Liveness Detection for Face Recognition System

Mrs. Jhansi Lakshmi[1*], B. Monica Sri[1], P. Harshitha[1], P. Pragna[1]
[1]*Department of Computer Science and Engineering, Vignan's Foundation for Science Technology and Research, Guntur, AP, India*
pjl_cse@vignan.ac.in

Abstract

The pandemic state of affairs turns each one's lives into online mode even though training had been undertaken via digital assembly sessions. But for a maximum of the conferences duplication or spoofing of faces turned into traced even for a few secured conferences in the event that they were given assembly hyperlinks they used to get connected. But our gadget helps, authenticated customers handiest can login and the relaxation could not make it possible. In this paper, face popularity is primarily based on a total identity technique used to offer authentication for the consumer there's an opportunity for face spoofing consequently the early level of the procedure is to confirm whether the face is actual or faux then modify the database include the registered one or not. To deal with this problem, face cascaded characteristics had been calculated and the usage of deep mastering technique and an answer turned finalized. We use face biometric authentication in an Open Authorization (OAuth) framework to regulate consistent access to internet resources. We enforce an entire face verification gadget that includes the detection of a living face accompanied by face authentication that makes use of Local Binary Patterns as functions for face popularity. The whole face recognition procedure includes offerings like a photograph registration service and a face liveness detection service.

Keywords: *Face recognition, deep learning, pandemic, virtual*

1. Introduction

A person's face can reveal a lot about their personality and emotional state. Face recognition is a fascinating and challenging topic with numerous applications, including law enforcement identification, banking, and security system access verification, and personal identification [1].

Authentication using facial recognition is susceptible to various attacks, particularly spoofing attacks. This attack influences the operator by representing the acquisition sensor in order to breach the system of biometric authentication. Especially, a face-duplication attack can be carried out by imitating the user with a 2D image, digital video, or 3D mask and thereby getting access as a valid user [2]. This helps to give the precautions to avoid spoofing or duplication attacks. Before validating the identification of the face, the collected measures are used to detect the "liveness". Those anti-spoofing methods are divided into two groups such as static techniques and dynamic techniques [3]. The static approaches work by examining a single 2D static snapshot. The analysis of the temporal properties of a sequence of input frames is the basis of dynamic approaches. Implementation of dynamic techniques is slow and hard. Moreover, some dynamic solutions demand users to follow instructions in order to confirm their existence, but not all users are willing to do so. The dynamic approaches become disadvantageous as a result of this. Traditional credentials are used by the OAuth protocol to verify the resource owner's identity [4], putting the privacy of users' data at risk. Therefore, creating reliable,

scalable, and maintainable systems has become an essential core of the function of security. So many safety procedures have been advanced to protect the customers' identities. These approaches are routinely used in online user authentication to manage access to users' data and verify their identities. Knowledge-based approaches, on the other hand, are prone to attacks such as man-in-the-middle, replay, and stolen-verifier assaults [5]. Based totally techniques are primarily based totally on something the consumer owns, along with a clever card or a token that may be reused, stolen, or manipulated. In each expertise and possession technique, the authentication gadget checks what the consumer is aware of or possesses in place of actually verifying the identification of the requester. Biometric authentication, on the other hand, checks the identity of requesters by examining their physiological and/or behavioral characteristics [6].

2. Literature Survey

We have summarized the innovative work from the current literature that is connected to our given study in this part. In [3], the authors suggested that DT recognition be approached in an innovative way. In order to blend motion and appearance, a volume LBP approach was devised. A simplified LBP-TOP operator was also described recently, which was based on concatenated LBP histograms generated from three orthogonal planes. Experiments on two DT datasets, as well as comparisons to state-of-the-art findings, demonstrated that our technique is effective for DT recognition. For the MIT and DynTex datasets, classification rates of 100% and 95.7% were obtained using VLBP and 100% and 97.1% using LBP-TOP. The authors in [7] seek to advance the state of the art in the field of 3D mask assaults by assessing spoofing performances on 2.5D and 3D systems, then analyzing each mask independently with LOOCV, and lastly experimenting on another 3D mask spoofing database. Face verification studies on 2D, 2.5D, and 3D baseline systems reveal that they are subject to facial mask spoofing attacks. They also show how the two types of masks used in the two databases differ. According to the findings, 3D MAD masks that rebuild face shapes using 2D pictures are less competent than those in the Morpho database that get facial shapes using a 3D scanner. In [4], the authors offered a thorough root cause analysis of security risks across the OAuth protocol's distinct phases. Replay attacks, network eavesdropping, forced-login CSRF attacks, and impersonation attacks were discovered by the attacker model to be frequent network assaults that attackers may exploit to impersonate users and get access to their protected resources.

