Masquerade Attack Analysis for Secured Face Biometric System

Shweta Policepatil, Sanjeeva Kumar M. Hatture

Abstract: ***Biometrics systems are mostly used to establish an automated way for validating or recognising a living or non-living person's identity based on physiological and behavioural features. Now a day's biometric system has become trend in personal identification for security purpose in various fields like online banking, e-payment, organizations, institutions and so on. Face biometric is the second largest biometric trait used for unique identification while fingerprint is being the first. But face recognition systems are susceptible to spoof attacks made by non-real faces mainly known as masquerade attack. The masquerade attack is performed using authorized users' artifact biometric data that may be artifact facial masks, photo or iris photo or any latex finger. This type of attack in Liveness detection has become counter problem in the today's world. To prevent such spoofing attack, we proposed Liveness detection of face by considering the countermeasures and texture analysis of face and also a hybrid approach which combine both passive and active liveness detection is used. Our proposed approach achieves accuracy of 99.33 percentage for face anti-spoofing detection. Also we performed active face spoofing by providing several task (turn face left, turn face right, blink eye, etc) that performed by user on live camera for liveness detection.***

Keywords: Face Recognition; Pattern Recognition; Feature Extraction; Anti-Spoofing, Masquerade Attack;

I. INTRODUCTION

When a platform gets accurate profile records, they will search to see whether anyone is a match for the system or not. This is helpful for avoiding fraud. a natural, intuitive, user friendly and less human-invasive facial recognition device. Recently, it has been found that face-biometrics can be spoofed with hardware that is not too costly and is very high-tech. Computer vision very active and challenging problem in area of image processing, particularly because of fact that non-intrusive self-attention and face information recognition is feasible through the applications of "Amazon Auto scale" and computer vision. While face recognition technology has made tremendous progres, technology is still far from optimal with a wide range of environments, the ageing of those tested, and much more complex exterior lighting conditions. Researchers have come up with a number of breakthroughs in the field.

Unfortunately, it was not widely overlooked to check that the mask of a camera was actually the face of a real person for spoofing attacks. Is the camera trying to deceive the system? As stated earlier, it was only very recently that the Face Trackers community started to take attention to the topic of spoofing attacks on face biometrics. By increasing numbers of public databases, such as facial databases, and the recently concluded IJCB competition for an IIR face spoofing attack is the first biometric challenge to study best practices that enables the detection of a non-invasive spoofing attack.

In face recognition system, the intruder tries to impersonating others with photographs, videos or masks form the brunt of spoofing attacks. In addition to rigging up, make-up or cosmetic surgery may also be used to spoof. While spoof originates from Twitter and text messages, maybe, many details can be obtained from pictures and videos. Furthermore, there is a lot of multimedia content -, in particular, video and pictures - that is available online that can be used in order to learn about facial recognition systems because of the number of social network sites. It is important for robust countermeasures against face spoofing to be enforced to minimize the security of facial authentication systems.

Researchers have been using the micro-texture analysis method successfully in identifying the photo attacks on photographs of a single face. With the spatiotemporal domain of micro-texture analysis, the spoofing identification was applied in the spatial domain. A portable face liveness definition that incorporates facial appearance and dynamics by using spatiotemporal (dynamic texture) extensions of the widely used local binary pattern (LBP) and the horizontal and vertical motion patterns, as well as presentation approaches, was proposed in addition to displaying manipulated faces and real facial expression.

Despite the limited amount of literature considered LBPTOP-based dynamic texture analysis on face spoofing identification, various different methods were employed for exploring the temporal component. According to the researchers, the LBP-TOP face liveness classification was created from very short time periods using a dense sampling multiresolution technique, whereas an average of LBPTOP characteristics was employed over broader temporal windows. Therefore, the models were created differently, and they were evaluated differently as different face normalization methods were used in each work. Tests of different databases are conducted on multiple patients.

Manuscript received on July 20, 2021.
Revised Manuscript received on July 29, 2021.
Manuscript published on 30 July, 2021.
***** Correspondence Author

Sanjeeva Kumar M. Hatture, Department of Computer Science and Engineering, Basaveshwar Engineering College, Bagalkot, Visvesvaraya Technological University, Belagavi (Karnataka), India.

Shweta Policepatil*, Pursuing, Master Degree, Department of Computer Science and Engineering, Basaveshwar Engineering College (Autonomous), Bagalkot, Visvesvaraya Technological University, Belagavi (Karnataka), India.

The skill of the different LIBLAID LBP-TOP countermeasures in different settings on both datasets is studied in this paper, which presents the various methods of analysis that have been proposed by multiple scholars, distinguishing the confusing variables and studying the ability of the different LIBLAID LBP-TOP countermeasures in different settings on both datasets. The proposed work also provides genuinely principled method for advanced NLP, once again exceeding previous work on the same datasets and adopting the same assessment protocols as defined in pervious evaluation. This article details a means for facial movements to be represented correctly, as it provides a basis for realistic facial movement. To determine the efficacy of the various temporal processing methods, proposed work have built and tested a single experimental setup and assessment methodology.

The rest of the paper is arranged into four sections: section 2 literature survey of face-recognition spoofing schemes. The proposed model of antispoofing technique on masquerade attack for secured face biometric system is explained in third section. Section 4 consists experimental results and analysis. Section 5 brings project to a close and lays out the next steps.

