3D Mask fake face detection using near set theory

Ms. Neha Kuchankar, Prof. S. D. Zade

Abstract— **Spoofing is the act of masquerading as a suitable user by falsifying data to gain an unlawful access. Susceptibility of recognition systems to spoofing attacks (presentation attacks) is still an open security issue in biometrics domain and among all biometric behavior, features is uncovered to the most severe hazard, ever since it is mainly effortless to admittance and replicate. In this paper, lots of dissimilar types of features spoofing attacks have been examined and various algorithms have been proposed to differentiate them. Largely focusing on 2D attacks counterfeit by displaying printed photos or replaying recorded videos on mobile diplomacy, a momentous part of these studies land their arguments on the flatness of the spoofing material in front of the feeler. On the other hand, through the advancement in 3D renovation and printing technology, this assumption can no longer be maintained. Here we aspire to examine the spoofing potential of subject-specific 3D facial masks for different recognition systems and address the detection problem of this more composite assail type. In order to measure the spoofing presentation of 3D masks against 2D,2.5D, and 3D features detection and to analyze various texture based countermeasures using equally 2D and 2.5D data, a comparable study with complete experiments is performed on two data sets: the Morpho database which is not publicly available and the newly distributed 3D mask attack database. The result existing in the effort undoubtedly propose that the analysis of the general image quality of real face samples reveals highly valuable information that may be very efficiently used to discriminate them from fake images.**

Index Terms— **Spoofing, presentation attack, feature recognition, masks attack.**

I. INTRODUCTION

Being the most commonly used biometric trait by humans, face recognition has become an active research topic for many decades now and it has found great application in consumer electronics and software. Face be obliged its character principally to being simply and non-intrusively reachable compared to further biometric traits like finger print or iris.

However, this advantage becomes a limitation in spiteful circumstances, enabling attackers to create copies and spoof features recognition systems without any difficulties. Spoofing assail is the act of outwitting a biometric system by presenting a false testimony in order to gain substantiation [1]. It is relatively simple to forge such an attack for facial
recognition systems, due to the point that the photographs or videos of a official user can be simply captured from a distance or obtained via internet, e.g. through social networks. Official users (simply users or clients) can be defined as the persons that are enrolled in a face acknowledgment system. An attacker can try to gain access by only showing their printed photos or replaying their recorded videos to the sensor.

This noticeable susceptibility of face has evoked great interest in the biometric society and lots of papers have been published on countermeasure studies. Mainly as a result of their simplicity and low-cost, the previously mentioned photo print and video replay attacks [2] constitute the focus of research activities in this domain. Existing anti-spoofing approaches against these type of attacks can be generally classified into three groups: texture analysis, motion analysis and liveness detection.

Assuming the occurrence of cues like printing artefacts [3]and/or blurring [4], many anti-spoofing techniques examine the texture of the taken face image. Congurently, in a recent study [5], micro-texture analysis using multi-scale local binary forms is proposed. It can be claimed that this type of methodologies highly depends on the quality of the printed image or video display. The second group of methods aims to suspect spoofing attacks by analyzing the motion in the scene based on the fact that planar objects like a sheet of paper or a mobile phone screen move in a significantly different way compared to real faces. For example, in [6], the trajectories of small regions of face images are examined to be classified as real or false. In a related manner, by computing geometric invariants of a set of automatically located facial points, Marsicoetal. [7] exploit the same singularity. Finally in the last group of methods, liveness of the face is determined based on live-face specific gestures such as eye blinking [8] or lip movements [9]. However, approaches of this kind are bound to fail in the case of video replay attacks or even more basically, with photographic masks which are really high resolution facial prints worn on face after the eyes and mouth regions are cut out, as claimed in [10].Similarly in [11], it is again shown that with eyes cut out from the photos, customary visible liveness detection method still suspect blinking, in further words, cannot distinguish a photo attack. Recently, several studies have been published that present methodical and reproducible analyses of several of these and some other methods, with a shared determination of providing similar results on public databases [12]–[14]. Work on fraud detection capabilities for face is still limited and a substantial part of it is based on the flatness of the captured surface in front of the sensor during an attack. This is also true for approaches that examine the 3D nature of the face by employing additional devices, which is much more realistic now with the introduction of affordable consumer depth cameras like Kinect. For instance, in [15], 3D data acquired with a low-cost sensor is utilized to localize face and at the same time to test its authenticity to decrease their system's vulnerability to spoofing attacks.

