SPOOFING RECOGNITION FOR FACE WITH MASKS: AN ANALYSIS

SruthiMol. P[1], Pradheeba. P[2]
[1]*PG Scholar, Biometrics and Cyber Security, Rathinam Technical Campus, Tamil Nadu, India*
[2]*Assistant Professor, Computer Science and Engineering, CMS College of Engineering & Technology, Tamil Nadu*

Abstract - ***In recent years, face recognition has often been proposed for personal identification. However, there are many difficulties with face recognition systems. Among tangible threats and vulnerabilities facing current biometric systems are spoofing attacks the problem of detecting face spoofing attacks (presentation attacks) has recently gained a well-deserved popularity. Focusing on 2D and 3D attacks morphed by displaying printed photos or recorded videos on mobile devices or any, a major portion of these studies keep their arguments on the flatness of the spoofing material in front of the sensor. And among all biometric traits, face is exposed to be the most serious threat, since it is particularly easy to access and reproduce. The goal of the position paper is to share the lessons learned about spoofing and anti-spoofing in face biometrics.***

Keywords: *Biometrics, Spoofing attacks, Recognition systems, presentation attacks, 2D and 3D attacks.*

1. INTRODUCTION

Biometrics is defined as an automated method of verifying or recognizing the identity of a living person based on physiological or behavioral characteristics. Many researchers have been done to determine which traits can differentiate humans and to optimize that differentiation, the problem of determining whether the presented feature has originated from a living person has received very less attention. One type of sensor attack that happens at the beginning of the process, like fake biometric data will be presented to the sensor known as a *spoof attack* [2], which takes the form of an artificial finger, a mask over a face, or a contact lens on an eye.

A *spoof* is a counterfeit biometric method that is used in an attempt to forge a biometric sensor. When a genuine biometric trait presented from a live person from some other source is differentiated is called *spoof detection*. The process of sensing vitality ("*liveness*") signs such as pulse is one method of spoof detection. In some research areas, the term liveness detection is meaning of spoof detection. Spoof detection methods can be grouped using three different approaches: a) using the data collected for biometric purposes alone b) process information already collected to generate
discriminating information or collecting additional biometric images over time or c) using additional hardware and associated software to detect signals that have higher discriminating power than biometric data. Thus spoof detection methods are categorized.

Humans often use face as a trait to recognize individuals. And improvements in computing capability over the past few decades now enable similar recognitions automatically and easily. Early facial recognition algorithms [33] used simple geometric models, the recognition process has now developed into a science using the standard and sophisticated mathematical representations and matching processes. The higher advancements and initiatives in the past 10 to 15 years have boomed facial recognition technology into the spotlight and priority.

Facial recognition is used for both verification and identification purposes (open-set and closed-set). The obtained identity is then verified by matching the submitted biometric traits with those stored into the system database corresponding to the claimed identity (which is usually referred to as "templates"). The output achieved 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, he is rejected as *impostor*. By analyzing different threats, the direct or spoofing attacks have lead the biometric community to study the vulnerabilities against the type of fraudulent actions in traits such as the fingerprint [1], the face [2], the signature [3], or even the gait [4] and multimodal approaches [5]. Among all the biometric traits, face is said to be more vulnerable to the spoofing attack. In the process, the user claims the identity of an enrolled client, and provides his biometric traits to the system to bypass the biometric system. Bypassing can be done with several methods. There are several researches undergoing in the current scenario. This paper introduces the analysis of spoofing face recognition with mask and a review is being produced.

2. THREATS OF THE BIOMETRIC SYSTEM

There are different types of threats to the biometric system which are explained as

- Circumvention**: -** An attacker gains access to the system protected by biometric authentication.
- Repudiation**: -** An individual who accesses a certain facility can later deny using it.
- Collusion**: -** A user with wide super user privileges.
- Coercion**: -** An attacker forces a legitimate user to access the system.
- Denial of service:-An attacker corrupts the

biometric system so that legitimate user can't use it.

