FACE SPOOFING ATTACKS DETECTION IN BIOMETRIC SYSTEM.

Mr. Kaustubh D. Vishnu[1], Dr. R.D.Raut[2], Dr. V. M. Thakare

SGBAU, Amravati, Maharashtra, India

ABSTRACT

Biometric system have evolved very well in last few years and in this digital era secure automatic solution for face spoofing is needed. Combining existing anti-spoofing approaches to come up with more robust mechanism is needed for preventing system from various spoofing types. In this paper, detecting face from image and extracting data from it and then optimizing that information with dataset rich network makes a reliable face spoofing attack detecting methodology. Proposed methodology can be used in various biometric systems suited with face detection mechanism. Simple execution with available resolution image and minimum use of extra hardware makes proposed methodology works for making biometric system more secure.

***Index Terms*— Biometric system, Face detection, Information Extraction, Spoofing attack, Face spoofing, Security**

I. INTRODUCTION

Digital era in computer system expects communication in form of images, audio, and video. Authentication gets user friendly with face recognition system. To make systems more Co-oprative now a days biometric authentication system are available with face recognition system. As systems have move on to digitalization then even system threats also attacks using various approaches which make difficult for developers to maintain security in system. Now a days most of smart phones have face oriented lock and unlock mechanism, this system is also affected by spoof attacks. Thus strong anti-spoofing attack mechanism for smart phone is preventing system from face spoofing attacks[1]. Iris, Face, and Fingerprint spoof detection is also the part of making biometric system spoof attack proof. A suitable convolutional network architecture is working to provide simple and effective authentication techniques[2]. Various approaches for face spoof detection and various methodologies are preventing systems from spoof attacks. Dynamic texture descriptor combining with blur tolerant descriptor with local phase quantization such multiple descriptor fusion works more effectively for face spoof detection[3]. Extracted information from input image are with various data patterns representation and grid and layered representation of information such digitalized representation improves the anti spoofing attacks strategies and making systems more secure[4]. Making different execution modes or combining approaches to verify the presence of real person is the matter of research. Face authentication system in biometric system have evolved from face detection to liveness detection which satisfies the present need[5].

In this paper face detection and conventional data representation are collectively used to give a method which expects easy and simple face spoof attack detection. Evolution of approaches from face detection to face liveness is making biometric system more robust to spoof attacks, presented method gives more reliable approach. Information extraction and using it effectively improves the performance of attack detection making system more secure.

II. BACKGROUND

Face Representation systems mainly faces face spoof attacks which minimises reliability of system. Different types of attacks increases vulnerabilities in face recognition system mostly consist of print attacks, replay attacks, and 3D mask attacks. Study of a large unconstrained smart phone spoof attack database (MSU USSA) with diverse 2D face spoof attacks help to present a new feature representation method for face liveness detection by considering the complementarily between different feature cues[1]

Biometric system have improved its performance, however system now a days have Iris, face and fingerprint detection system. Spoofing attacks is performed using printed iris images or cosmetic contact lenses. Faces spoofing can be done using a digital video, or even a 3D mask of a valid user. For fingerprints, the most common spoofing method consists of using artificial replicas created in order to spoof into system. To restrict such spoof attacks a method is proposed which presents a suitable learning convolution network architectures for each domain, and helps to learn the weights of the network via back propagation which benefits for evaluating Architecture Optimization and Filter Optimization apart and later combining them to build anti-spoofing systems[2].

Variety of different media is used for spoofing attacks in a different imaging conditions, the problem poses serious challenges to restrict spoofing in practical applications. MBSIF-TOP and MLPQ-TOP are two descriptor used with the SR-KDA approach proposes a method based on the dynamic multiscale binarized statistical image features and kernel discriminant analysis for face anti-spoofing. Method expects to perform better than similar dynamic texture descriptors such as LBP-TOP and LPQ-TOP.BSIF descriptors are used to deliver in the context of the spoofing detection application[3].

Biometric systems and its security evaluation and vulnerability assessment have been widely studied, Face recognition systems rely on flat images in order to detect people, Several face detection approaches include image quality analysis, motion analysis, texture analysis, or a combination of these. A face-spoofing 2D detection method is proposed by searching for Moiré patterns, which studies the multiple digital grids in the face-spoofing display and in the face-recognition camera. [4].

The biometric verification systems have a security threat of spoofing attacks and has been treated in past few years. An appropriate evaluation methodology which accounts for the application-dependent cost of the error rates is proposed which evaluate verification systems under spoofing attacks, which objectively assumes that both the zero-effort impostors and spoofing attacks need to be considered in the threshold decision process with a part that reflects the prior probability among all the misuses of the system[5].

