7th International Conference on Recent Development in Engineering Science, Humanities and Management
National Institute of Technical Teachers Training & Research, Chandigarh, India (ESHM-17)
3rd June 2017, www.conferenceworld.in ISBN: 978-93-86171-26-9

EFFECTIVE METHODOLOGY FOR DETECTING AND PREVENTING FACE SPOOFING ATTACKS

[1]Mr. Kaustubh D.Vishnu, [2]Dr. R.D. Raut, [3]Dr. V. M. Thakare

[1,2,3] SGBAU, Amravati ,Maharashtra, (India)

ABSTRACT

Biometric system has to deal with all kinds of spoofing attacks. Face spoofing attack prevention techniques must be reliable against print attack, mask attack etc. In this paper, proposed method works to make spoof attack more challenging for attackers by adding one extra preventive measure against spoof attack. Proposed method mainly works against such print attack and mask attack. Most of anti spoofing system prevents system without checking for liveness thus proposed method checks for liveness of accessing by giving any pre examined but random face sample to use that and trying to re-login which check for liveness of accessing. Adding extra step increases difficulties for spoofing. Extra user interface improves security and helps system to use simple method for anti spoofing rather than using complex methodology.

Index Terms— Face Detection, LBP, Spoofing Attack, Liveness Detection, User Interface, Security

I INTRODUCTION

Spoofing attacks are the attempts to access the system by presenting a copy of biometric trait of user which is mode of falsifying the data for access within system. In today's digital era most of systems uses faces for biometric authentication, but vulnerabilities in system makes spoofing attack possible. Most of techniques are their which works to prevent spoofing attack, extracting information from acquired images and checking for its validation is the most common technique. Extraction of information and matching issues are taken care more than state of liveness while accessing the data. Designing the framework for verification systems under spoofing attacks, which executes state-of-the-art verification, The framework works for comparison of the systems depending on the prior probability of the spoofing attacks or the cost of the error rates and helps decide which combination of verification system, anti-spoofing system and fusion method to use for a given application[1]. Another approach studies the client specific information used to develop anti-spoofing system and uses the huge datasets against spoofing attacks and examines the state-of-the-art anti-spoofing features. Gaussian Mixture Model(GMM) uses available users information to distinguish between real and fake authentication accesses[2]. Multimodal fusion technique investigates the dynamic detection and rejection of liveness-recognition pair outliers for spoofed samples in true multi-modal configuration. Fingerprint spoof-detection is also analyzed[3]. For authentication purposes using and assisting several datasets and expressing its preliminary analyzing on real data sets of spoofing attacks, improves the performance against spoof attack on fingerprint and face biometrics[4]. Method makes out combination of the facial expressions and the neural network concept, in a neural-network-based soft biometric face recognition system these facial expressions gives the persistent base for face validation purposes[5].

ISBN: 978-93-86171-26-9

In this paper, proposed method suggest an approach for face spoof detection and its prevention. After execution of information validation, second face acquisition is performed to test for liveness of authentication procedure. Proposed method helps to prevent print spoof attack and 3d mask spoof attack. With the help of user interaction proposed method gives a simple method to prevent face spoof attack.

II BACKGROUND

The spoofing attacks are security threat for the face authentications systems in many modes and the problem of anti-spoofing has been significantly treated in the past few years. Due to varying attack scenarios and environment conditions, there is no absolutely superior face anti-spoofing technique. The combination of liveness features from the image quality-based and motion-based visual cues provides a promising direction to enhance the generalization and stability of a face anti-spoofing classifier. Multi-cues integration-based face anti-spoofing approach combines liveness features from three aspects, the image quality feature, the optical flow based face motion feature, and the optical flow-based scene motion feature. Integration based face anti-spoofing detection system is proposed for face anti-spoofing which is preventing system from face spoofing attacks[1].