The authors in [1] use the database search, identifying "matches" or "non-matches" based on distance or similarity measurements acquired from the pattern matcher, and lastly making a "accept/reject" decision-based on system policy. Finally, it makes a "accept/reject" decision depending on system policy. Under such a determination policy, any user's identity claim (positive or negative) whose pattern could not be obtained could be rejected. For an acquired pattern, the policy could declare a match for any distance less than a fixed threshold and "accept" a user identity claim on the basis of this single match, or it could declare a match for any distance less than a user-dependent, time-variable, or environmentally linked threshold and require a user identity claim on the basis of this single match. In [5], the authors suggest a method that takes into account the effect of a flashlight on a user's hair. The efficacy of liveness detection has improved by utilizing a low-cost auxiliary device, such as a flashlight. Using a dataset encompassing individuals with haircut-fringe hair, the suggested method is tested and compared to the existing method. The proposed features produce satisfactory results for the classifiers. The method's biggest flaw is that users' haircuts are restricted. In [6], the authors for the first time a countermeasure strategy for detecting mask attacks has been proposed. Because the mask attack database is 2D+3D, the proposed countermeasure can be used on 2D and 3D

data. An LBP-based method is presented as a countermeasure. On texture pictures, LBP-based techniques are commonly used. Although the number of research using LBP on depth maps is increasing, it is still not as frequent as it is with texture pictures. The results show that the technique works well on texture photos as well as depth maps.

The authors in [8] utilized visible and LWIR pictures to compare and contrast classical and state-of-the-art appearance-based face recognition systems. Human face LWIR imagery is not only a genuine biometric, but it is almost certainly superior to equivalent visible data. The authors in [9], approaches based on Gabor filtering or wavelets detecting the frequency contents of face image points or regions at various resolutions and orientations are generally effective, but computationally challenging. Faces can be considered as a composite of micro-patterns that are well characterized by the operator, which motivates the use of the computationally simple LBP operator for face description. Combining multiple texturing methods, such as employing Gabor filtering with LBP, could be a viable option. The authors in [10], for high-accuracy person recognition, constructed and evaluated a system that combines facial recognition and speaker identification modules. To merge the results of our face and speech modules, they employed a basic Bayes net. Deriving and adding confidence scores that can forecast each module's reliability makes this method very effective. The authors in [2], developed a method for detecting spoofing based on learning. the micro-texture patterns that distinguish real from false face photos. The suggested method encodes the results using multi-scale local binary patterns (LBP), which are then fed to a support vector machine classifier, which detects whether or not there is a living person in front of the camera. incorporating micro-texture patterns into a feature histogram.

The newly reported technique requires an estimate of fields or other direction-oriented features on target pictures, but it can significantly improve spoofing detection accuracy. This appears to apply to a wide range of assault types, as well as different media and support. Stationarity constraints can be eased by substituting smaller backdrop windows for bigger background windows, which limit the region around the face to the lowest set attainable for a specific condition. It is also possible to exchange processing time for accuracy by restricting the size of the time windows in which countermeasures are implemented. The tool used to generate the figures in the work [11] has been made open-source and publicly available such that our results may be duplicated.

To recognize the eyeblink behavior, the model dependencies among the observations and states in an undirected conditional graphical framework, incorporated a new-defined discriminative measure of eye state in order to expedite inference and convey the most effective discriminative information. The authors in [12], showed that the proposed approach can achieve great performance with just one typical web camera under uncontrolled indoor illumination circumstances, even while wearing glasses is permitted. The approach outperforms cascaded Adaboost and HMM in comparison experiments. In nature, the proposed eyeblink detection approach can be used for a variety of applications, including fatigue monitoring, psychological experimentation, medical testing, and interactive gaming. The authors in [13], summed up to begin, it introduces REPLAY-ATTACK, a novel spoofing attack database that includes three different sorts of conceivable attacks that use three different media and two different recording situations. The database offers a framework for training, development, and testing, as well as evidence of a baseline facial recognition system's vulnerability to attacks. Second, it offers a simple and repeatable LBP-based face spoofing countermeasure and investigates its effectiveness against a variety of attacks. The standard LBPu233shows the best