This paper presents the brief introduction of face spoof attack detection in section I.Section II discusses background. Section III discusses previous work. Section IV discusses existing methodologies. Section V describes proposed methodology. Section VI discusses analysis and discussion. Section VII discusses the possible outcomes and result. Finally section VIII concludes this paper. And section IX states future scope for the proposed method.

III PREVIOUS WORK DONE

Keyurkumar Patel et.al (2016) [1] proposed a method gives which works better for face liveness detection. Using image distortion analysis, moiré patterns, shape deformations, surface reflection by the spoof medium, colour distortions face spoofing detection is done. This method handles spoofing attacks issues which includes printed photo, Replay attack, and 3D mask attack.

David Menotti et.al (2015) [2] proposed a method which states benefits of evaluating AO and FO apart and later combining them to build anti-spoofing system. The methodology for architecture optimization (AO) and filter optimization (FO) as well as pre-processing of benchmark images and execution of AO and FO with benchmarks is proposed. Proposed method states new architecture for spoofing detection i.e Spoofnet.

Shervin Rahimzadeh Arashloo et.al (2015) [3] proposed a method known as spectral regression kernel discriminant analysis (SR-KDA) is focused. The beneficial impact of combining the novel descriptor MBSIF-TOP with MLPQ-TOP improves the performance of the spoofing detection system. The kernel fusion is also executed by SR-KDA with CASIA dataset, Replay-Attack and NUAA databases which works reliably with low-resolution biometric data or short image sequences on the, the fusion consistently improves the performance.

Diogo Caetano Garcia and Ricardo L et.al (2015) [4] proposed a method which searches for artifacts due to the overlapping of digital grids using detection of Moiré patterns at the spatial domain. As their is not any a priori method to distinguish this kind of pattern from any other so its important to point out that prior to resampling, low-pass filtering may take place.

IvanaChingovska et.al (2014) [5] proposed a novel evaluation framework for verification systems under spoofing attacks. The proposed biometric verification system analyses all parameters imposed by the new problem domain. Reviewing the standards for evaluation of biometric systems in their common setup and inspecting efforts to adapt them to the new problem definition reporting on their drawbacks for deployment in real world conditions together expects to deliver stable performance and spoof attack free framework.

IV. EXISTING METHODOLOGY

Biometric system have improved its performance at all stages but still faces many spoofing attack issues. Various attacking approaches makes it difficult to prevent system from spoof attack but still their are many methodologies which works effectively to detect and prevent spoof attack, some of such methodologies are as follows,

A. Spoof Detection on Smart phones:

Five steps proposed for spoof detection are Face Detection, Normalization, Representation, Multi-Frame Voting, Reject Option. Variability in face detection increases challenges thus face detection and normalization is important. For representation proposed method uses Local binary pattern and multiscale LBP and SURF descriptor. IPD values used in discripter comparisons are compared using following relation.

$$r_{IPD}(d,a) = |d - \mu_{IPD}| \leq a \cdot \sigma_{IPD},$$

And area to be analysed are decided using following equations,

$$t(\mu,\sigma) = \begin{cases} 1 & \text{if } \mu < 5,\ \sigma < 5 \\ 1 & \text{if } \mu > 220,\ \sigma < 5 \\ 0 & \text{otherwise,} \end{cases}$$

Image quality and face texture features information leads to more robust performance. In voting step, If two or more frames within the three frames in a sequence are classified as live faces, then this sequence is classified as live, otherwise it is classified as spoof. Rejection options also improves performance[1].

B. Deep Representation For Spoofing Detection:

Implementations includes feed forward convolution operations are stacked by means of hyper parameter optimization, results into effective yet simple convolution networks that do not require expensive filter optimization and from which prediction is done by linear support vector machines (SVMs). Operations in convolution networks can be viewed as linear and non-linear transformations that, when stacked, extract high level representations of the input. Pooling operation equation used for network optimization is as follows,

$$K_i(p) = \sqrt[\alpha]{\sum_{\forall q \in \mathcal{B}(p)} J_i(q)^\alpha},$$

Divisive Normalization is expressed as follows,

$$O_i(p) = \frac{K_i(p)}{\sqrt{\sum_{j=1}^{n} \sum_{\forall q \in \mathcal{C}(p)} K_j(q)^2}}$$

Here use a well-known set of operations performed called (i) convolution with a bank of filters, (ii) rectified linear activation, (iii) spatial pooling, and (iv) local normalization to improve representation which helps to detect spoof attack[2].