Liveness detection and anti-spoofing algorithms has more importance for many biometric modes. Specific hardware device can be used to check presence of a living person in front of the system but this approach can be costly. Combination of multiple modalities could be a safe approach. Most of system uses user's information to match the input sample against a stored model. The anti-spoofing systems rarely make use of information this matching approach helps to use the available information. Face anti-spoofing features handles the available information of real accesses and spoofing attacks, like texture, quality, motion patterns etc. and this information helps a lot to decide the real and fake access of images. Method applies suitable anti-spoofing method which is inexpensive and convenience to use[2].

Spoofing problem are handled either by actively assessing the liveness, or by passively analyzing patterns of spoofed materials. Among the most common techniques for extracted from single image, texture-based anti-spoofing methods are statistical features, Power Spectrum Fourier analysis, Ridge Frequency Analysis, Local Binary Patterns and Local Phase quantization. A fusion method is proposed which extend research into multiple modalities. This paper investigates 1-median based fusion using outlier detection applied in the biometric setup. Aggregating of classifier is employed in combining the decision outcomes affects performance of preventing sppof attack[3].

Spoofing attacks on biometrics is also a topic of research field of liveness detection. Several hardware- and software based liveness detection systems have been proposed ,Biometric identity verification is needed to be explored. Proposed method works for biometric identification system which is indirectly working against spoofing attacks on biometrics. Identity of an enrolled client, and provides his biometric traits to the system. The claimed identity is then verified by comparing the submitted biometric traits with those stored into the system database corresponding to the claimed identity. The output of this step is a matching score which is then compared with a decision threshold. If the matching score is above the threshold, the user is accepted as genuine; otherwise, user is rejected as impostor[4].

(ESHM-17)
ISBN: 978-93-86171-26-9

Accepting facial expression is a way humans communicate with others and react, for a computer to achieve human-like performance it will have to know what our feelings are and if are expressed by us and not someone else. Facial expressions in a neural-network-based soft biometric face recognition system and investigating the improvements it brings to standard face recognition systems and if it makes it less susceptible to spoofing attacks. Combination of Facial expressions and neural network based soft biometric face recognition system gives feasible and cost effective system which will prevent system from spoofing attacks. Facial features of an individual do not change, cannot be forgotten, or lost, a method take help of that and this proposed soft biometric system could be more accurate than other identification systems because its using persistent base for validation.[5]

This paper presents the brief introduction of face spoofing prevention and its 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.

III PREVIOUS WORK DONE

LitongFeng et.al (2016) [1] proposed face anti-spoofing approach combines liveness features from three aspects: the shearlet-based image quality feature, the optical flow based face motion feature, and the optical flow-based scene motion feature. Providing a better image quality descriptor. Generalization of the motion-based feature is analyzed; no motion assumption or scenic model for face anti-spoofing is adopted. A higher face anti-spoofing classification accuracy is achieved by the proposed approach compared with the state-of-the-art methods

Ivana Chingovska et.al (2015) [2] proposed a anti-spoofing method which uses one of three categories such as texture based, motion-based and liveness-based. The texture-based features finds the differences in texture between real accesses and attacks. The motion-based methods examines the movements on the scene which are unusual for a 3D human face, and uses them as a cue that an attack is being performed. The liveness based methods try to detect clues of liveness in the scene such as eye-blinking and involuntary lip movements. Proposed method tries to develop the idea of considering the client identity information when building anti-spoofing systems and not other complex classifier strategies . Proposed method aims to demonstrate how client-specific classification can be beneficial even when using simple features, upon which many of the best performing methods are built.

Peter Wild et.al (2015) [3] proposed a efficient and robust anti spoofing method. Proposed method is combination of multiple modalities which prevents the spoofing attacks. Proposed method tests the m out of n samples which are spoofed which helps to highlight the tradeoff between accuracy and security for different fusion methods, latest datasets are used to analyze these impacts. Score level fusion rule is experienced to get best fusion method. This paper investigates 1-median based fusion using outlier detection applied in multi-biometric setup. And this paper proposes fusion principle known as bootstrap aggregation of classifier. This technique is combining the decision outcomes of multiple different classifiers. Combination of anti-spoofing and recognition is proposed and anti-spoofing in fingerprint and face recognition is proposed broadly be classified into texture based and motion based counter measures.

