.

## 3. PROBLEM DEFINITION

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.

In last few years the research on biometric systems against various types of attacks experienced an important growth. In general visual inspection of an image of a real image and a fake sample of the same image shows that they can be very similar. But, when the images are converted into proper features, some differences between the real and fake images may become evident. These disparity provided by their own optical qualities (absorption, reflection, scattering, refraction), which other materials such as paper, gelatin are artificially manufactured samples do not possess. To design an algorithm which can assess the images or videos by their quality in a perceptually consistent manner is the main goal of image quality assessment.

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.

## 4. Motivation and Objectives

We propose an efficient and rather robust face spoof detection algorithm based on image distortion analysis (IDA).

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. The specific objective of this work is to study the existing techniques for face spoof recognition and implement Template Matching algorithm for face recognition, to recognize spoof faces by live streaming to improve the performance of the system.

### 5. EXPERIMENTAL RESULT

The results have been demonstrated in the form of comparison. After the comparison graphical representation has also been done for a quick analysis of results. All the techniques have been tested for all the assumed standard test images. Different types of results are extracted from Face Recognition Process. Followings are the results.

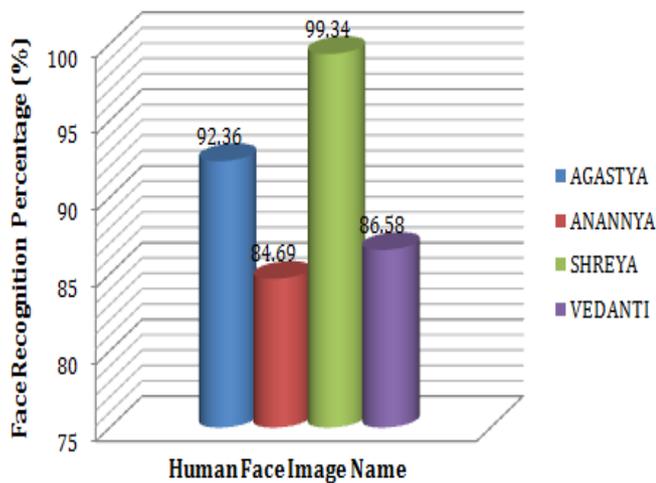


Figure No. 5.1: Face Recognition Percentage graph

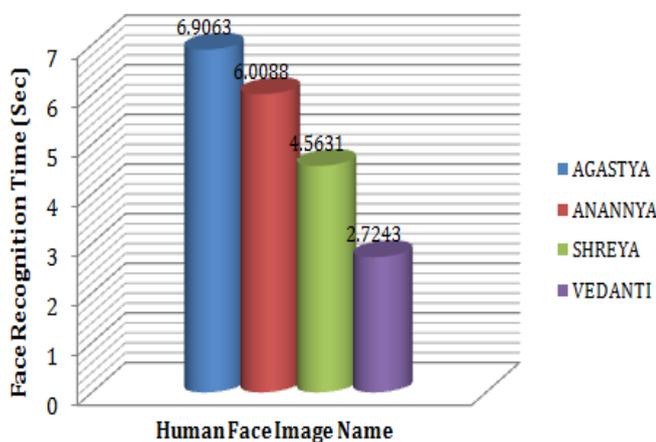


Figure No.5.2: Face Recognition Time graph

Fig No. 5.1 and 5.2 shows the recognized image, Time required for face reognition. Recognition times are specified for each recognized image. With the percentage of Matched image which is stored in database.

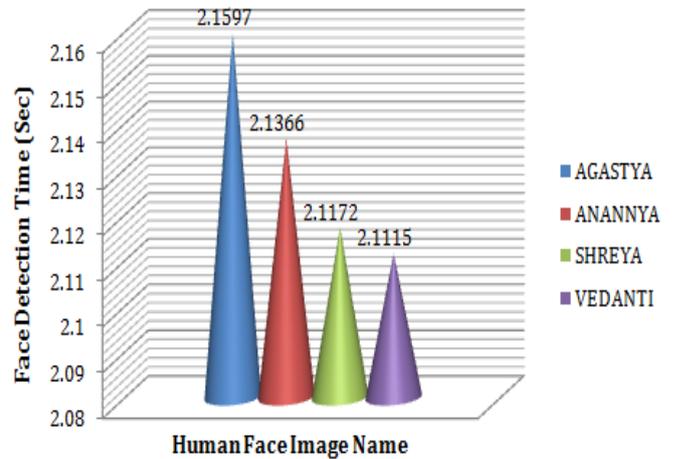


Figure No. 5.3: Face Detection Time graph

Sr. No .	Input Image	Mean of Image	Entrop y of Image	Standar d Deviati on of Image	Dimensi on (HxW)of image	Human Face Detect ed
01	Agasty a	123.48 86	7.5356	46.4056	205x615	YES
02	Anann ya	88.014 2	7.2833	39.5908	171x513	YES
03	Shreya	98.986 1	7.3749	42.6321	148x444	YES
04	Vedant i	100.58 82	7.5287	47.3935	164x492	YES

Table 5.1: Human Face Detection Result.

