IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Special Issue || Dec. 2019 || PP 51-53
International Conference on Management Practices, Innovations & Research 2019

A Survey paper on face authentication system

1.Arshad Khan2.UkeshKewat 3.SameerRamteke4.Prof.Manisha
More,Asst. Professor, Dept. of Computer Science and Engg, Rajiv Gandhi College of Engineering, Chandrapur, Maharashtra,India.

Abstract:-*Biometric system can be either an 'identification' system or a 'verification' (authentication) system. Biometrics can be used to determine a person's identity even without his knowledge or consent.In this survey paper, we have made an effort to study and analyze the approaches of one of the existing biometric systems i.e. face recognition system. A face authentication system can recognize static images and can be modified to work with dynamic images. In 2008, H. Bay invented SURF descriptor which is invariant to a scale and in-plane rotation features. It consists of two phases such as interest point detector and interest point descriptor. In the first phase, he located the interest point in the image and second phase, used the Hessian matrix to find the approximate detection.*

In2012, Raja, A.S. from IIT-Delhi Database has worked on face authentication system using Neural Network Based SOM for Face recognition and its reorganization ratio is 88.25% to 98.3% . In 2013,J.yang focused on the face tracking, head rotation and pose variations issues. Face tracking is a significant procedure in face recognition. It usually exploits statistical model, example-based model, and skin color information to accomplish the tracking task. In addition, for these methods it also exploits CAMSHIFT, condensation, adaptive Kalman filter algorithms.

Keywords: *SURF Descriptor, Hessian matrix SOM, CAMSHIFT, Adaptive Kalman filter*

I. Introduction

Biometrics methods are automated methods of identifying a person or verifying the identity of a person based on a physiological or behavioural characteristic such as fingerprints, voice, face and iris.

A face recognitation system can help it many ways.

- Checking for criminal records.
- Enhancement of security by using survelliance cameras in conjunction with face recognitation system.
- Finding lost children by using the images recived from the camera filled at public places.
- Knowing in advance if some VIP is entering the hotel.
- Detecting of a criminal at public place.
- Can be used in different areas of science for comparing an entity with a set of entites.
- Patternrecognitation.

II. Literature survey:-

To our knowledge, one of the earliest studies on face spoof detection was reported in 2004 by Li et al. [6]. With the growing popularity of using face recognition for access control, this topic has attracted significant attention over the past five years [7], [8]–[10]. One of the major focus of the FP7 EU funded project, TABULA RASA [4], 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, (ii) 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 [5] and head rotation [1]. 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 [2].

(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 [6], 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 [7] and 7.60% in [1] to 6.62% in [2] 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.

(iii) Image Quality Analysis Based Methods:

A recent work [20] 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. A face-specific information has been considered in designing informative features for face spoof detection. Four features are designed specifically for face feature representation in this method, and it demonstrates the effectiveness of these features for spoof face detection. They have used both the Idiap and CASIA databases, which are two important public-domain databases.

(iv) Methods Based on Other Cues:

Face spoof countermeasures using cues derived from sources other than 2D intensity image, such as 3D depth [7], IR image [9], spoofing context [8], and voice [9] 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 [9], a microphone and speech analyzer was required in [9], and multiple face images taken from different viewpoints were required in [7]. Additionally, the spoofing context method proposed in [8] can be circumvented by concealing the spoofing medium.

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.

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.

III. Classification Method:-

A.Ensemble Classifier:-

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 [10] in signal processing [4], pattern recognition and classification applications [3], [4], one can choose to use SVM via the Lib SVM Library [2]. There are also a number of variations of SVM for handling large-scale classification problems, such as LIBLINEAR [5] and ALM-SVM [2]. A SVM classifier with RBF kernel is trained for each group of training data, with parameters optimized by cross-validation. 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.

Table of Comparison:-

Authors	Years	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	Feasiable,effective
N.kose	2012	To contrast between captured and recaptured images	Non intrusive and simple
T.de Freitaspereira	2012	Texture based method	Fast response(<1s)low computational complexity
J.yang	2013	Face liveness detection method	But 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. Conclusion:-

In this paper, 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 paper, a face spoof detection method based on
Image Distortion Analysis (IDA) is proposed.

References:-

[1]. Kavita,Ms. ManjeetKaur ,"A Survey paper for Face Recognition Technologies",International Journal of Scientific and Research Publications, Volume 6, Issue 7, July 2016,ISSN 2250-3153

[2]. Priyanka P. Raut , Namrata R. Borkar," Techniques and Implementation of Face Spoof Recognition: Perspectives and Prospects ", International Journal of Engineering Science and Computing, January 2018 , Volume 8 Issue No.1 10.1109/ICETT.2016.7873742.

[3]. Chung-Hua Chu* and Yu-Kai Feng," Study of Eye Blinking to Improve Face Recognition for Screen Unlock on Mobile Devices ", J ElectrEng Technol.2017, the Ministry of Science and Technology, R.O.C., under Contracts MOST 106-2221-E-025 -001.

[4]. Xiwei Dong, Fei Wu and Xiao-Yuan Jing," Generic Training Set based Multimanifold Discriminant Learning for Single Sample Face Recognition", KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS VOL. 12, NO. 1, January 2018.

[5]. Priya Gupta, NidhiSaxena, Meetika Sharma, JagritiTripathi,"Deep Neural Network for Human Face Recognition", International Journal of Engineering and Manufacturing(IJEM), Vol.8, No.1, pp.63-71, 2018.DOI: 10.5815/ijem.2018.01.06.

[6]. 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.

[7]. 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.

[8]. 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.

[9]. 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.

[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.