3. SPOOFING ATTACKS

Spoofing attacks are the major security traits that biometric recognition systems are proven to be vulnerable to. If spoofed, a biometric recognition system is bypassed by presenting a copy of the biometric evidence of a valid user. Spoofing attack is defined as the action of outwitting a biometric sensor by presenting a biometric evidence of a valid user [6]. Spoofing is a direct attack to the sensory input of a biometric system and the attacker does not require previous knowledge about the recognition algorithm. Many of the biometric modalities are not resistant to spoofing attacks, the biometric systems are usually designed to only recognize identities without concerning whether the identity is living or not. Despite the presence of very sophisticated biometric authentication and verification systems, implementing anti-spoofing schemes for them is still in its infancy nowadays. Depending on the biometric modality being attacked, fake biometric data can be fabricated with having different levels of difficulty.

Spoofing Related Risks

- A Fake artifacts is used to mount attacks against existing enrollments in order to gain unauthorized access in the systems.
- A fake artifact is used to enroll and authenticate in a biometrics system.
- A fake artifact is used to mount attacks against existing enrollment in order to gain unauthorized access to the resource protected by biometric system.
- Above given are the results of attacks- due to inability of the biometrics system to ensure liveness of an individual.

4. ANTISPOOFING METHODS FOR FACE BIOMETRICS

Face recognition systems can be easily spoofed using a simple photograph of the enrolled person's face, which may be displayed in hard-copy or on a screen. In 2-D face recognition systems, Anti-spoofing can be broadly classified in 3 categories with respect to process clues used for attack detection: motion, texture analysis and liveness detection.

In the process of motion analysis clues are generated when 2D counterfeits are presented to the system input camera, for example photos or video clips. 2D objects motion is different from real human faces which are 3-D objects, in many cases these deformation patterns are the base for spoof detection. For example, [7] presents the Lambert an reflectance model to differentiate between the 2-D face images used during an attack and a real (3-D) face, in enrollment. In such cases the latent reflectance information of images captured in both cases using either a variation retinex-based method or a far simpler difference-of-Gaussians [8] based approach is estimated and an equation is derived.

1. In Texture analysis counter-measures are based on texture patterns such as printing failures or overall image blur this may look unnatural when exploring the input image data. [9] Proposes a method for print-attack detection by 2-D Fourier spectra comparing the hard-copies of client faces and real accesses. In [10] the author have proposed a method based on micro-textures presented on the paper using a linear SVM classifier [11]. Defect of this method is that input image needs to be reasonably sharp.

2. The method of Liveness detection is used to determine if the biometrics data is being captured from a legitimate, live user who is physically present at the point of acquisition. [12] A technique to estimate liveness based on a short sequence of images using a binary detector which calculates the trajectories of specific parts of the face which is given to the input sensor using a simplified optical flow analysis and then followed by heuristic classifier is being explored. A method for fusing scores based on concurrently, the 3-D face motion scheme introduced the work on the previous work and liveness properties such as eye-blinks or mouth movements are obtained. Real-time liveness detection which uses an undirected conditional random field framework to model the eye-blinking relaxed the independence assumption of generative modelling and state dependence limitations from hidden Markov modelling.

5. DISCUSSIONS

The detection of face spoofing attacks (presentation attacks) has recently gained a well-deserved popularity and is being widely studied. While focusing on 2D attacks that is being forged by displaying printed photos or replaying videos on mobile devices or other devices, have achieved relatively wide popularity in the field of the biometric system. In paper [13], the spoofing potential of subject-specific 3D facial masks for 2D face recognition is previewed. Further, Local Binary Patterns based countermeasures using both color and depth data, obtained by Kinect is also being analyzed. For this purpose, the 3D Mask Attack Database (3DMAD), which is the first publicly available 3D spoofing database is recorded with a low-cost depth camera and introduced. Several experiments on 3DMAD show that easily attainable facial masks can bring a serious threat to 2D face recognition systems and LBP is a powerful weapon to eliminate and neglect it.

For this experiment, a verification scenario is assumed. After the Universal Background Model is created using the training set, match scores are generated on the probe partitions of development and test sets. The Equal Error Rate (EER) threshold is calculated on the development set as the decision threshold for verification.