The Fig. No.5.3 and table 5.1 shows the result of human face detection. It shows four input images and their mean of image, entropy of image, Standard Deviations, Height, and Width. It gives clarification of image containing face is a human face is detected or not. Detection times are specified for each input image.

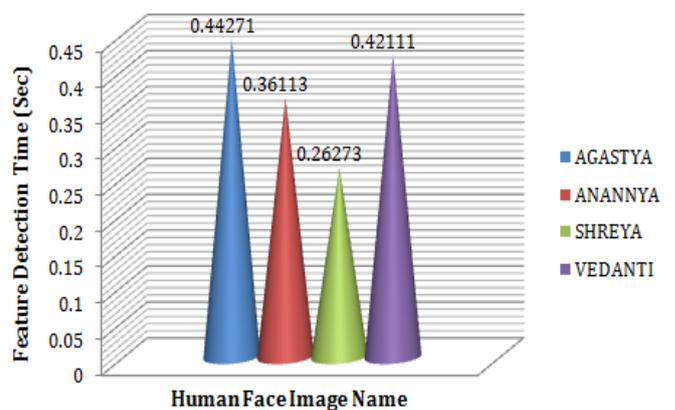


Figure No. 5.4: Feature Detection Time graph

In Fig No. 5.4 shows the result of feature detection. It shows four input images and time required for feature detection.

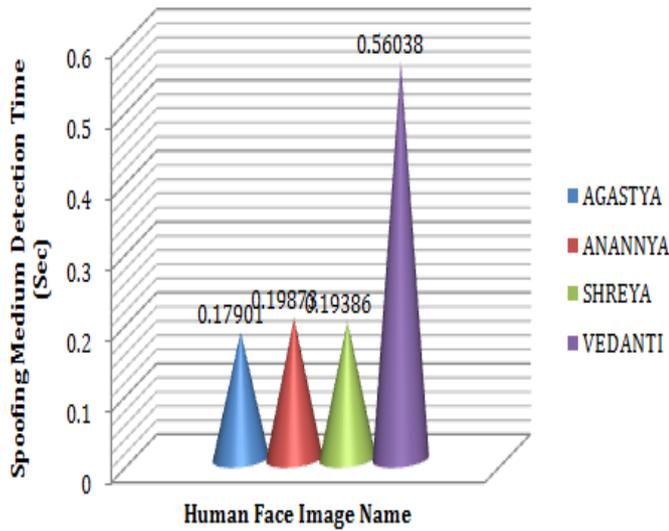


Figure No. 5.5: Spoofing Medium Detection Time graph

Table 5.2 shows the recognized image and spoofing medium detected in Grayscale image in which small rectangle is detected in Grayscale image which detect spoofing medium use for spoofing attack. It also gives required time for spoofing medium.

Sr. No.	Recognized image	Spoofing Medium Detected Image	Time for Spoofing Medium Detection	Detected Spoofing Medium
01			0.17901 Sec	Printed Photo
02			0.19873 Sec	Mobile
03			0.19386 Sec	Printed Photo
04			0.56038 Sec	Printed Photo

Table 5.2: Result for spoofing Medium Detection

## 6. CONCLUSION

An efficient and rather robust face spoof detection algorithm based on image distortion analysis (IDA) is implemented in this work using template matching algorithm for face recognition. From results, performance of the system for Face recognition by live streaming is improved. The image is given as input and facial features like eyes, nose, and mouth are extracted from the image efficiently. The proposed algorithm compares input images with stored patterns of face or features and collects the database. By implemented the detection medium for spoofing, the experimental result shows that it detects the medium used for face spoofing like mobile, printed photo better than the existing methods use for face spoof recognition.

From this work it is summarizes that from the previous literatures regarding Rein Lien Hsu it was shown that the accuracy of method was obtained 87.37% and by implementing the this method, accuracy increases to 99.34%.

## REFERENCES

- 1) 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.
- 2) 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.
- 3) 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.
- 4) 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.
- 5) 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.
- 6) 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.
- 7) 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.

- 8) 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.
- 9) J. Komulainen, A. Hadid, and M. Pietikäinen, "Context based face antispoofing," in Proc. BTAS, Sep./Oct. 2013, pp. 1-8.
- 10) G. Chetty, "Biometric liveness checking using multimodal fuzzy fusion," in Proc. IEEE FUZZ, Jul. 2010, pp. 1-8.
- 11) 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.
- 12) R. Tan and K. Ikeuchi, Feb. 2005. "Separating reflection components of textured surfaces using a single image". IEEE Trans. Pattern Anal. Mach. Intell., vol. 27, no. 2, pp. 178-193.
- 13) K. Kollreider, H. Fronthaler, M. I. Faraj, and J. Bigun, 2007. "Real-time face detection and motion analysis with application in "liveness" assessment," IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 548-558.

**BIOGRAPHY:**

	<p>Priyanka Prakash Raut            Education details            1) M.E.(CSE) (Pursuing) From KGIET, Darapur            2) B.Tech. (CSE) from Shri Guru Gobind singhji Institute of Engineering, Nanded            3) Dipoloma in Computer Science and Engineering, From Government Women's Polytechnic, Yavatmal            4) International Journal Publication- 03</p>
--	---