ISBN: 978-93-86171-26-9

B. Biggio Z et.al (2012) [4] proposed an approach to prevent biometric system from spoofing attacks. Using verification and validation techniques the difference between genuine and imposer user is examined. Proposed method gives analysis of finger print spoofing and face spoofing, Multi-model biometric system against spoofing attacks has been defined, Sensors, feature, matching score and decision making these steps are applied. Robustness against spoofing attacks is proposed in the method which makes this approach effective.

Mihai Gavrilescu et.al (2016) [5] proposed methodology which mainly focused on using facial expressions other than any technical strategy, thus typically proposed method is divided in sub-blocks such as Face detection, face segmentation, AU detection, AU classification. BM building. Artificial neural-network for pattern recognition. The architecture works in two main blocks such as individual expression recognition block and standard principal component analysis -based face recognition block. To defect expressions effectively expected distance must be maintained so few distant quantities must be considered which are Vertical distance between eyes and brows which is used to determine in what degree brows are outlying eyes. Vertical distance from mouth peripherals to eyes which is used for analyzing various emotions which will be used to detect valid and invalid faces. Vertical distance from cheek internal extremities to mouth centre which is used with previous distances to increase accuracy.

IV EXISTING METHODOLOGY

4.1 Image quality and motion cues for face anti-spoofing.

Integration of image quality and motion cues for face anti-spoofing methodologies extracted SBIQF vector features from a normalized face image. Face coordinates are determined using face detector and aligned with eyes-location. A face video is collected using the same face coordinates and normalization process as in the previous step. All different liveness cues are concatenated as a fused bottleneck feature, which is further fed into the subsequent neural network for liveness detection. False acceptance rate, and False rejection rate are used to calculate HTER, which is useful to find out associated time required to access database effectively.

$$\mathrm{HTER} = \frac{\mathrm{FAR}(\tau, D) + \mathrm{FRR}(\tau, D)}{2}$$

The liveness status is finally determined and uses to detect and prevent spoof attack[1].

4.2 Client Identity Information for Face Anti-spoofing

Implementation of proposed method starts with categorizing clients inputs with the error rates of the verification system, like False Acceptance Rate (FAR), False Rejection Rate (FRR) and others. Evaluation of the scores of state-of-the-art client-independent anti-spoofing systems using the aforementioned LBP, LBP-TOP and MOTION features gets done. The likelihoods of the cohort attack models is examined as follows and is then used to calculate C_{LLR} as follows,

ISBN: 978-93-86171-26-9

$$p(\mathrm{X}|\mathcal{H}_1) = \frac{1}{|\mathcal{C}|}\sum_{\mathrm{J}\in\mathcal{C}} p(\mathrm{X}|c = \mathrm{A}, i = \mathrm{J})$$

$$c_{LLR} = \log \frac{p(\mathrm{X}|c = \mathrm{R}, i = \mathrm{I})}{\frac{1}{|\mathcal{C}|}\sum_{\mathrm{J}\in\mathcal{C}} p(\mathrm{X}|c = \mathrm{A}, i = \mathrm{J})}$$

The analyzed client-independent classifier is SVM, which is the baseline classifier used in which evaluates the verification scores, method analyzes the anti-spoofing scores per client[2].