C. Multiple Discriptor Fusion Approach:

Histograms of dynamic texture descriptor on three orthogonal planes to encode texture micro-structure of an image sequence is proposed for face liveness detection. For this purpose, two effective spatio-temporal texture descriptors, namely histograms of multiscale dynamic binarized statistical image features (MBSIF-TOP) and multi scale dynamic local phase quantization (MLPQ-TOP) are advocated. Linear filter *Wi* of acorresponding size, the filter response *si* is obtained by,

$$s_i = \sum_y W_i(y) X(y) = w_i^\top x$$

Collected representations are then combined for further enhancement of system performance. Their fusion is done using the SR-KDA method. Fusion technique for face spoofing detection improves the performance, compared to either one of the descriptors used individually[3].

D. Moire-Pattern Analysis Approach:

The Moire-patterns and digital grids of image patter helps to collect more information about input image. The face spoofing detection algorithm based on Moire-patterns analysis works with the images taken at different distances from the displays, in order to evaluate how the proposed algorithm operates under different circumstances. difference-of-Gaussians filter is expressed as following equation, where **G***(*0*, σ*2*)* is a 2D-Gaussian function with zero meanand standard deviation *σ*.

$$\mathbf{D}(\sigma, k) = \mathbf{G}(0, \sigma^2) - \mathbf{G}(0, k\sigma^2),$$

These different conditions were chosen so that two fundamental factors could separately be accounted for: (a) the distance between the display and the camera; and (b) the pixel resolution. This analysis help to detect the legal face preventing spoofing attack[4].

E. Biometric Evaluation Analysis:

Mechanism for rejecting spoofing attacks has been studied but now such attacks approach pattern has to handle as an additional input class. The proposed biometric verification system have three classes at input so that system can have as much as testing cases. The proposed biometric verification system considers all the parameters imposed by the new problem domain. And Weighted

Error Rate (WER) is defined as following equation where, *β* ∈ [0, 1] is the parameter balancing between the cost of FPR and FNR.

$$\mathrm{WER}_\beta(\tau^*, \mathcal{D}_{test}) = \beta \cdot \mathrm{FPR}(\tau^*, \mathcal{D}_{test}) + (1-\beta) \cdot \mathrm{FNR}(\tau^*, \mathcal{D}_{test})$$

To do this, firstly review the standards for evaluation of biometric systems in their common setup. Then, inspect the efforts to adapt them to the new problem definition reporting on their drawbacks for deployment in real world conditions[5].

V. ANALYSIS AND DISCUSSION

Biometric systems and face identification mechanism are most fundamental services of today's digital era. Most of system acquires face authentication mechanism most of them successfully uses that but still their is threat of face spoof attack in face authentication system. For anti-spoofing system many techniques are their but due to vulnerabilities of problem definition, need of new effective face anti-spoofing is expected. Face detection from an input image is challenging and most effective mechanism for making biometric system more robust, as if only face portion of image gets sorted and only that portion of image gets processed to extract useful information will help to improve accuracy and effectiveness of proposed method. Thus first step to approach is to detect face and extract information from it. Then the processes are executed to perform optimization on available information. Filtering information helps to improve accuracy and conventional network architecture to make available datasets when the step of matching of contents takes place.

Existing methodologies are having issues regarding resolutions and vulnerabilities of system, proposed method tries to combine method to improve performance thus with minimum complex mechanism face detection and face spoof detection method is expressed. Using existing image information effectively and being less dependent on extra hardware, maximum efficiency can be achieved to protect system from face spoofing.

Face spoof detection and prevention technique	Advantages	Disadvantages
Secure Face Unlock: Spoof Detection on Smartphones	. 1.Useful for cross-database and intra database testing. 2.Effective face spoof detection method.	1.Lack of autofocus capabilities may affect performance.