performance/complexity tradeoff among the LBP variants studied. The authors in [14], suggested the system's key feature is that it evaluated the trajectory of numerous face components utilizing the optical flow of lines. With an equivalent error rate of 0.5 percent on the test data, the liveness detection is successful in distinguishing live face sequences from still images in motion. The scheme's resilience was proven by further examination into actual implementation. Despite being limited to line velocity estimates, the proposed OFL is capable of providing reliable measurements for face liveness assessment. The implementation based on Gauss is both efficient and effective. In the case of face localization, a rapid technique based on optical flow patterns was also demonstrated to be possible. Furthermore, model-based Gabor feature classification's face component recognition is resistant to common sources of inaccuracy, such as glasses and facial hair.

For the nonlinear diffusion filter of [15], the authors have introduced totally stable additive operator splitting (AOS) techniques. These schemes meet all of the criteria for discrete nonlinear diffusion scale-spaces while being simple to implement in any dimension. In terms of computational and storage effort, the number of pixels has a linear relationship. AOS schemes on parallel architectures are implemented. These investigations show that by utilizing the inherent parallelism of AOS schemes, it is possible to achieve a speedup of an order of magnitude. Face liveness detection is now possible thanks to a component-based development approach. On three databases, they tested recognition performance. Various spoofing types present significant obstacles to earlier techniques in these databases. The most informative regions are kept, however, thanks to the introduction of H-Face. In the meantime, the authors in [16], apply Fisher criterion analysis to guide the pooling method, avoiding interferences between regions with different discriminant abilities. As a result, the proposed solution improves database performance across the board. The authors in [17] proposed a solution for modeling the difference in the illumination properties of live and fake faces, and use the diffusion speed. They proposed using the TV flow and AOS technique to compute the diffusion speed effectively and in a way that is resistant to changing illumination conditions. They attempted to encode the local pattern of diffusion speed values, known as the local speed pattern, to better capture the difference between real and false faces (LSP). The LSP-based scheme works in real-time and can thus be used on a variety of mobile devices.

The authors in [18], developed a unique approach for detecting liveness in facial recognition software that protects against picture spoofing. Based on the Lambertian model analysis, they investigated the different characteristics of imaging variation from a living person or a photograph, leading to the design of a novel approach for utilizing the data contained in the provided image. They proved that an illumination-invariant face recognition approach may be used to get the necessary latent samples, allowing us to create a sparse nonlinear/bi-linear discriminative model to distinguish the inherent surface properties of an image from those of a genuine human face. Experiments on a large picture imposter database show that the proposed technique works well for image spoof identification, with the advantages of real-time verification, non-intrusion, and no extra hardware needs. The authors in [19], attempts were investigated utilizing high-resolution printed photographs and photos obtained from LCD panels. Although there are various types of spoofing, we focused on recognition algorithms that only use one image. Even with dim photos, the proposed extension method for detecting spoofing attempts under changing illumination yields good classification results with low false positive and false negative rates. When compared to the state-of-the-art counterpart, the proposed

extension lowered the classification error by more than 50% for high-quality printing spoofs (NUAA Imposter Database) and more than 65 percent for recovered LCD images. Anti-spoofing is an urgent must with so many devices adopting facial recognition biometric authentication. The work in [20], proposes combining the CNN analysis model with the face liveness detection module for image input. The results of module testing reveal that the system can effectively avoid various sorts of face spoofing attacks. We put static and dynamic spoof face attacks to the test, including masks, photo posters, and digital pictures, as well as video replays. Further research could look into parallel programming techniques that could help facial recognition programs run faster.

3. Related Work

Face spoofing assaults might be made with the aid of using showing the face the usage of a show system like a phone or tablet. Efforts at assault which includes this create low-first-rate face textures and are without problems detected with the aid of using assessing HSV's sense and photo first-rate [14]. Color reproduction of display media, like motion pictures or photos, will likely be constrained as compared to the actual face. Besides, faces that are represented may also incorporate nearby color versions. The color gamut relies upon the show media, and friend's chroma versions might be defined with the aid of using analyzing the chroma channel's color feature. It additionally wishes to be tested wherein the color version gives the maximum precious micro-texture illustration with the aid of using extracting LBP (Local Binary Pattern) facts from diverse color spaces [11]. This way is needed to research spoofing in regions with insignificant lighting.