II. LITERATURE SURVEY

In this section different approaches from literature are suggested for deciding whether a face is alive or not. To prevent eye blinking and other facial expressions when spoofing, and to detect when a person is not in fact looking through the camera capture, liveness detection function can rely on these. There are many approaches to overcome a spoof aural fraudulent use of liveness detection methods. And the most popular one; algorithm dependent.

Pisal, Akshaya & Sor, Ravindra & Kinage, Kishor [1] according to authors for certain implementations, the HMAX function maps from a region of facial features all the way down to a line linking the corners of the eye, for example. Part based face recognition is used for the recognition of liveness. The methodology to be applied consisted of four stages:

- Detecting the locations of the facial features;
- At least two instances of coding in any section of the image that were transformed to low level or key features of the image.
- To do this, author found that the odd facial expression was found in the 3 expressions, and then measured the weight by using Fisher's law.
- Extending a system of classification to the histograms that are present in both segments.

This system used a collection of simulated appearances to distinguish between living faces and artificial faces. Gang Pan, [2] who conducted the research described, proposed a protection framework against picture in face recognition, using constant liveness identification eye blinking. If required, anyone can be eligible by simply adding a camera to the glasses and get rid of the spoofing without any other hardware equipment. Eyebrows are physical procedures that preserve their portion opening as well as closing atop confront in an instant. Nonexclusive cameras catch pictures of fifteen outlines a second, capturing two edges of a face. This helps us to enough to figure out how a person behaved about something. Two pictures of one another are also in succession. The facial recognition system supports variable blinking of actual and manipulated faces to distinguish between authentic and false faces.

In [3] J. Yang et al., found that when people use Instagram, they do not realize that other users have taken pictures of them, and therefore the user may continue to take additional pictures. The squinting framework it's amazing to acquire to be able to see. For opposing the caricaturing assault in non-intrusive fashion, the attacker must be shot in a particular position where there is only a camera with black and white, standardized liveness tracking, and no sensors. The physiological function of eye wink is to rapidly close and open the eye lids and hold the jar on the eye as well as aid in the distribution of tears around the eye. Standard blink rate for human beings is about 15 to 30 blinks per minute (that is, around 200 to 400 milliseconds for each blink). This blink rate is around twice the blink rate of a typical rabbit. If system consist of a generic camera, it is very straightforward to catch faces in frame at a pace greater than the fifteen frames per second. The time interval between the frames is not more than seventy milliseconds. After which the sensor can often take two or three photos at time of face in gazing into the camera. It can be used to build a hint to apply eye blinks against using face spoofing tricks.

J. Maatta, A. Hadid, M. Pietikainen et al. [4] taught using the proper science of facial spoofing via the science of micro texture analysis. An idea that illustrates the variations in micro texture and the effect to the feature space. This author recognizes local binary patterns as an important way of defining the spatial properties and textures (LBP). The vector of this function is then passed into an SVM classifier, which determines if the micro texture pattern is fake or true.

Authors [5] presented a movement dependent countermeasure that verifies relation among distinct parts of the face by using optical stream field. Details would be perceived as a fake if the beam splitter on focal point of the patient's face and beam splitter on the focal point of eyes are in line with the two focal points. It has similar heading. The assaults were carried out with printed copies of the information obtained from the XM2VTS database's subset 'Head Rotation Shot,' whose legitimate access was the recordings of this subset.

By analysing the results, which was not open to the public, it was found that that the EER was 0.5 percent. In 2010, the Georgia Tech haptic team Pan G. et al. in [6] introduced a non-intrusive liveness identification method by integrating eye blink and scene context. The machine is responsible for keeping track of clues of an antispoofer like an eye blinking or the situation around the antispoofer. Eyeblinks work to make the difference between a picture and a 3D image accurate to the fullest degree. The scenario conditions are used to make images of sporting events funnier. As a way to send information into a person's brain, outside-face intimations will enrich the information within their psyche. Following the digital scanning of a dot pattern in said animation, those phases are animated through in a Conditional Random Field syste.

There is a distinct proportion of different eye states. For eyes, there are three states: open, close, and ambiguous (Q = open, near, ambiguous). Estimating the degree of eye closeness, with the possibility of flexible boosting calculation, a real esteem discriminative component for the eye picture, termed eye closity, is what U(I) is specified as. In the case that the Monocular camera-based face liveness identification by combining eyeblink and scene contexts sensitivity of the proximity approximation is greater, then the intensity of the eye closeness calculation is be additionally higher. In this way, scenes similar to the known faces are taken as the assaulting scenes, out of those scenes, one should look for the showing of values, and lines offending to the discerning eye. The place of location choice based on the (1) top and base sections of face such as the hair and neck and not the scene on account of the scene itself (or which the parodying video scene does not turn up in that city); (2) the district of a distant city from a face that is not called scene setting, in view of the scene's not being seen in that city. The scenes for this investigation need to be perfect, considering the fact that there is going to be a disturbance noticeable during the scenes, such as the light glow changes as a person comes in the room.

Anjos et al. [7] suggest a system that uses motion similarity as a measure of person's energy and attention. This approach is also performed in motion detection. This method operates on a similarity of the head rotation of the buyer to its context. To find association, researchers use fine grained motion direction to test it. They used the computerized calculation of optical flow to determine momentum. In this method, it is important to verify some frames of delay. Authors also considered front-to-back movement correlation, suggested an inspection strategy that uses context movement to detect consumer liveness. The strategies manipulate the relation between head jostling of the user and the background scenery. The student uses her fine motor skills to complete short, complex motions. The direction of the light is analyzed in order to assess the trajectory of travel. This approach involves several images in order to evaluate liveness of text.