With this setting, 65.70% of the mask attack attempts in the test set are incorrectly classified as clients. This Spoof False Acceptance Rate (SFAR) validates the mask attacks in 3DMAD as successful spoofing attempts against 2D face recognition. Utilization of 3D masks in spoofing attacks becomes easier, cheaper each day with the advancements in 3D printing technology. In that paper, the aim was to contribute to the current state of research in this domain by presenting a novel public database of 3D mask attacks accompanied by protocols and a baseline 2D face recognition system that is proved to be vulnerable to those attacks, and by giving an analysis on various LBP-based anti-spoofing methods using color and depth images obtained from Kinect. The experimental results generally suggest that for both data types, LDA classification of block- based extracted uniform LBP features is more accurate in mask detection.

The work of Kim et al. [14] can be listed as one of the first papers published in mask anti-spoofing. It aims to distinguish between the facial skins and mask materials by exploiting the fact that their reflectance should be different. For this purpose, the distribution of albedo values for illumination at various wavelengths is analyzed to see how different facial skins and mask materials (silicon, latex, or skin jell) behave in reflectance. As a result, a 2D feature vector consisting of 2 radiance measurements under 850 and 685 nm illuminations is selected to be classified via Fisher's linear discriminant. The proposed method is reported to have 97.78% accuracy in fake face detection. In that paper, the experiments are done directly on the mask materials instead of real masks and hence, spoofing performances are not included. Additionally, for mask detection, the measurements are required to be done at exactly 30cm and on the forehead region. The occlusion possibility in the forehead together with range limitations makes the method quite impractical.

Similarly in [15], multi-spectral analysis is proposed claiming that fake, by its definition, is indistinguishable for human eyes and therefore, it is not possible to detect attacks using only visual face images. After measuring the albedo curves of facial skin and mask materials with varying distances, two discriminative wavelengths (850 and 1450 nm) are selected. Finally, an SVM classifier is trained to discriminate between genuine and fake attempts. Experiments are conducted on a database of 20 masks of different materials: 4 plastic, 6 silica gel, 4 paper pulp, 4 plaster and 2 sponge. The results show that the method can achieve 89.18% accuracy. Eliminating the range limitation and experimenting on real facial masks, the authors bring the state of the art one step further, but still no analysis of how well the spoofing attacks work is presented. These two papers handle the mask attacks in an evasion context rather than spoofing. They don't examine masks that are replicas of real subjects to be impersonated.

Contrarily, in [16], Kose et al. work on a mask database which consists of printed masks of 16 real subjects. For this purpose, the scans of subjects were acquired by a 3D scanner and the masks were manufactured using a 3D printing service. a Local Binary Pattern (LBP) based counter measure to detect mask attacks is tested on two modes: color images and depth maps.1 A depth map is also a grayscale image which contains information relating to the distance of the surfaces of 3D objects from a viewpoint. Multi-scale LBP features are extracted from both 2D and 2.5D images and a linear Support Vector Machine (SVM) classifier is trained to determine whether a feature belongs to a real or an attack sample. A training set is utilized which not overlap with the testing partitions. The results are presented separately for 2D and 2.5D modes as correct classification rates that are calculated at the thresholds giving best performances. Since a development partition does not exist, the thresholds are optimized on the test scores.

In addition to texture images, the database also includes range images for both real and fake samples. The authors propose to apply an LBP-based method [17] on both color and depth channels and claim 88.12% and 86% accuracy, respectively. This study has two main shortcomings: Firstly, although they have the means to do so, the authors unfortunately do not report on the spoofing performances of the printed masks. To certify the alleged threat is nearly as important as to counter it. Secondly and more importantly, the utilized database is not public, posing a barrier to comparative and reproducible research.

In [10] the author proposes a method based on micro-textures present on the paper using a linear SVM classifier [11]. Drawback of this method that input image needs to be reasonably sharp.

It explores a real-time liveness detection that uses an undirected conditional random field framework to model the eye-blinking that relaxes the independence assumption of generative modelling and state dependence limitations from hidden Markov modelling use the publicly available PRINT-ATTACK database and its companion protocol with a motion-based algorithm that identifies correlations between the person's head movements and the scene context which can be used to compare to other counter-measure techniques.