The software program-primarily based on a totally anti-spoofing assault detection technique has a low fee and better precision that has grown quick withinside the ultimate numerous decades. Early utility structures require customers to blink, flow their lips or appear in line with instructions [12] that might successfully reply to print strikes, however additionally the person revel in is terrible, and it can't react to video playback assaults. The researchers commenced investigating an evaluation machine primarily based totally on a handmade characteristic in coping with those problems. Even though those techniques can feature properly withinside the selected dataset, they're now no longer appropriate for actual-global applications. With the developing variety of public benchmark datasets, a look at liveness detection has been held, and the accuracy of detection is refreshed continuously [16].

Compared with all of the primarily based totally software program structures, the hardware setup technique makes use of a completely unique sensor for image acquisition, making the distinction between the actual face and the spoofing assaults extra notably, so the detection impact is substantially extra stable [17]. Due to the distinction in reflectivity between an actual face and spoofing assault, multi-spectral infrared [8], and faraway Photo Plethysmography techniques may be hired in liveness detection that has excessive precision. However, the gathering states are relatively strict, together with the hardware setup process, which is surprisingly complicated. Therefore, it's miles tough to be extensively utilized. Besides representing data, density-primarily based totally gadgets also are used for liveness detection, a time-of-flight camera. These strategies can effectively deal with a 2D assault however now no longer 3D [7] ref. offers a machine of liveness detection with a mild area camera, which may also come across many exceptional spoofing assaults. However, the moderate area imaging equipment is pricey, and the invention outcomes are seriously suffering from the mild. In general, hardware-primarily based totally detection methods' weak spot is the fee of the device which is steeply priced

or tough to reap and calls for a further setup process. Therefore, this technique can't be broadly applied.

4. Existing System

The overall performance of face recognition devices improved considerably due to enhancements observed inside hardware and software program strategies withinside the pc imaginative and prescient field. Whereas, researchers proposed and examined numerous techniques to defend face reputation structures in opposition to those intrusions. According to the present strategies, anti-spoofing for face techniques were gathered to most important groups are hardware primarily based totally method and software program-primarily based totally method. First, the hardware primarily based totally method calls for a further tool to hit upon a selected biometric trait including sweat of finger, increase in heart rate, face thermogram, or mirror image. This tool, included in a biometric verification device, calls for a person used to hit upon the sign for a residing thing. Few additional gadgets, including infrared equipment, attain better precision whilst in comparison to less difficult gadgets. However, additional gadgets were high-priced and they are hard to implement. Secondly, the software program-primarily based totally method extracts from the function of the biometric trends via a general sensor for differentiating between actual and pretend trends. The function extraction takes place after the biometric trends, including the feel functions withinside the facial image, are received via way of means of the sensor.

The software program-primarily based totally strategies deal with each of the received 3-D and 2-D trends as 2-D for gathering facts function. By this, the intensity facts are applied for distinguishing between 3-D stay face and flat 2-D faux face images.

5. Proposed System

The best biometric traits to apply in a specific authentication need to have 5 qualities: robustness, distinctiveness, availability, accessibility, and acceptability. Robustness is the shortage of extrade for a person's function for a period. Distinctiveness is a version of records about the populace in order that characters may especially recognize. Availability shows where any customer can use this feature. Accessibility is to benefit from obtaining the function for the usage of a digital sensor. Accessibility refers back to the attractiveness of amassing the function of a person. The functions that offer those five features were used for biometric authentication and Verification machine. Verification is described because of some same character's facts to the saved profile, whereas identity refers to where the joining person's records fit any person withinside the saved dataset. Before authentication (verification or identity), only enrolled people are allowed.

For enrollment, the customers were told to expose their behavioral or physiological traits to the detector. The function record is obtained and exceeded via one in all used algorithms will tests whether or not the obtained records are real or fake. And, it guarantees the fine of the picture. The subsequent task is to sign in only the obtained records with the aid of using appearing localization and alignment. And the obtained records are moved right into a layout that could be a series of identities saved withinside data.

The biometric system performs four steps in the authentication phase and they are:

1. *Data Acquisition*: It's a sensor, like a fingerprint sensor or a web camera, that gathers biometric data in three different quality levels: low, normal, and high.
2. *Preprocessing*: It uses noise filters, smoothing filters, and normalizing procedures to eliminate different data and provide an appropriate set of data.
3. *Feature Extraction*: Before classifying the obtained data, it will extract important information.