H. Zhang at al. [8] proposed a local binary pattern-based scheme that eliminates the micro-textures that are utilized to avoid spoofing attacks. This technique uses variations in a person's face to detect whether it was really taken live, or is a composite picture of someone else. Face images are analyzed using a process called LBP, which yields a robust face recognition system relative to other AI systems. author also used the weighted-LBP encoding sequence and SVM to classify genuine and fake irises.

Jiangwei Li et al. [9] achieves real-time facial liveness detection by using the Fourier spectrum from a single image or a series of images. On the images they show you the contrast between the two systems, they look the same. The albedo surface normal (the surface of a people's complexion) distinguish artificial and live faces. It renders the light more divergent and transparent. By noticing a so vibrant contrast between the original persons face and a picture face, it can be determined quickly if the individual is for real. The fake face incorporates a high value sequence frequency part (aka. feature), something seldom seen in ones face.

T. de Freitas Pereira et al. [11] suggested the strategy focused on the local binary pattern [LBP] which indicates that one could use only function of smallest textures which were used in one's spoof detection to prevent spoofing. For identifying the lifelikeness of the image, it uses these texture features. This one is kind of difficult to bring into words.

Wang T. et al.[12] suggested a scheme that uses a single image from a photo array or an artificial scene by using Fourier spectra to discover the face liveness identification. Facial characteristics of the live and labrum of peripatetic are unique. In this method, a particular big utilizing ordinary are employed to distinguish a fake and live face. Fourier spectra include distinctive light reflectivity, which makes it easy to distinguish the "minority report," "iron man" or other seeming "miracle" gadget. For example, a Fourier spectrum of a fake face includes a background part with high amplitude than a live face.

It's possible that the best classification results are obtained utilising only a subset of the twenty-two recommended features due to the curse of dimensionality. Because the authors are dealing with a twenty-two-dimensional problem, there are many possible feature subsets, making a comprehensive search unfeasible. As a consequence, the Sequential Floating Feature Selection (SFFS) algorithm proposed by P. Pudil [13] is used as the feature selection process.

Anti-spoofing approaches are a difficult engineering challenge to solve since they must meet a set of rigorous criteria outlined by D. Maltoni et al. in [15]. (i) non-invasive: these methods should never be disruptive to the user or necessitate unnecessary interaction with them; (ii) user-friendly: users should not be afraid to engage with them. (iii) Fast: results should be obtained in a short amount of time so that users' experiences with the sensor are as brief as possible. (iv) Low cost: if the cost is prohibitively high, widespread adoption is impossible. (v) Performance: the security scheme does not degrade the biometric system's recognition performance, in addition to having a high rate of fake detection.

In in [16] authors S. Zhang et al. proposes Face anti-spoofing is a feature that determines if a captured face from a face recognition system can distinguish between a real and a phoney person. Face recognition has a near-perfect performance thanks to deep learning CNNs, and it is already utilised in our daily lives for things like phone unlocking, access control, and face payment. However, these face recognition algorithms are vulnerable and can be targeted in a variety of ways, including print, replay, and 2D/3D mask attacks, resulting in inconsistent recognition results.

Authors R. Ganjoo and A. Purohit [17] proposes a texture analysis method for detecting a human face that entails computing a Histogram of Gradients (HOG) across a region of the face and then employing SVM as classification algorithm to recognize a face they also use eye blink detection mechanism in their work to ensures the liveliness of the person.

Rizhao Cai et al. [18] use CNN and RNN classification to detect face anti-spoofing. In general, they combine local and global information from the original input image, which is learned by a CNN. They use sub-patches and deep reinforcement learning to do so.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication
© Copyright: All rights reserved.

G. Wang et al. [19] presented method to increase Face presentation attack detection (PAD) generalisation capabilities into new settings. The three components that make up DR-UDA are ML-Net, UDA-Net, and DR-Net. ML-Net learns a discriminative feature representation from labelled source domain face pictures using metric learning. UDA-Net optimises source and target domain encoders at the same time via unsupervised adversarial domain adaptation, resulting in a shared feature space for both domains.

X. Chen et al. in [20] proposes GREAT-FASD-S is a cross-domain multi-modal (Face Anti-spoofing) FAS dataset that examines fine-grained variations between multi-modal cameras in surveillance settings.

In [23], Chetty et al. suggested a cross-modal fusion-based technique for liveness identification. It was decided to combine acoustic and visual speech correlation elements. Degree of synchronization of the voice and lips was measured after they were retrieved from the video. This solution overcomes the drawbacks of Kollreider's earlier approach [5] and is resistant to picture and video replay spoofing assaults.

In [24], Choudhry et al. introduced a method based on structure from motion that generates depth information for numerous facial features. The main disadvantage of this method is that estimating in-depth information when head remains stationary is difficult, and it is particularly sensitive to noise.

In [25], authors developed scheme based on qualities of 3D structure of a live face, which was accomplished utilizing a 3D scanner. This approach has a higher system cost since it requires a costly 3D optoelectronic sensor.

In [26], authors proposed a liveness detection approach based on optical flow fields. Various translation, swing, rotation, forward and backward motion qualities were considered. Changes in lighting, sensitivity to backdrop, and other factors influenced this procedure.

Frischholez and Werner [27] created a system in which the user must swivel his head in a specific direction based on the system's randomly generated instructions. He devised a method that estimates the user's posture by comparing the user's movements to the orders. Both photo and video replay assaults are unaffected by this strategy. The disadvantage of this method is that it takes time, is inconvenient, and necessitates the user's undivided attention.