[18] Proposed a new IQA scheme based on the concept of gradient similarity. Gradients convey important visual information containing structural and contrast changes which affect the image quality. Luminance changes also affect the image quality. Finally, the effects of these changes are integrated via an adaptive method to obtain the overall image quality score. The effectiveness of the proposed IQA scheme has been demonstrated with six public benchmark IQA databases.

[19] Address the problem of detecting face spoofing attacks by inspecting the potential of texture features based on Local Binary Patterns (LBP) and their variations on three types of attacks: printed photographs, and photos and videos displayed on electronic screens of different sizes. A publicly available face spoofing REPLAY-ATTACK database, containing all above 3 types of attacks.

[20] Presented an approach Inspired by image quality assessment, characterization of printing artifacts and

by differences in light reflection, for anti-spoofing based on learning the micro-texture patterns that differentiate live face images from fake images. Furthermore, reflected light from human faces and prints is different in many ways because a human face is a complex non rigid 3D object whereas a photograph is a planar rigid object. In this approach the micro-texture patterns are encoded into an enhanced feature histogram using multi- scale local binary patterns (LBP). In addition, the texture features are used for spoofing detection as well as for face recognition. This provides a unique feature space for coupling spoofing detection and face recognition.

In [21] the spoofing detection has been detected using 3D projective invariant for moving face.Starting from a set of automatically located facial points, we geometric invariants for detecting replay attacks was exploited. The presented results demonstrate the effectiveness and efficiency of the proposed indices.It appears that a robust anti-spoofing technique must rely not only on verifying captured face three-dimensionality, but also on a specific user interaction with the system. A face detection module analyzes each input frame and returns the detected face. Location is performed by implementing a cascade combination of the Viola Jones' algorithm with an Extended Active Shape Model, realized by STASM software as in [22]. STASM searches relevant landmarks by minimizing a global distance between candidate image points and their homologues on a general model (shape model), which is pre-computed over a wide set of training images. 68 interest points are located, a subset of which is used for invariants computation. Among the most robust methods, we mention those combining 3D verification and user interaction. In this work we presented a system in this category exploiting projective invariants. Our approach can verify if the face is truly 3D still maintaining a low computational cost. User interaction allows to also detect more complex spoofing such as the presentation of pre-recorded videos. Experiments show effectiveness and efficiency of the method. In the current implementation, the system could not detect spoofing via a 3D moving facial mask.

In [23], Li et al. described a method for print-attack detection by exploiting differences in the 2D Fourier spectra comparing the hard-copies of client faces and real-accesses. In that work, the authors derive the probability of attack by applying a high-pass filter to the spectra of the sample being analyzed and computing a score which is then classified according to some heuristic. The method works well for down sampled photos of the attacked identity, but is likely to fail for higher-quality samples. The used dataset is not publicly available.

In [24], the authors proposed a method to detect spoofing attacks using printed photos by analyzing the micro-textures present in the material using a linear SVM classifier to achieve a 2.2% False-Acceptance Rate (FAR) against a 13% False- Rejection Rate (FRR). A major limitation of this method is that the input image needs to be reasonably sharp. In contrast to the works cited above.

The authors in [25], [27] presented a technique to evaluate liveness based on a short sequence of images. The work describes a binary detector that evaluates the trajectories of select parts of the face presented to the input sensor using a simplified optical flow analysis followed by a heuristic classifier. Such a classification scheme achieves an equal-error rate of 0.5% for samples of real accesses extracted from XM2VTS and attacks produced using hard-copies of those data. The same authors also introduced in [26] a method for fusing scores from different expert systems that observe, concurrently, the 3D face motion scheme introduced on the previous work and liveness properties such as eye-blinks or mouth movements.

The works in [28] and [31] brings a real-time liveness detection specifically against photo-spoofing using (spontaneous) eye blinks which are supposed to occur once every 2-4 seconds in humans. The system developed uses an undirected conditional random field framework to model the eye-blinking that relaxes the independence assumption of generative modelling and state dependence limitations from hidden Markov modelling. The system is tested on a dataset provided by the authors and was made publicly available. Such a dataset is composed of short video clips of eye-blinks and spoofing attempts using photographs. The attacks are not solely composed of still images but also arbitrary shaking behavior which increases the task difficulty. With this setup, the proposed detector is able to achieve 95.7% true-positive classification against a false alarm of less than 0.1% when considering a simultaneous blink of both eye lids in all test samples.