4. *Classification*: In this method, uses the obtained characteristics as input and allow them to the output labels

6. Architecture

The architecture of the technique considered is shown in Figure. 1. At first, it will detect whether the person entering into the meeting is real or face. If the person is fake, then it will not allow him/her into the meeting. If the person is real, then it will check whether the person is authenticated person or not. If yes, it will allow him into the meeting. If not, then it will not allow him into the meeting. This process will continue throughout the session. If any person spoofs his face or any other person enters the meeting behalf of him then it will detect and shows that person is fake.

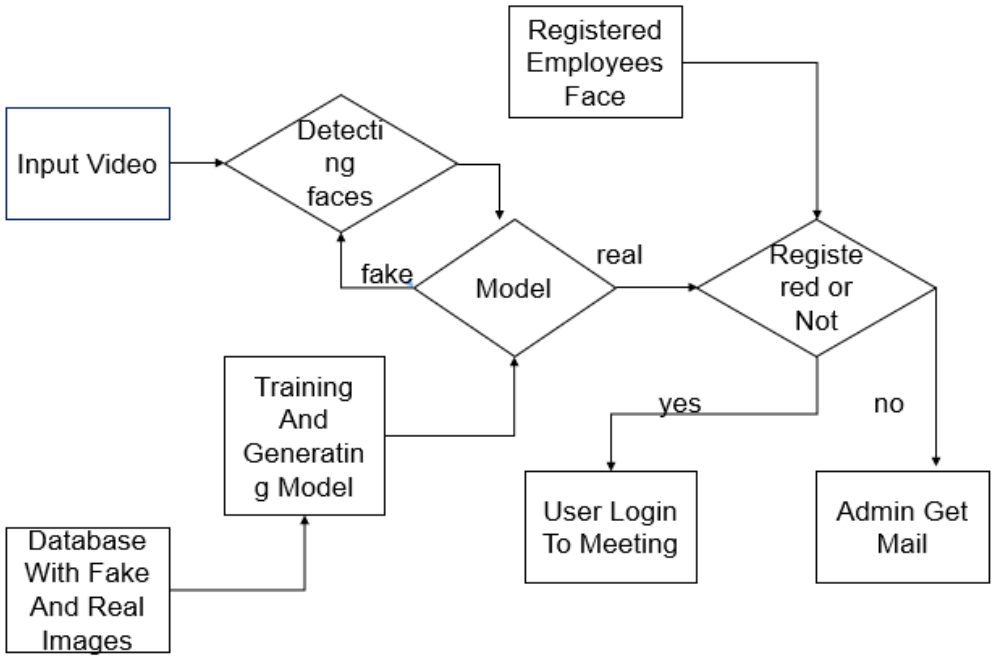


Figure 1. Proposed Architecture

7. Methodology

7.1. Convolution Neural Network

We endorse building an anti-spoofing version with principal modules: the liveness detector and CNN classifier. The scheme for the way our version works is pretty easy. The enter will skip thru the liveness detection module, with a view to come across eye blinks or lip actions. If detected, the entry will stay processed to the CNN classifier module for whether or not the face is faux or actual.

The lifestyles signal detection module at the face is similarly divided into modules: the blink detection module and the lip movement detection module. For the lip movement detection module, we use the lip-motion-internet module. The detector module may be run in actual time on a video document or a webcam's output. This module detects lip motion with the aid of using creating a clear out to decide the higher and decrease lips' places then calculate the lips separation distance.

To decide if the eyes are blinking or not, we use a module that we've got created in our preceding research. We use an eye-fixed vicinity clear out to discover whether or not the eyes are blinking or not. Filters are beneficial for detecting the presence of the attention

vicinity from a person's face picture graph enter. Once the attention vicinity is captured, the following step is to use detection for eye openness. In this step, the attention openness class is applied. This class generates an opportunity of beginning the attention to the entered image, that's then analyzed in step with the value.

7.2. Non-linear Diffusion

The main thing for our method is to cope with spoofing assaults the usage of a nonlinear diffusion primarily based totally on an AOS scheme with a huge time interval to achieve the pointy edges and maintain the boundary places of the input image. Moreover, we use a specialized deep convolution neural network structure that can extract complicated and high-degree capabilities to differentiate the subtle image.