4.3 Face and fingerprint fusion against spoofing attacks.

Implementation of proposed method is done by joint liveness and score pairs is conducted, incorporating liveness information into decision. Obtained EER results shows more stable results. Proposed method uses own algorithm for fusing Score and liveness fusion, which gives effective methodology for face spoof detection. Fusion method used in method is expressed as follows,

$$F_{mf}(\vec{s}) := \frac{1}{\sum_{i=1}^{n} M(\vec{s}, s_i)} \sum_{i=1}^{n} M(\vec{s}, s_i) s_i.$$

$$M(\vec{s}, s_i) := \begin{cases} 1 & \text{if } \left| s_i - \underset{j=1}{\overset{n}{med}}\, s_j \right| < \phi; \\ 0 & \text{else.} \end{cases}$$

Fingerprint liveness detection can also be implemented by using proposed method[3].

4.4 Biometric authentication systems against spoofing attacks.

Users available valid image gets validated with the captured image by user. Both face and figure print matching is done and datasets used are very useful for this process. Implementation of proposed method is done by developing chimerical data sets, by randomly associating face and fingerprint images of pairs of clients of the available five fingerprint and three face data sets. Then data set gets randomly subdivided into five pairs of training and testing sets. Each training set included 40% of the fake matching scores were computed by comparing each fake image of a given client with the corresponding template image. Captured value score are used to find out Likelihood ratio as follows. Also these value scores are used for various relations used to analysis purpose.

$$f(s_1, s_2) = \frac{p(s_1, s_2|G)}{p(s_1, s_2|I)}$$

The performance is studied by computing DET curves (FRR against FAR).By this way implementing biometric system will help to prevent system from spoofing attacks[4].

ISBN: 978-93-86171-26-9

4.5 Study on using facial expressions for a face recognition system immune to spoofing attacks.

Data collected from different information resources is then associated with the neural network generators which are then matched with the available datasets which is useful to detect the valid and spoofed face image. Technically speaking implementation of method is done in the implementation of processes such as Face detection, face segmentation, AU detection, AU classification, BM building, Artificial neural-network (ANN) for pattern recognition. The difference between the outputs values and the expected values is used to determine the average absolute relative error (AARE) which is defined as follows,

$$\text{AARE} = \frac{1}{N}\sum_{n}^{1}\left|\left(\frac{y_p - y_e}{y_e}\right)\right|$$

Overall output is then gets analyze with available datasets and efficiency gets checked. Used databases gives availability of vast number of faces images which is useful for expression analysis[5].

V. ANALYSIS AND DISCUSSION

Spoof detection and prevention techniques mostly works on extracting the information from available images and processing that information to use that output for validation procedure.Due to this approach the requirement of quality image acquisition is expected which may increase the cost of procedure. Thus the new approach of prioritizing the liveness than the secured authentication is needed to accept. If validation of the liveness of process of accessing system is done initially then the spoof attack detection and prevention efficiency may increases. Advantages and disadvantages of some of techniques are tabularized below:

Face spoof detection and prevention technique	Advantages	Disadvantages
Integration of image quality and motion cues for face anti-spoofing.	Integration-based approach achieves an EER	It is complex to implement and implementation cost is also high
Client Identity Information for Face Anti-spoofing	Uses client specific information Low cost and convenient to use.	Incorrect matching score may misguide results.
Face and fingerprint fusion against spoofing attacks	Combined fingerprint and face recognition. Alternative option to sum rules for combinations.	Difficulties may arise in score and liveness fusion.
. Biometric authentication systems against spoofing attacks.	Robustness against spoofing attacks. Benchmarked datasets used	Difficulties in finding exact matching score. Wrong matching score leads to wrong

ISBN: 978-93-86171-26-9

		identification.
Study on using facial expressions for a face recognition system immune to spoofing attacks	Gives low cost and soft biometric face detection platform.	execution time must be managed well.