A later work by the same authors [29] augment the number of countermeasures deployed to include a scene context matching that helps preventing video- spoofing in stationary face-recognition systems. To achieve this, the eye-blink detector output scores are fused with the output of a simple local-binary-pattern- _2 detector. The scene context detector uses some carefully chosen fiducial points coming from near regions outside the face boundaries that characterize the expected scene context. To test this new setup, the authors constructed a new private dataset with which they obtained an almost perfect scoring
- 99.5% true-rejection against 100% true-acceptance.

The earliest studies in mask detection aim to distinguish between facial skin and mask materials by exploiting the difference in their reflectance characteristics. This idea can be traced 30 years back to [33], which claims that a face thermogram is not vulnerable to disguises and even plastic surgery can be detected, since it reduces the thermal signature of face. Later, stating that disguises can be detected even better in near-infrared, Pavlidis and Symosek propose to utilize the 1.3-1.7 μm sub-band of the upper band [34]. Simple thresholding is suggested for classification, without reporting any experimental results, but only illustrations. Two more studies that follow the same way of thinking are published with systematic experiments and results [32], [35]. A multi-spectral analysis is proposed in both, claiming that fake, by its definition, is indistinguishable for human eyes and therefore, using only visual images is not sufficient to detect the attacks. On the other hand, they both handle the mask

attack problem in an evasion/disguise scenario rather than spoofing since they don't examine masks that are replicas of valid users to be impersonated.

In [35], the authors conduct experiments on different mask materials such as silicon, latex or skin-jell to see how different they behave in reflectance when compared to facial skin that is sampled from the forehead region. For this purpose, the distribution of albedo values for illumination at various wavelengths are analysed and two best wavelengths, one from visual and one from near-infrared spectrum (685 and 850 nm) are selected. Finally, the resulting 2D vectors that consist of radiance measurements under these illuminations and strictly at a distance of 30cm from the sensor are classified as skin or non-skin via Fisher's linear discriminant. The method is reported to detect fake faces with 97.78% classification rate. However, the possibility of occlusion in the forehead region and the imposed range limitation restricts practical application. Additionally, in this study, masks don't even exist since the analyses are done directly on mask materials.

In [36], three baseline face recognition algorithms are implemented to observe the spoofing performances of the masks. In their experiments, a probe sample is compared to the enrolment (gallery) sample of the claimed ID and a binary decision is made based on a similarity metric. In their analysis, the authors do not designate an enrolment set, but instead they employ a method that is referred as *all vs all* and propose two scenarios. In the first scenario, the baseline performance is assessed by only using the real access samples (DB-r) in the database. Each DB-r sample is compared with all other DB-r samples. This results in two types of scores: *real genuine scores* if the compared samples belong to the same user and *real impostor scores*, otherwise. In the second scenario which is referred as the mode under spoofing attacks, mask attack samples (DB-m) are utilized as the probe set. Each sample in DB-m is compared with all DB-r samples, again resulting in two types of scores, that is *mask genuine* and *maskimpostor scores*. The results are reported for both identification and verification settings as rank-1 close-set identification and Equal Error Rates (EER), respectively. Although this analysis gives an idea about the spoofing potential of 3D facial masks, it suffers from two major problems.

Firstly, one can strongly argue that spoofing is irrelevant in a close-set identification setting. This is because the probe will always be assigned to an identity in the gallery irrespective of the attack quality. Identity match can be achieved as long as the mask better resembles the target, compared to enrolment samples of other IDs. Secondly, in the verification setting considered for the second scenario, mask impostor scores are obtained by matching DB-m images to DB-r samples of IDs different than the one targeted by the attack. This is irrational since no attacker would produce an attack for a valid user and claim the identity of another. Additionally, the verification setting does not really evaluate the vulnerability of the recognition systems since apart from the algorithms used, their specifications, e.g. operating thresholds, are not determined and fixed using a development set. The correct approach would be to evaluate mask genuine scores against real genuine scores, which congregates the two scenarios in one score space and enables us to calculate false acceptance rates at the same operating point for both real and fake access scenarios.