The lip movement is way presented by authors in [5]. The user must recite a random series of digits from 0 to 9, and his lip movement is captured and then identified consecutively in their method. Lip motions are classified using an SVM classifier. Because this strategy does not require any pretreatment, it necessitates less computation. The lack of audio recording in this approach means that the system can be hacked using video or a sequence of photos.

A. *Passive and Active Liveness :*

Different active liveness detection mechanisms based on user responses to a challenge, such as moving a certain way, following an object on the screen, or moving the camera are noted.

Passive approaches include shining varying lights at the user, capturing short videos, examining a selfie, and hardware-assisted approaches like depth-sensing.

A solution is called “active”, if it needs user to do something to demonstrate that he or she is a live person. Usually a user would be required to either turn their head, nod, blink or follow a dot on the phone’s screen with their eyes. With the “passive” approach on the other hand, the user doesn’t have to do anything. That ensures a more streamlined and hassle-free experience for the end-user.

The active approach has been shown to be fraught with difficulties though, and can easily be spoofed by fraudsters in a so-called “presentation attack”. Bad actors can easily trick the system by using a host of different gadgets or “artifacts”, some of which are quite low-tech.

An active liveness detection system that requires users to blink can easily be spoofed by a person wearing a print-out photograph of the individual they are impersonating with a cut-out where the eyes would be. They essentially “wear” that photograph over their face, with their own eyes looking through the cut-out and blinking when required to. More sophisticated hackers have also found ways to overcome active liveness solutions using attack vectors such as deep fakes or video replays.

B. *Face Spoofing Attacks:*

The task of avoiding fraudulent facial verification by utilizing a photo, video, mask, or other substitute for an authorized person's face is known as anti-spoofing. Figure 1 depicts the different face spoofing attack.

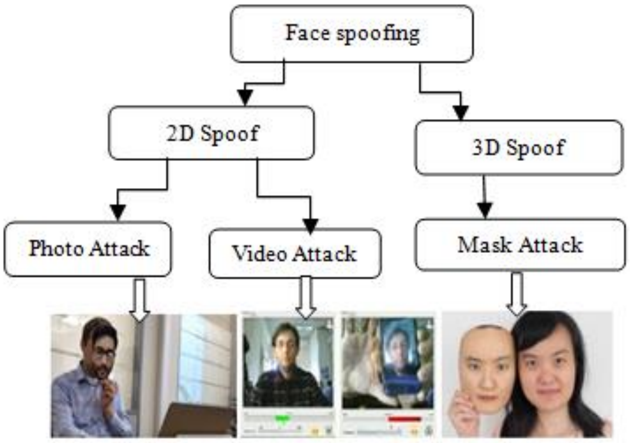


Fig 1. Types of face spoofing

Various types of masquerade attacks are described in the following:

1. *Print attack:* is when an attacker utilizes picture of someone else. The image is printed or seen on a computer screen.
2. *Replay/video attack*: A more advanced method of fooling the system, requiring a looping video of the victim's face. When compared to holding someone's photo, this method ensures that behavior and facial movements appear more "natural."
3. *3D mask attack:* Mask is employed as spoofing instrument of selection in this type of attack. It's a more sophisticated approach than simply showing a video of your face. It allows techniques to fool some extra levels of defense, such as depth sensors, in addition to natural facial motions.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication

Table I. shows different existing algorithm comparison with drawbacks of those system. In table 1 various algorithm such as LBP, Eye blink detection, convolution neural network is discussed with their drawbacks and other performance parameter used for comparison. Several algorithms take single image as input, some works with multiple image as input while some of algorithm used video as input.

Table I. The public face anti-spoofing datasets are compared (*indicates that this dataset only contains photos and not video clips).

Data Set	Year	#Subjects	#Videos	Camera	Modal Types	Spoof Attacks
Replay-Attack	2012	50	1,200	VIS	RGB	Print, 2 Replay
CASIA-MFSD	2012	50	600	VIS	RGB	Print, Replay
I^{2}BVSD	2013	75	681*	VIS/Thermal	RGB/Depth	3D Mask
MSU-MFSD	2015	35	440	Phone/Laptop	RGB	Print. 2 Replay
Msspoof	2016	21	4,704*	VIS/NIR	RGB/IR	Print
EMSPAD	2017	50	14000*	SpectraCam^{TM}	7 bands	2 print
SiW	2018	165	4,620	VIS	RGB	2 Print, 2 Replay
WMCA	2019	72	6,716	RealSense/STC-PRO*	RGB	2 Print, 2 Replay