TABLE 1: COMPARISON BETWEEN DIFFERENT ANTI FACE SPOOFING TECHNIQUES

VI. PROPOSED METHODOLOGY

Proposed method works to give more importance to liveness detection process. Database for the procedure is managed with already collected featured face images of user. Thus after first matching step, framework again does the face acquisition for liveness testing and then matching procedure is performed. Extra user interaction just for face acquisition expects more accurate face spoof detection. Proposed framework is shown in following diagram:

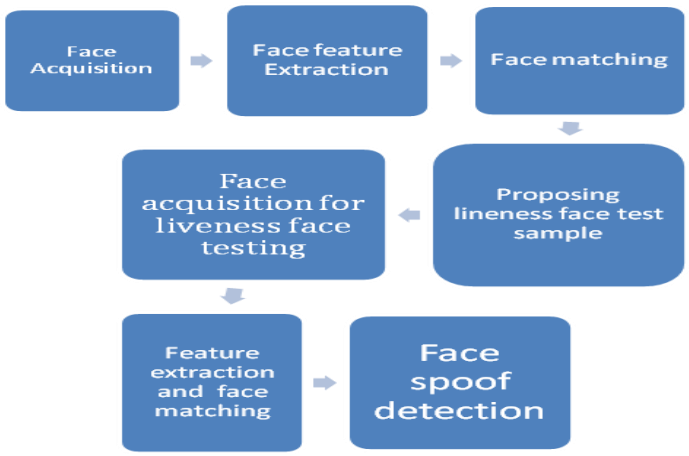

Fig: Proposed framework for Face Recognition & detection of spoofing attack

Proposed algorithm:

Step 1: Face Acquisition.

Step 2: Face feature Extraction form collected face image.

Step 3: Information and Face matching procedure.

Step 4:Proposing lineness face test sample by data mining for effective liveness detection.

Step 5:Required sample shown for Face acquisition for liveness face testing.

Step 6:Feature extraction and face matching.

Step 7:Face spoof detection.

ISBN: 978-93-86171-26-9

Proposed method works more to test liveness which minimizes harms of spoof attack. Databases are made ready for extracting random face test sample for liveness test. Proposed method aims to restricts print and mask spoof attack which are mostly used for spoofing purposes.

VII. POSSIBLE OUTCOMES AND RESULT

Giving more importance to liveness test, face spoof detection execution done at early stages of authentication. Use's live interaction is improved so that no need to maintain and remember authentication information because user don't have to remember or save its face information used for authentication purposes. Thus the easy and simple execution approach is proposed for face spoof detection and prevention.

VIII. CONCLUSION

This paper gives approach which works on giving more importance to liveness detection than collecting and extracting information from collected resources. Simple acquisition and pattern matching procedures are used for spoof detection and prevention. Print attack and mask attacks are most common in spoof attacks proposed method restricts both kind of attack.

IX. FUTURE SCOPE

Future work is expected on efficient face acquisition strategies. And strategies to access database values effectively which will be useful to improve response time.

REFERENCES

[1] LitongFeng, Lai-Man Po, Yuming Li, XuyuanXu, Fang Yuan, Terence Chun-Ho Cheung, Kwok-Wai Cheung, "Integration of image quality and motion cues for face anti-spoofing: A neural network approach" ELSEVIER. Volume 38 , Issue no 38, PP 451-460 April 2016

[2] Ivana Chingovska and André Rabello dos Anjos, "On the Use of Client Identity Information for Face Anti-spoofing" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. Volume 10 , Issue No 4 , PP 787-796 April 2015

[3] Peter Wild , Petru Radu, Lulu Chen, James Ferryman, "Robust multimodal face and fingerprint fusion in the presence of spoofing attacks" Issue No 50, PP 17-25 August 2015

[4] Allan Pinto, Helio Pedrini, William Robson Schwartz and Anderson Rocha, "Face Spoofing Detection Through Visual Codebooks of Spectral Temporal Cubes" IEEE TRANSACTIONS ON IMAGE PROCESSING. Volume 24,No 12,PP 4726-4740 December 2015

[5] B. Biggio Z. Akhtar G. Fumera G.L. Marcialis F. Roli**, "**Security evaluation of biometric authentication systems under real spoofing attacks" Published in IET Biometrics Volume 1 , Issue No 1, PP 11-24 February 2012