Later in [38], two fusion schemes, at feature and score levels, are proposed to combine previously proposed LBP histograms calculated from the 2D and 2.5D images. Results are given in the same previous manner; best performances obtained by tuning the decision threshold on the test set. While the 2D and 2.5D modes give 89.4% and 82.4% classification rates separately, the fusion of these two modes increases this rate to 93.5%. Additionally, a proper analysis is included in the paper on the impact of the mask attacks and the proposed counter measure method on two baseline (2D and 3D) face recognition algorithms. The detection error trade-off (DET) plots reveal that without any counter measures 3D masks can be highly detrimental to both 2D and 3D face recognition performances.

Most recently NelsiErogmus proposed spoofing face recognition with 3D masks [37], Theaim was to inspect the spoofing potential of subject-specific 3D facial masks for different recognition systems and address the detection problem of this more complex attack type. In order to assess the spoofing performance of 3D masks against 2D, 2.5D, and 3D face recognition and to analyze various texture based countermeasures using both 2D and 2.5D data, a parallel study with comprehensive experiments is performed on two data sets: the Morpho database which is not publicly available and the newly distributed 3D mask attack database.

Two types of experiments are conducted on both databases: Face verification experiments in which success rates of spoofing attacks with 3D masks are assessed using baseline face recognition algorithms. Anti-spoofing experiments in which mask attack/real face classification accuracies of aforementioned counter measure methods are measured. Firstly by assessing spoofing performances on 2.5D and 3D systems, secondly by analyzing each mask separately with LOOCV and lastly experimenting on another 3D mask spoofing database which has been used in some of the previous studies but is not publicly available, in addition to 3DMAD. The parallel evaluations of LBP based anti-spoofing methods on these two databases allowed to associate previously published results on the Morpho database with our current work and with possible future studies on 3DMAD.

Furthermore, the success rates of LBP based features in 3D mask attack detection are assessed via exhaustive tests using three different classifiers. Theresults for both 2D and 2.5D images indicate an advantage in the block-based approach. Among different LBP types tested, modified LBP is observed to deliver best results for Morpho database, despite its shorter length compared tomulti-scale LBP which was proposed in previous publications. On the other hand in 3DMAD, regular block-based LBP shows the

best performance for both 2D and 2.5D data. As for classification, LDA and SVM are found to be better than $\chi 2$, while LDA is proved to be best in case of 3DMAD database.

6. CONCLUSION

In this paper, as one of the objectives in the project, we present an overview of current research of spoofing mechanisms used for face in biometrics. Algorithms and features used in are broadly discussed. Their pros and cons are briefly summarized for reference. The study of the vulnerabilities of biometric systems against different types of attacks has been a very active field of research in recent years [2]. Spoofing is a real concern with regard to security of biometric system. More and more successful spoofing attempts are being published. It is possible to combat spoofing attacks with liveness detection testing but all of these countermeasures come at certain price often affecting user convenience, hardware prices. Another point that needs to be deliberated is the utilization of mask attack samples for training the anti-spoofing systems. Ideally, a countermeasure algorithm against spoofing should be able to decide whether the face image captured by the sensor belongs to a real face or not, regardless of the attack type. Because it is not realistic for a biometric system to employ a different anti-spoofing module for each attack type. In all of the previous works and in this study, the classifiers are trained using both real and attack samples.

REFERENCE

[1] J. Galbally, R. Cappelli, A. Lumini, G. G. de Rivera, D. Maltoni, J. Fierrez, et al., "An evaluation of direct and indirect attacks using fake fingers generated from
)SO templates," *Pattern Recognit. Lett., vol. 31,no. 8, pp. 725–732, 2010.*

[2] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in Proc.)EEE)JCB, Oct. 2011, pp. 1–7.J. (ennebert, R. Loeffel, A. (umm, and R.)ngold, "A new forgery scenario based on regaining dynamics of signature," *in Proc. IAPR ICB, vol. Springer LNCS-4642. 2007, pp. 366–375.*