II. LITERATURE SURVEY

Author in this paper [1] focuses on the face recognition ,which has become an active research topic for many decades now and it has found great application in consumer electronics and software.

The earliest studies in mask detection aim to distinguish between facial skin and mask materials by exploiting the difference in their reflectance characteristics. The authors explore another type of counter measure technique based on reflectance analysis in [12]. The proposed method utilize the variational retinex algorithm to decompose face texture images into reflectance and illumination components.

Technique:- Local Binary Pattern (LBP) based counter measure to detect mask attacks is tested on two modes: color images and depth maps.

Author in this paper[2] author in this paper focuses on Multimodal biometric systems.Which are usually believed to be more robust to spoofing attacks than unimodal systems, as they syndicate information coming from dissimilar biometric traits. Although recent work has shown that multimodal systems can be misled by an impostor even by spoofing only one biometric trait, this result was obtained under a very obstructive "worst-case" hypothesis, where the attacker is supposed to be able to perfectly replicate a genuine biometric trait[15]. This hypothesis allows one to simulate the similar scores of spoofing attacks by sampling from the distribution of the genuine matching scores, without any need of constructing realistic fake traits. However, whether and to what extent this hypothesis holds under realistic fake traits is still an open issue. In this paper, we address the above issue by verifying the validity of the "worst-case" assumption on several data sets consisting of realistic deceiving attacks, and considering a multimodal authentication system based on face and fingerprint biometrics. Our results disclose some interesting insights about the design of multimodal verification systems; in particular, on the choice of the score fusion rule, that should take into account robustness to realistic spoofing attacks.

Technique **:-**In this section, we discuss our experimental analysis and results, whose main goal is to verify if the "worst-case" hypothesis holds for realistic spoofing attacks, and if it can be reliably exploited for designing robust fusion rules. Some interesting insights on the development of robust fusion rules are also highlighted on the basis of the reported results.

This section is organized as follows: the data sets used in our analysis are described, the performances of different fusion rules under realistic and worst-case spoofing attacks are reported, and the distributions of realistic spoofing attacks are eventually shown.

Author in this paper[3] deal with the problem considered in this paper is how to approximate sets of objects that are qualitatively but not necessarily spatially close each other. The term qualitatively near is used here to mean closeness of descriptions or distinctive features of objects. The solution to this problem is stimulated by the work of Zdzisław Pawlak during the early 1980s on the classification of objects by means of their attributes. This article presents a unusual theory of the nearness of objects that are either static (do not change) or dynamic (change over time). The basic method is to consider a link relation, which is defined comparative to measurements associated with features shared by objects independent of their 3-D relations[14]. One of the outcomes of this work is the introduction of new forms of approximations of objects and sets of objects. The closeness of objects can be approximated using rough set methods. The planned approach to estimate of objects is a straightforward extension of the rough set approach to approximating objects, where approximation can be considered in the context of information granules (neighborhoods). In addition, the typical rough set approach to concept estimate has been enriched by an increase in the number of granules (neighborhoods) associated with the classification of a concept as near to its approximation. A byproduct of the proposed approximation method is what we call a near set. It should also be observed that what is presented in this paper is considered a special (not a general) theory about nearness of objects. The influence of this article is an approach to nearness as a vague concept which can be approximated from the state of objects and domain knowledge.

*Technique:-*Nearness, Structural Inclusion, and Structural Indiscernibility Based on Part-Whole Relation.In this section, we outline an approach to approximation of a nearness relation. This relation is unclear and should be learned from sample objects and domain knowledge.

III. PROPOSED SYSTEM

Figure 1 shows the proposed research methodology. In which first we are taking colour input images from the dataset. After recognizing face from the dataset we are plotting landmarks on all the images. Finally we are implementing near set theory and SVM classifier on the landmark plotted images and compare the results. Basically 1st we train the data set.