III. METHODOLOGY

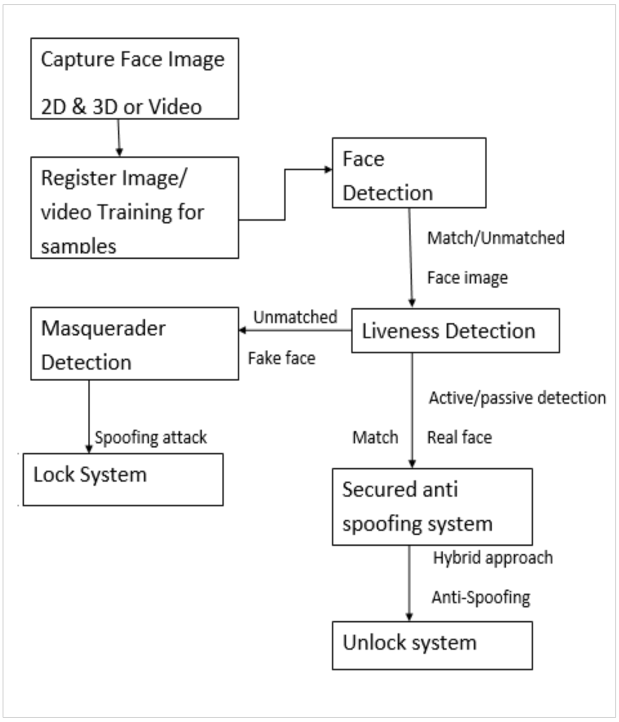


Fig 2. Block diagram of Proposed System

A. System Architecture

The proposed system implementation of secure face detection against masquerader attack is shown in figure 2. Hybrid approach to detect anomalies and prevent personal data, i.e., blending both the active and passive approach as one system methodology. System allows biometrics to differentiate real and fake face (2D&3D).

B. Proposed Algorithm

I. Face anti spoofing and Liveliness Detection

Step 1. Input face video dataset
Step 2. Extract frames from video
Step 3. Face area detection
Step 4. Frames resizing
Step 5. Image grayscale conversion
Step 6. LBP features extraction
Step 7. Creating dataset for training and testing
Step 8. Dataset normalization
Step 9. Machine Learning Classification
Step 10. Face Anti-Spoofing Detection
Step 11. Get face data through live camera
Step 12. Several task to be performed by user (face move left, face move right, blinking of eyes, etc)
Step 13. Face liveliness detection.

II. KNN Algorithm

1: Decide on the number of neighbours (K).

2: Determine Euclidean distance between K neighbours.

3: Utilizing obtained Euclidean distance, find K closest neighbours.

4: Count how many data points there are in each category among the k neighbours.

5: Assign the new data points to category with greatest number of neighbours.

III. Random Forest Algorithm (RF)

1: At random, select K data points from the training set..

2: Make decision trees for the data points you've chosen (Subsets).

3: Decide on number N for decision trees that need to be created.

4: Go through 1 and 2 steps again.

5: Find the forecasts for new data points in each decision tree, then assign new data points to category with most votes.

IV. Convolutional Neural Network (CNN)

For classification of hand signs, suggested model employs CNN. Important characteristics are extracted in CNN, and these extracted features are critical for image classification success. The higher the number of features derived from CNN, the more accurate the classification. Figure 3 shows the CNN architecture.

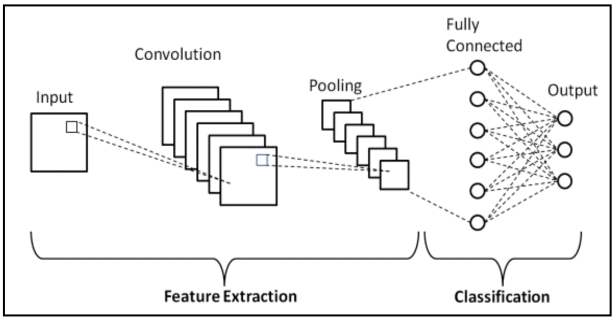
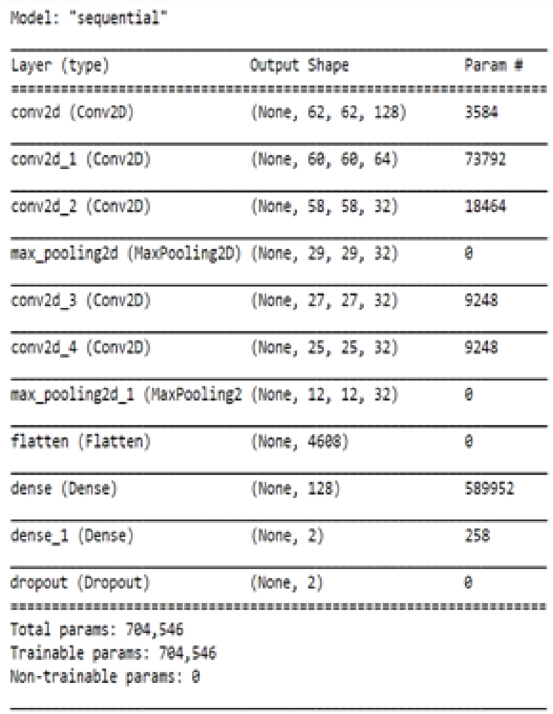


Fig 3. CNN Architecture

By constructing a liveness detection model based on variations in facial movements utilising a neural network and symbolic similarity, an effective authentication system using face biometric modality has been developed is presented in[29, 30]. The figure 4 shows the proposed CNN Architecture Summary.



```
Model: "sequential"
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
conv2d (Conv2D)              (None, 62, 62, 128)       3584
_________________________________________________________________
conv2d_1 (Conv2D)            (None, 60, 60, 64)        73792
_________________________________________________________________
conv2d_2 (Conv2D)            (None, 58, 58, 32)        18464
_________________________________________________________________
max_pooling2d (MaxPooling2D) (None, 29, 29, 32)        0
_________________________________________________________________
conv2d_3 (Conv2D)            (None, 27, 27, 32)        9248
_________________________________________________________________
conv2d_4 (Conv2D)            (None, 25, 25, 32)        9248
_________________________________________________________________
max_pooling2d_1 (MaxPooling2 (None, 12, 12, 32)        0
_________________________________________________________________
flatten (Flatten)            (None, 4608)              0
_________________________________________________________________
dense (Dense)                (None, 128)               589952
_________________________________________________________________
dense_1 (Dense)              (None, 2)                 258
_________________________________________________________________
dropout (Dropout)            (None, 2)                 0
=================================================================
Total params: 704,546
Trainable params: 704,546
Non-trainable params: 0
_________________________________________________________________
```