[3] Hennebert.J, R. Loeffel, A. (umm, and R.)ngold, "A new forgery scenario based on regaining dynamics of signature," *in Proc. IAPR ICB, vol. Springer LNCS-4642. 2007, pp. 366–375.*

[4] A. Hadid, M. Ghahramani, V. Kellokumpu, M. Pietikainen, J. Bustard, and M. Nixon, "Can gait biometrics be spoofed?" *in Proc. IAPR ICPR, 2012, pp. 3280–3283.*

[5] Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Evaluation of serial and parallel multibiometric systems under spoofing attacks," *in Proc. IEEE 5th Int. Conf. BTAS, Sep. 2012, pp. 283–288.*

[6] K. Nixon, V. Aimale, and R. K. Rowe, "Spoof detection schemes," *Handbook of Biometrics, 2008.*

[7] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," *Computer Vision ECCV 2010, vol. 6316, pp. 504-517, 2010.*

[8] Y. Li and X. Tan, "An anti-photo spoof method in face recognition based on the analysis of fourier spectra with sparse logistic regression," *in Chinese Conference on Pattern Recognition, 2009.*

[9] J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of fourier spectra," *in In Biometric Technology for Human Identification, 2004, pp. 296-303.*

[10] J. Bai, T. Ng, X. Gao, and Y. Shi, "Is physics-based liveness detection truly possible with a single image?" *in International Symposium on Circuits and Systems. IEEE, 2010, p. 3425-3428.*

[11] V. N. Vapnik, "The nature of statistical learning theory". *Springer, 1995.*

[12] K. Kollreider, H. Fronthaler, and J. Bigun, "Nonintrusive liveness detection by face images," *Image and Vision Computing, vol. 27, no. 3, pp. 233-244, 2009.*

[13] N. Erdogmus and S. Marcel, "Spoofing 2D face recognition systems with 3D masks," in *Proc. Int. Conf. Biometrics Special Interest Group*,2013.

[14] Y. Kim, J. Na, S. Yoon, and J. Yi. "Masked fake face detection using radiance measurements". *Journal of the Optical Society of America A, 26(4):760–766,2009.*

[15] Z. Zhang, D. Yi, Z. Lei, and S. Li. "Face liveness detection by learning multispectral reflectance distributions". *In IEEE International Conference on Automatic Face Gesture Recognition and Workshops, pages 436 –441, March 2011.*

[16] N. Kose and J.-L. Dugelay. "Countermeasure for the protection of face recognition systems against mask attacks". *In IEEE International Conference on Automatic Face and Gesture Recognition, April 2013.*

[17] J. Maatta, A. (adid, and M. Pietikainen. "Face spoofing detection from single images using micro-texture analysis". *In International Joint Conference on Biometrics, pages 1–7,2011*.

[18] A. Liu, W. Lin, and M. Narwaria, ")mage quality assessment based on gradient similarity," *IEEE Trans. Image Process., vol. 21, no. 4, pp. 1500–1511, Apr. 2012.*

[19] A. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," *in Proc. IEEE Int. Conf. Biometr. Special Interest Group, Sep. 2012, pp. 1–7.*

[20] J. Maatta, A. (adid, and M. Pietikainen, "Face spoofing detection from single images using micro-texture analysis," *in Proc. IEEE IJCB,Oct. 2011, pp. 1–7.*

[21] Maria De MarsicoSapienzaUniversità di Roma v. Salaria 113, 00198, Rome (IT),Michele

NappiUniversità di Salerno v. Ponte don Melillo, 84084, Fisciano (IT), Daniel RiccioUniversità di Salerno v. Ponte don Melillo, 84084, Fisciano (IT), Jean-Luc DugelayInstitut EURECOM, Sophia Antipolis, (France)"Moving Face Spoofing Detection via 3D Projective)nvariants," *EurecomTABULA RASA.*

[22] S.Milborrow, F. Nicolls., "Locating facial features with an extended active shape model," *European Conf. Computer Vision*, pp. 504–513, 2008.

[23] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia. "On the vulnerability of face verification systems to hill-climbing attacks." *Pattern Recogn.*, 43(3):1027–1038, 2010.