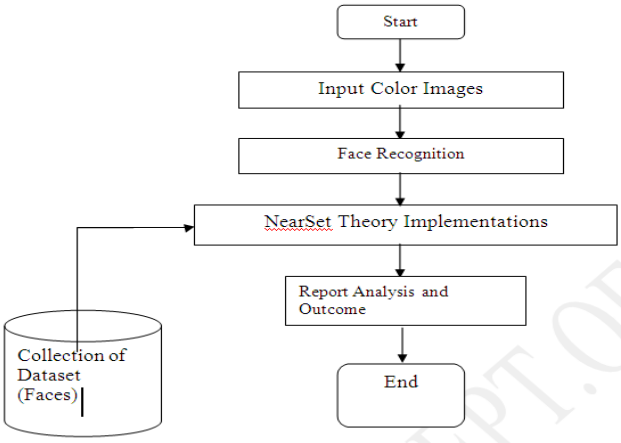

Fig. 1: Proposed research methodology.

We took face images and calculate landmarks of that image and store them for calculating the landmarks we use ASM (Active shape model algortihm).example shapes from a training set of 300 labelled faces (see Figure 2 for an example image showing the landmarks). Each image is annotated with 133 landmarks. The shape model has 36 parameters, and can explain 98% of the variance in the landmark positions in the training set. Figure 3 shows the effect of varying the first three shape parameters in turn between ±3 standard deviations from the mean value, leaving all other parameters at zero. These 'modes' explain global variation due to 3D pose changes, which cause movement of all the landmark points relative to one another. Less

significant modes cause smaller, more local changes. The modes obtained are often similar to those a human would choose if designing a parameterised model, for instance shaking and nodding the head, or changing expression. However, they are derived directly from the statistics of a training set and will not always separate shape variation.

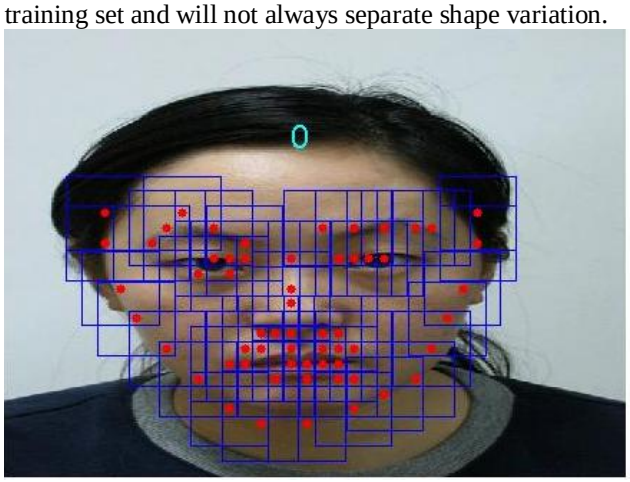

Fig. 2: Landmark plotted image.

Fig. 3: Examples shapes from training set of faces

In testing module we take input of mask and then apply ASM on it to calculate landmarks of input image. After calculating landmarks we apply near set theory to obtain related image of mask image.

A. Near set Theory

Near sets are either spatially close or descriptively close. Spatially close sets have nonempty intersection[15]. The underlying assumption with descriptively close sets is that such sets contain elements that have location and measurable features such as colour and frequency of occurrence. The description of the element of a set is defined by a feature vector. Comparison of feature vectors provides a basis for measuring the closeness of descriptively near sets. Near set theory provides a formal basis for the observation, comparison, and classification of elements in sets based on their closeness, either spatially or descriptively[18]. Near sets offer a framework for solving problems based on human perception that arise in areas such as image processing, computer vision as well as engineering and science problems. Descriptively close sets contain elements that have matching descriptions. Such sets can be either disjoint or non-disjoint sets. Spatially near sets are also descriptively near sets

IV. EXPERIMENTAL RESULTS

In the first module we are recognizing face by extracting image from the collection of data set through the browse button as shown in figure 4.1 and figure 4.2.After recognizing image it is showing the extracted image as shown in figure 4.3.