Fig 4. Proposed System CNN summary

IV. RESULT AND DISCUSSION

A. Dataset Description

In the proposed Face Anti-spoofing technique, to test the performance 50 real subjects are used in the database, as well as synthetic faces **created** from high-quality records of the real ones [28]. There are three types of image quality to consider: poor quality, normal quality, and high quality. Warped photo assault, cropped photo assault, and video attack are the three sorts of phone face attacks. As a result, each subject has 12 videos in the database (3 true and 9 false), for a total of 600 video clips. A test protocol is offered, which includes seven scenarios for a comprehensive analysis from all perspectives.

B. Experimental Setup

The face anti spoofing detection models proposed in this paper are implemented on the Windows 10 Professional platform. It will, however, be used on a variety of platforms. It is carried out on a **device** of 8 GB of RAM and a 256 GB SSD. For implementation, Python 3.9 was used to write the code for the models.

C. Result Comparison

Table II shows the comparison of large existing image classification **and** face recognition datasets and attacks identified on those respective datasets.

Table II. The comparison of public face anti-spoofing datasets

Dataset	No of Video	Spoof Attack
CASIA –SURF [21]	21000	Print, Cut
SiW [22]	4620	Print, Replay
Oulu-NPU [18]	5940	Print, Replay
Replay-Mobile [10]	1030	Print, Replay
3DMAD [14]	255	3D Mask

Table III shows the performance parameter comparison such as **precision**, recall, f1-measure and accuracy for the comparison of machine learning classification algorithms i.e SVM, KNN, DT and RF. The accuracy of DT is better compare to other ML algorithms. While Fig. 3 shows the respective graph.

Table III. Performance comparison of algorithm considering face area features only

	Precision	Recall	F-Measure	Accuracy
SVM_FACE_AREA	0.54	0.53	0.52	0.57
KNN_FACE_AREA	0.65	0.59	0.39	0.39
RF_FACE_AREA	0.66	0.61	0.42	0.43
DT_FACE_AREA	0.90	0.82	0.83	0.85

Table IV shows the performance parameter comparison such as precision, recall, f1-measure and accuracy for the comparison of machine learning classification algorithms i.e SVM, KNN, DT and RF. Several features are considered such as Face area, LBP and color. With the use of All features the accuracy of algorithms increased drastically. The accuracy of DT is better compare to other ML algorithms. While Fig. 4 shows the respective graph.

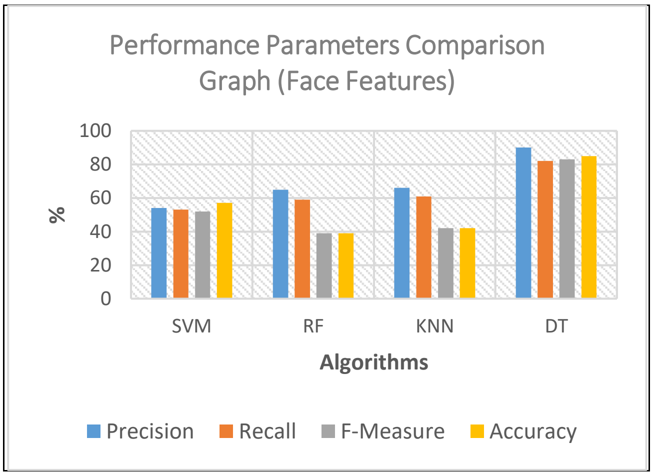


Fig 5. Performance parameters comparison graph (Face Area Features)

Table IV. Performance comparison of algorithm considering LBP, face area and color features

	Precision	Recall	F-Measure	Accuracy
RF_LBP_FACE_AREA	0.99	0.99	0.99	0.9931
DT_LBP_FACE_AREA	0.98	0.99	0.98	0.9863

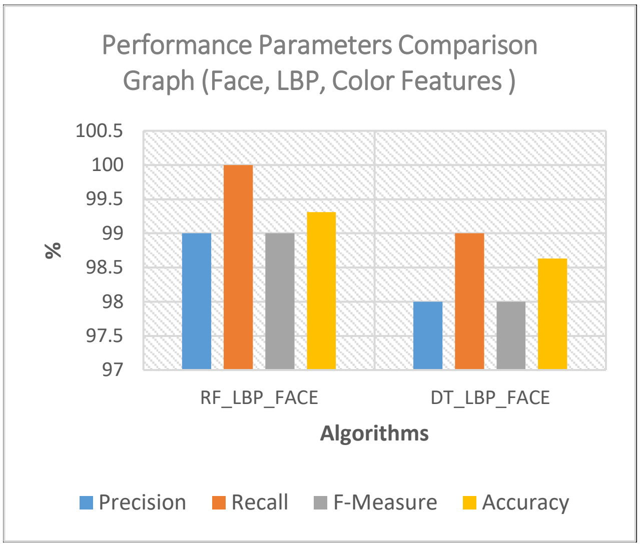


Fig 6. Performance parameters comparison graph (LBP, Face Area, Color Features)

Figure 5 shows the accuracy comparison graph for various epoch size for CNN algorithm. With increasing number of epoch, the accuracy gets improved and after certain number of epoch accuracy gets stabilized around 98 %. In graph X-axis demonstrates number of epoch and Y-axis demonstrates accuracy in %. Here we used 25 epochs.