[24] J. Bai, T. Ng, X. Gao, and Y. Shi. ")s physics-based liveness detection truly possible with a single image?" *In Circuits and Systems ISCAS Proceedings of 2010 IEEE International Symposium* on, page 34253428. IEEE, 2010.

[25] K. Kollreider, H. Fronthaler, and J. Bigun. "Evaluating liveness by face images and the structure tensor". *In Fourth IEEE Workshop on Automatic Identification Advanced Technologies AutoID05*, pages 1–6. IEEE, 2005.

[26] K. Kollreider, (. Fronthaler, and J. Bigun. "Verifying liveness by multiple experts in face biometrics".)n *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, pages 1– 6. IEEE, 2008.

[27] K. Kollreider, (. Fronthaler, and J. Bigun. "Non-intrusive liveness detection by face images". *Image and Vision Computing*, 27(3):233–244, 2009.

[28] G. Pan, L. Sun, Z. Wu, and S. Lao. "Eyeblink-based anti-spoofing in face recognition from a generic webcamera". *IEEE 11th International Conference on Computer Vision* (2007), pages 1–8, 2007.

[29] G. Pan, L. Sun, Z. Wu, and Y. Wang. "Monocular camera-based face liveness detection by combining eyeblink and scene context". *Telecommunication Systems*, 47(3-4):215–225, 2011.

[30] G. Pan, Z. Wu, and L.Sun. "Liveness detection for face recognition".)n K. Delac, M. Grgic, and M. S. Bartlett, editors, *Recent Advances in Face Recognition*, page Chapter 9. IN-TECH, 2008.

[31] G. Pan, Z. Wu, and L. Sun. "Liveness detection for face recognition". *Recent Advances in Face Recognition*, (December):109–124, 2008.

[32] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li, "Face liveness detection by learning multispectral reflectance distributions," *in Proc. IEEE Int. Conf. Autom.Face Gesture Recognit. Workshops*, Mar. 2011, pp. 436–441.

[33] F. J. Prokoski, "Disguise detection and identification using infrared imagery," *Proc. SPIE*, vol. 0339, pp. 27–31, Jun. 1983.

[34] I. Pavlidis and P. Symosek, "The imaging issue in an automatic face/disguise detection system," *in Proc. Workshop Comput. Vis. BeyondVis. Spectr., Methods Appl.*, 2000, pp. 15–24.

[35] Y. Kim, J. Na, S. Yoon, and J. Yi, "Masked fake face detection using radiance measurements,"*J. Opt. Soc. Amer. A*, vol. 26, no. 4, pp. 760–766, 2009.

[36] N. Kose and J.-L. Dugelay, "On the vulnerability of face recognition systems to spoofing mask attacks," *in Proc. IEEE ICASSP*, May 2013, pp.2357–2361

[37] NesliErdogmus, and Sébastien Marcel, "Spoofing Face Recognition with 3D Masks" *IEEE transactions on information forensics and security*, vol. 9, no. 7, july 2014.

[38] N. Kose and J.-L. Dugelay, "Shape and texture based countermeasure to protect face recognition systems against mask attacks," in *Proc. IEEEConf. CVPRW*, Jun. 2013, pp. 111–116.

BIOGRAPHY

Mrs. SRUTHIMOL P, PG Scholar in Rathinam Technical Campus, Anna University Tamil Nadu, India. Received Bachelor of Technology, in the stream of Information Technology from Anna University, Tamil Nadu, India and also completed IBM Mainframe certification. Participated in National Conference on Topic Biometric Identification and Verification for Face: An analysis and also in various other National Level Workshops and Seminars. Area of Interest is Biometrics security, Face Recognition and Mainframe.

Ms. PRADHEEBA P, Assistant Professor, completed her Master of Engineering in Angel College of Engineering and Technology affiliated to Anna University, Chennai, Tamil Nadu, India and her Bachelor of Engineering from Nehru Institute of Engineering and Technology, affiliated to Anna University, Coimbatore, Tamil Nadu, India. Her area of interest is Networking and Cloud Computing. She has presented papers in various National conferences and International conferences on emerging technologies. She has participated in many seminars, workshops, national conference and international conferences on various topics. She is a active member in IAENG. She has published paper in IEEE Explore and in International Journal of Internet Computing and various other Journals.