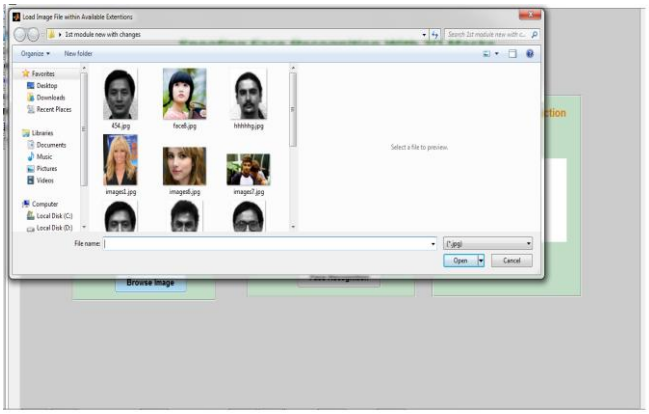

Fig. 4.1: First Module

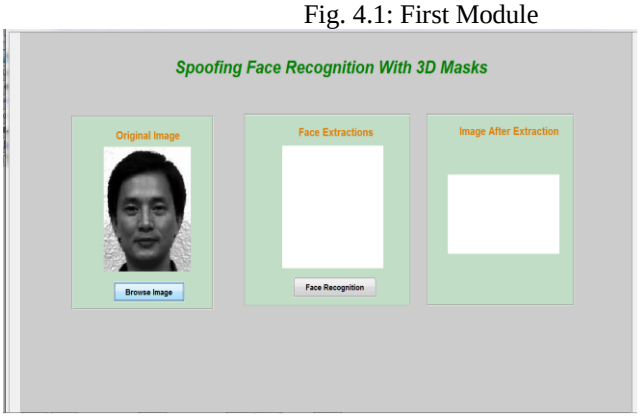

Fig. 4.2: First Module

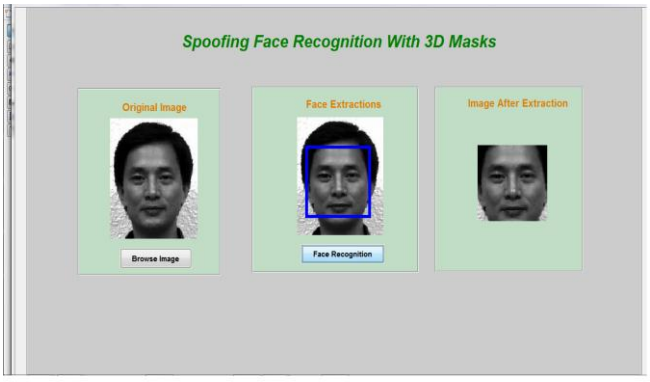

Fig. 4.3: First Module

In the second module we are plotting ladmark on the trained dataset of 3D mask images as shown in figure 5.1, and 5.2.