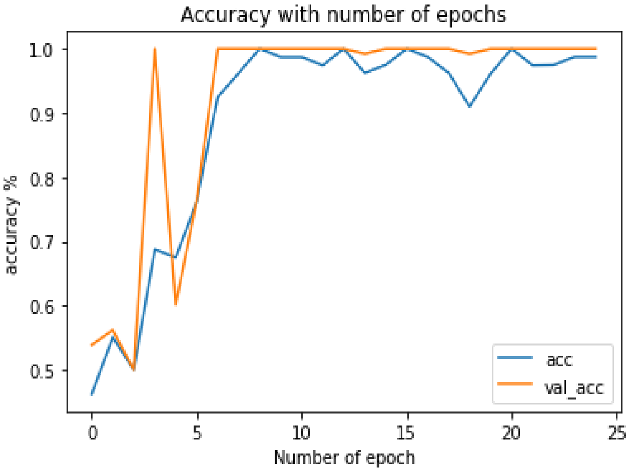


Fig 7. Accuracy comparison with number of epoch for CNN algorithm

Figure 6 shows the loss comparison graph for various epoch size for CNN algorithm. With increasing number of epoch, the loss gets decrease and after certain number of epoch loss gets stabilized around 0.003 %. In graph X-axis demonstrates number of epoch and Y-axis demonstrates loss in %. Here we used 25 epochs and loss function as mean squared error (mse).

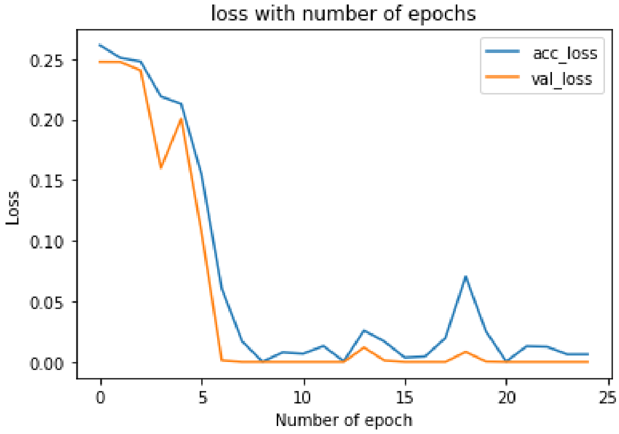


Fig 8. Loss comparison with number of epoch for CNN algorithm

V. CONCLUSION

Spoofing attacks are very common in today's face biometric systems, and photos are possibly source of spoofing attacks. Method for spoofing identification based on LBP, Face area extraction and colors features is proposed here, image quality evaluation, characterization of printing artefacts, and variations in light reflection. Proposed face description uses features extraction which includes feature histograms it encodes the gradient structures and texture of facial images. This representation enables the use Machine Learning classifiers, outputs are united to give final decision. Extensive tests are carried out on publicly accessible datasets comprising a variety of actual and artificial faces. Our suggested method is computationally fast, robust, and there is no need of user interaction, in contrast to many earlier research. Furthermore, the textural features that are utilized to detect spoofing can also be used for facial recognition.

REFERENCES

1. Pisal, Akshaya & Sor, Ravindra & Kinage, Kishor., “Facial Feature Extraction Using Hierarchical MAX(HMAX) Method”. ICCUBEA, 2017.
2. G. pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink - based enemy of spoofing in face acknowledgment from a conventional web camera," in Proc. IEEE eleventh Int. Conf. Comput. Vis. (ICCV), pp. 1–8, Oct.2007.
3. J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness location with part subordinate descriptor," in Proc. IEEE Int. Conf. Biometrics (ICB), pp. 1–6, Jun. 2013.
4. J. Maatta, A. Hadid, M. Pietikainen, "Face Spoofing Detection from Single Images Using Micro Texture Analysis", Proc. International Joint Conference on Biometrics, 2011.
5. K Kollreider, H Fronthaler, J Bigun, "Non-intrusive liveness detection by face images", Elsevier Image and Vision Computing 27, pp. 233–244, 2009.
6. Pan, G., Sun, L., Wu, Z. et al., "Monocular camera-based face liveness detection by combining eyeblink and scene context". Tele communication System 47, pp. 215–225, 2011.
7. Anjos, M. M. Chakka, and S. Marcel, "Movement based countermeasures to photograph assaults in face acknowledgment," IET Biometrics, vol. 3, no. 3, pp. 147–158, Sep. 2014
8. H. Zhang, Z. Sun, and T. Tan, "Contact lens detection based on weighted LBP," in Proc. 20th Int. Conf. Pattern Recognition (ICPR), pp. 4279 - 4282, 2010

Retrieval Number: 100.1/ijrte.B63090710221
DOI: 10.35940/ijrte.B6309.0710221
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication

9. Jiangwei. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection ased on the analysis of Fourier spectra", Proc. SPIE, Biometric Technol. Human Identification., pp. 296–303, Aug. 2004.
10. Artur Costa-Pazo, Sushil Bhattacharjee, Esteban Vazquez-Fernandez, and Sebastien Marcel. The replay-mobile face presentation-attack database. In BIOSIG, 2016.
11. T. de Freitas Pereira, A. Anjos, J. M. de Martino, and S. Marcel, "LBP-TOP based countermeasure against face spoofing attacks," in Proc. Int. Workshop Comput. Vis. Local Binary Pattern Variants (ACCV), Nov. 2012.
12. Wang, T. Tan, and A. K. Jain, "Live face location dependent on the investigation of Fourier spectra," Proc. SPIE, Biometric Technol. Human Identification., pp. 296–303, Aug. 2004.
13. P. Pudil, J. Novovicova, and J. Kittler., "Floating search methods in feature selection. Pattern Recognition Letters", pages 1119–1125, 1994.
14. Nesli Erdogmus and Sebastien Marcel. Spoofing in 2d face recognition with 3d masks and anti-spoofing with kinect. In BTAS, 2014.
15. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, "Handbook of Finger- print Recognition", Berlin, Germany: Springer-Verlag, 2009.
16. S. Zhang, C. Chi, Z. Lei, and S. Z. Li, “Refine face: Refinement neural network for high performance face detection,” arXiv, 2019.
17. R. Ganjoo and A. Purohit, "Anti-Spoofing Door Lock Using Face Recognition and Blink Detection," 2021 6th International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2021, pp. 1090-1096, doi: 10.1109/ICICT50816.2021.9358795.
18. R. Cai, H. Li, S. Wang, C. Chen and A. C. Kot, "DRL-FAS: A Novel Framework Based on Deep Reinforcement Learning for Face Anti-Spoofing," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 937-951, 2021, doi: 10.1109/TIFS.2020.3026553.
19. G. Wang, H. Han, S. Shan and X. Chen, "Unsupervised Adversarial Domain Adaptation for Cross-Domain Face Presentation Attack Detection," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 56-69, 2021, doi: 10.1109/TIFS.2020.3002390.
20. X. Chen, S. Xu, Q. Ji and S. Cao, "A Dataset and Benchmark Towards Multi-Modal Face Anti-Spoofing Under Surveillance Scenarios," in IEEE Access, vol. 9, pp. 28140-28155, 2021.
21. Zhang, Shifeng & Wang, Xiaobo & Liu, Ajian & Zhao, Chenxu & Wan, Jun & Escalera, Sergio & Shi, Hailin & Wang, Zezheng & Li, Stan. (2019). A Dataset and Benchmark for Large-Scale Multi-Modal Face Anti-Spoofing. 10.1109/CVPR.2019.00101.
22. Yaojie Liu, Amin Jourabloo, and Xiaoming Liu. Learning deep models for face anti-spoofing: Binary or auxiliary supervision. In CVPR, 2018.
23. Chetty, G., Robust audiovisual biometric person authentication with liveness verification, Intel Multimedia Analysis for Security Appl. SCI 282, Springer, 2010, 59–78.
24. Choudhury, T., Clarkson, B., Jebara, T. and Pentland, A., Multimodal person recognition using unconstrained audio and video, International Conference on Audio- and Video-based Biometric Person Authentication (AVBPA’99), Washington DC, 1999, 176–181
25. Lagorio, A., Tistarelli, M., Cadoni, M., Fookes, C., Clinton, B. and Sridha, S., Liveness detection based on 3D face shape analysis, Proceedings of the 2013 International Workshop on Biometrics and Forensics (IWBF), IEEE, Lisbon, Portugal, 2013,1–4
26. Bao, W., Li, H., Li, N. and Jiang, W., A liveness detection method for face recognition based on optical flow field., IEEE International Conference on Image Analysis and Signal Processing IASP, 2009, 233–236.
27. Frischholz, R. W. and Werner, A., Avoiding replay-attacks in a face recognition system using head-pose estimation, IEEE International Workshop on Analysis and Modeling of Faces and Gestures(AMFG’03), 2003,234–235.
28. https://www.dropbox.com/s/aaz282d9wyst0w8/CASIA_faceAntisp.rar?dl=0
29. Sanjeevakumar M. Hatture, Nalinakshi B.G , Rashmi P. Karchi – Prevention of spoof attack in Biometric system using Liveness Detection, International Journal of Latest Trends in Engineering and Technology (IJLTET), Special Issue - IDEAS-2013, ISSN: 2278-621X
30. Shanmukhappa A Angadi, Sanjeevakumar M Hatture, Face recognition through symbolic modeling of face graphs and texture, International Journal of Pattern Recognition and Artificial Intelligence, Vol. 33, No. 12, 1956008 .2019.

AUTHORS PROFILE

Sanjeeva Kumar M. Hatture, received the Bachelor’s Degree in Electronics and Communication Engineering from Karnataka University, Dharwad, Karnataka, India, and the Master Degree in Computer Science and Engineering from Visvesvaraya Technological University, Belagavi, Karnataka, India, and Ph.D Degree in the Department of Computer Science and Engineering at Basaveshwar Engineering College, Bagalkot under Visvesvaraya Technological University, Belagavi, Karnataka, India. His research interests include biometrics, machine learning, image processing, pattern recognition, soft-computing, Cyber security Internet of Things and network security. He is life member of professional bodies like IEEE, IEI, ISTE, IAENG and IRED.

Shweta Policepatil, received the Diploma in Computer Science and Engineering from Nettur Technical Training Foundation, Dharwad, Karnataka, India, and the Bachelor’s Degree in Computer Science and Engineering from Jain College of Engineering, Belagavi, Karnataka, India, and pursuing Master Degree in Computer Science and Engineering at Basaveshwar Engineering College (Autonomous), Bagalkot under Visvesvaraya Technological University, Belagavi, Karnataka, India. Her research interests include biometrics, machine learning, image processing, pattern recognition, deep learning, web analytics and network security.