Deep Representations for Iris, Face, and Fingerprint Spoofing Detection	1.Effective and reliable database interface.	1.Small changes in the attack could require the redesign of the entire system
Face Spoofing Detection Based on Multiple Descriptor Fusion Using Multiscale Dynamic Binarized Statistical Image Features	1.Avoids the costly analysis computations	1.Challenging testing process
Face-Spoofing 2D-Detection Based on Moiré-Pattern Analysis	1.Database used is one of benchmarked among face datasets.	1.Issues related to resolution for the capturing image.
Biometrics Evaluation Under Spoofing Attacks,"	1.Fusion is highly beneficial to the systems. 2.Robustness to spoofing	1.It leads to unnecessary high vulnerability to spoofing

TABLE 1: COMPARISON BETWEEN DIFFERENT ANTI FACE SPOOFING TECHNIQUES

VI. PROPOSED METHODOLOGY

Biometric system are rich with face recognition technologies, method preventing system from spoof attack is what expected. Proposed method expect to detect spoof attack when input face image gets encountered with given framework of detecting real and fake face. Given method works primarily to extract face features from given image and passing it on for architecture optimization and filter optimization. Goal of proposed method is to give a simple and robust approach for face detecting and checking its originality. Publicly available datasets helps to develop a more robust anti spoofing system.

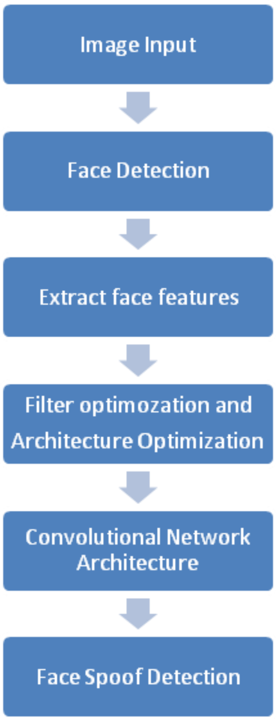
Image Input
Face Detection
Extract face features
Filter optimozation and Architecture Optimization
Convolutional Network Architecture
Face Spoof Detection

Fig.1: Framework of proposed methodology.

Architecture optimization verifies the linear scores of extracted linear SVM information and filter optimization processes the extracted information and its representing datasets. Convolutional Network when linked with available database improves reliability of method. Layered representation and multiple validation of extracted information improves robustness of proposed method.

ALGORITHM:

1) Pass on input image for face detection.

2) Extract features from face image.

3)Evaluate the architecture according to an optimization objective based on linear SVM scores;

4) Filter optimization with training sets of extracted information

5) Combine optimizational results with convolutional network.

6) Stop.

VII. POSSIBLE OUTCOMES AND RESULT

By detecting face portion from a image and extracting information at primary level and minimizing complexity to get information have made possible to give simple and effective approach to prevent spoofing attack. Proposed method is not dependent on high resolution image only, thus gives best result with available quality. Optimization and filtering of data improves the reliability. Database rich architecture and effective use of information makes the approach more promising.

VIII. CONCLUSION

This paper presents the face spoof detection mechanism and protecting biometric system from spoofing attacks. Digital era of technology expects spoofing free systems making more secure sharing of data. Proposed method makes biometric system with ability to detect the spoof attacks before losing any data makes systems more secure. Combining existing anti-spoofing mechanisms to develop more strong mechanism to make biometric system more robust is best with result as its expected from this proposed method.

IX. FUTURE SCOPE

Future work should work on efficient method to capture quality image which will help to have more accurate output as well as test cases should be analysed.

REFERENCES

[1] Keyurkumar Patel, Hu Han, and Anil K. Jain, “Secure Face Unlock: Spoof Detection on Smartphones,” IEEE transactions on information forensics and security. Volume 11 , Issue No. 10 , PP 1-16,OCTOBER 2016

[2] David Menotti, Giovani Chiachia, Allan Pinto,William Robson Schwartz, Helio Pedrini, Alexandre Xavier Falcão and Anderson Rocha, “Deep Representations for Iris, Face, and Fingerprint Spoofing Detection,” IEEE Transactions On Information Forensics And Security.Volume 10, Issue No. 4,PP:864-879,April 2015

[3] Shervin Rahimzadeh Arashloo, Josef Kittler, and William Christmas, “Face Spoofing Detection Based on Multiple Descriptor Fusion Using Multiscale Dynamic Binarized Statistical Image Features,” IEEE Transactions On Information Forensics And Security.Volume:10 , Issue No: 11 , PP: 2296-2407,November 2015

[4] Diogo Caetano Garcia and Ricardo L. de Queiroz, “Face-Spoofing 2D-Detection Based on Moiré-Pattern Analysis,” IEEE Transactions On Information Forensics And Security. Volume:10 , Issue No:4 , PP:778-786,April 2015

[5] IvanaChingovska, André Rabello dos Anjos, and Sébastien Marcel, “Biometrics Evaluation Under Spoofing Attacks,” IEEE Transactions on Information Forensics And Security. Volume: 9, Issue no: 12, PP: 2264-2276,December 2014