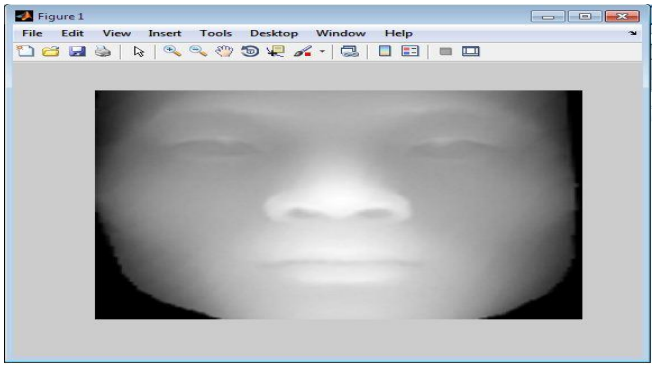

Fig. 5.1: Second Module

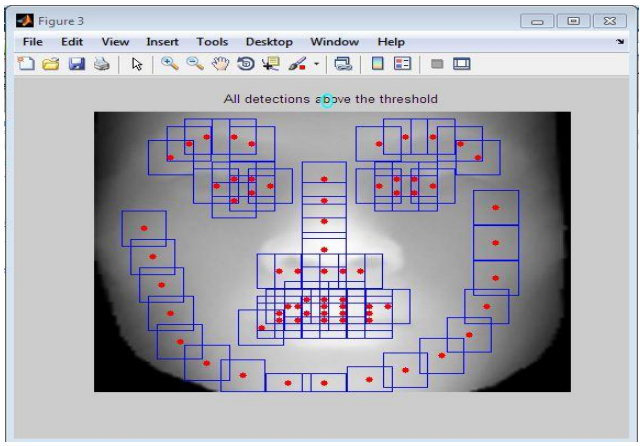

Fig. 5.2: Second Module

In the third module we are applying near set theory and svm classifier for results comparison. After comparing results we concluded that results of near set theory are giving the nearest accurate results. Also the time required to fetch the nearest result from the dataset for nearset theory is less than SVM classifier.

Fig. 6.1 : Third Module

In the below figure 6.1 first we will load the input and after applying classifier on that input image it will show 13 landmark plotted images comparrision (as shown in figure 6.2). Out of the 13 images it will show the best match after as shown in figure 6.3.

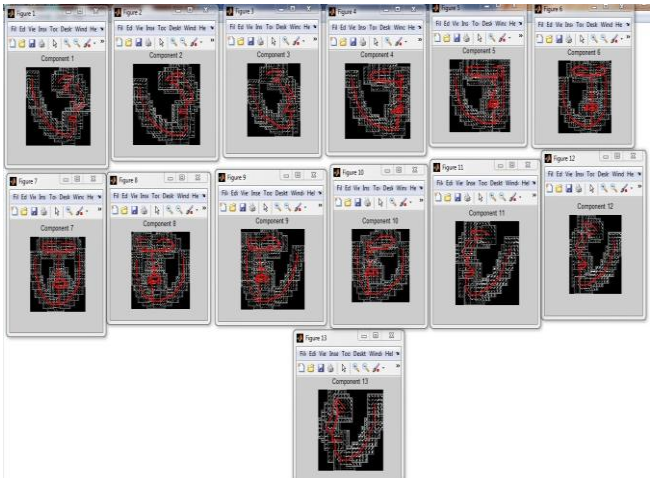

Fig. 6.2 : Third Module

As shown in figure 6.3 near set theory took 0.25339 seconds while SVM took 49.5066 seconds.According to te accuracy near set theoryis fetching the same nearest matched real time input image of loaded input while SVM is fetching any random image from the data set .

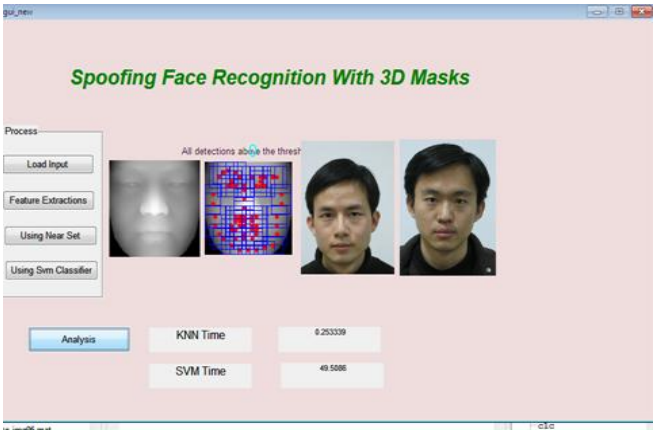

Fig. 6.3 : Third Module

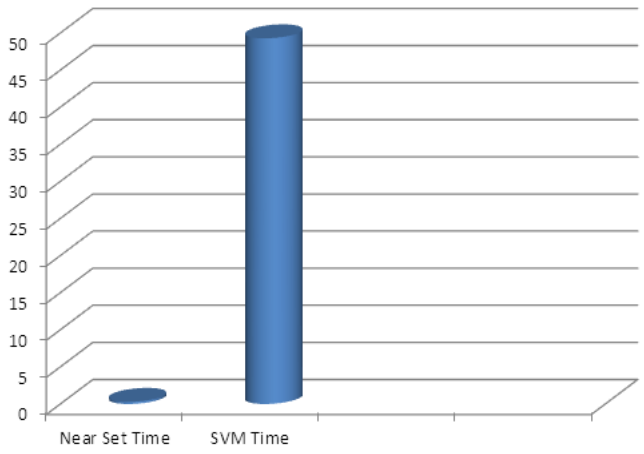

Fig 6.4: Time complexity graph

V. ACKNOWLEDGMENT

Professor S. D. Zade has guided me along the way for the completion of this paper and the project. With his support and expert advice on the subject matter I was able to complete this paper successfully. I thank him for his valuable input and time.

VI. CONCLUSION

Spoofing attacks continue to be a security threat for biometric recognition systems and face is among the most vulnerable traits due to its high accessibility. Majority of previous studies in face spoofing focus on preventing 2D attacks performed by displaying printed photos or replaying recorded videos on mobile devices. However, utilization of 3D masks for face spoofing attacks has become easier and cheaper with the advancements in 3D reconstruction and printing technologies. In our paper, we aim to contribute to the current state of the art in the research domain of 3D mask attacks.We aim to provide the nearest accuracy using near set theory also the efficiency will be increased.

VII. REFERNCES

[1] K. Nixon, V. Aimale, and R. Rowe, "Spoof detection schemes," in *Handbook of Biometrics*, A. Jain, P. Flynn, and A. Ross, Eds. New York, NY, USA: Springer-Verlag, 2008, pp. 403–423.
[2] B. Biggio, Z. Akhtar, G. Fumera, G. L. Marcialis, and F.Roli,"Security evaluation of biometric authentication systems under real spoofing attacks," *IET Biometrics*, vol. 1, no. 1, pp. 11–24, Mar. 2012.
[3] J. Bai, T.-T. Ng, X. Gao, and Y.-Q. Shi, "Is physics-based liveness detection truly possible with a single image?" in *Proc. IEEE ISCAS*, May/Jun. 2010, pp. 3425–3428.
[4] J. Maatta, A. Hadid, and M. Pietikainen, "Face spoofing detection from single images using micro-texture analysis," in *Proc. IEEE IJCB*, Oct. 2011, pp. 1–7.
[5] G. Pan, L. Sun, Z.Wu, and S. Lao, "Eyeblink-based anti-spoofing in face recognition from a generic webcamera," in *Proc. IEEE ICCV*, Oct. 2007, pp. 1–8.
[6] G. Chetty and M. Wagner, "Multi-level liveness verification for face-voice biometric authentication," in *Proc. Biometrics Symp., Special Session Res. Biometric Consortium Conf.*, Sep./Aug. 2006, pp. 16.
[7] 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.
[8] M. M. Chakka *et al.*, "Competition on counter measures to 2-D facial spoofing attacks," in *Proc. IJCB*, Oct. 2011, pp. 16.
[9] 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.
[10] 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.
[11] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li,"A face antispoofing database with diverse attacks,"in*Proc. IAPR ICB*,Mar./Apr.2012,pp.26-31.
[12]R. W. Frischholz and U. Dieckmann. Bioid: A multimodal biometric identification system. *Computer*, 33(2):64–68,Feb. 2000.
[13] R. W. Frischholz and A. Werner. Avoiding replay-attacks in a face recognition system using head-pose estimation. In *Proceedings of the IEEE International Workshop on Analysis*
[14] Z. Pawlak, R. Slowinski, "Rough Set approach to multi attribute decision analysis", Invited Review, Eur. Journal of Oper. Res., Vol.72, 1994, pp. 443-459.
[15] P. Chen, G. Wang, Y. Yang, J. Zhou, "Facial Expression Recognition based on Rough set theory and SVM", Lecture Notes in Computer Science, Springer Berlin/ Heidelberg, Rough sets and knowledge Technology, Vol. 4062, 2006, pp. 772-777.

Neha Kuchankar, *Department of Computer science and Engineering, Priyadarshini Institute Of Engineering And Technology, Nagpur, India.*
Prof S. D. Zade, *Department of Computer science and Engineering, Priyadarshini Institute Of Engineering And Technology,*