7.3. Additive Operator Splitting

Use non-linear diffusion to detect facial vibrancy to capture sharp edges and preserve border positions. This allows you to use the input image to quickly distinguish between a fake image and a real image. This will remove the edges obtained from the flat image. On the other hand, the actual face remains clear. We used a low-pass filter, the Gaussian smoothing kernel, and used the scale space parameter (t) to smooth out image noise, especially in multiscale representations as given by (1).

$$I(x, y, t) = I_{OriginalImage}(x, y) * G(x, y, t) \quad (1)$$

Koenderink eventually showed that convolving a picture at any scale with a Gaussian function equals the linear diffusion solution, such as the Heat equation as shown in (2).

$$I_t = I_{xx} + I_{yy} \quad (2)$$

A generalized diffusion equation is given in (3).

$$\partial I = div(g \nabla I) \quad (3)$$

The diffusion coefficient g is a constant R connected to the speed of the diffusion process in this case. Linear diffusion has numerous drawbacks, including It involves the blurring of essential features as well as edge changes while flattening fine scales to coarse scales. Perona and Malik pioneered the use of a nonlinear diffusion approach based on partial differential equations (PDEs). This method was dubbed anisotropic diffusion. This method eliminates the following blurring and localization difficulties that impact linear diffusion. The non-linear diffusion filter determines edges and uses an explicit scheme to preserve the position of the edges during the diffusion process which is given in (4).

$$\partial I = \partial_x(g|\nabla I|\partial_x) + \partial_y(g|\nabla I|\partial_y) \quad (4)$$

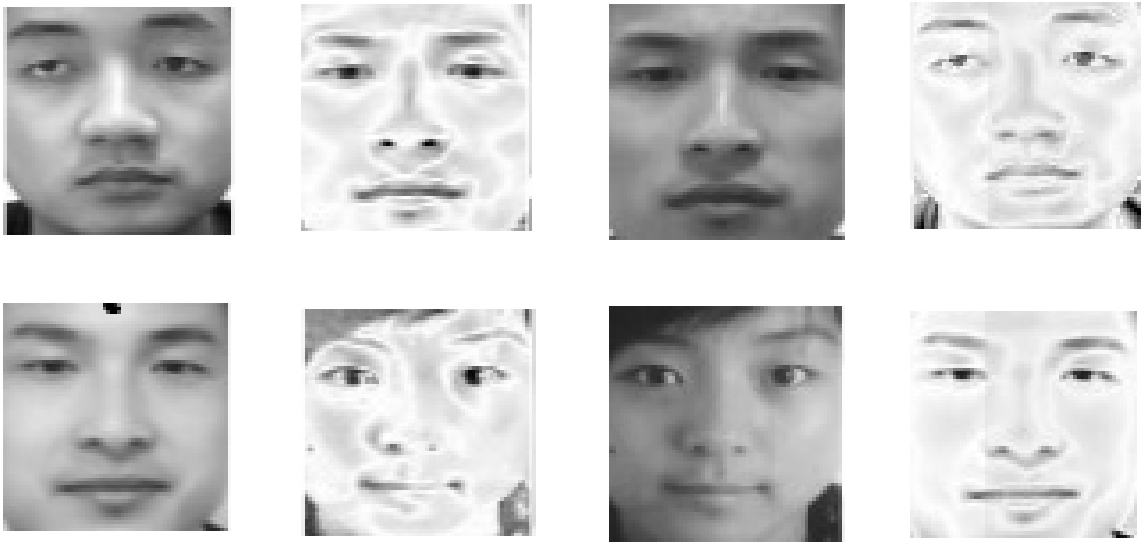
However, this scheme has regularization. Weickert has given a semi-implicit scheme to mark this issue. This scheme works at any timestep size, using the AOS scheme, which treats the coordinates of all axes the same. The AOS scheme gives fast diffusion even at large time step size values (for example, it shows the difference between edges on flat and round surfaces). As shown in Figure 2, smoothing the surface texture of the printed counterfeit image fades the edges, but the actual image retains the edges and prevents the spread from spreading. The non-linear diffusion technique for real and forgery images is depicted in Figure 3.

(a) The above image depicts the True face and the below image a forgery.

(b) A normalized face with a 64 × 64 pixel dimension.

(c) Diffused picture using AOS (above - 100 iterations, below - 5 iterations).

Figure 2. Non-linear diffusion depicting using different images



(a) The above image depicts the True face and the below image forgery.

(b) Both images depict diffused surfaces scaled from 0 – 255.

(c) The above image depicts the True face and the below image forgery.

(d) Both images depict diffused surfaces scaled from 0 – 255.

Figure 3. Non-linear diffusion for real and forgery images

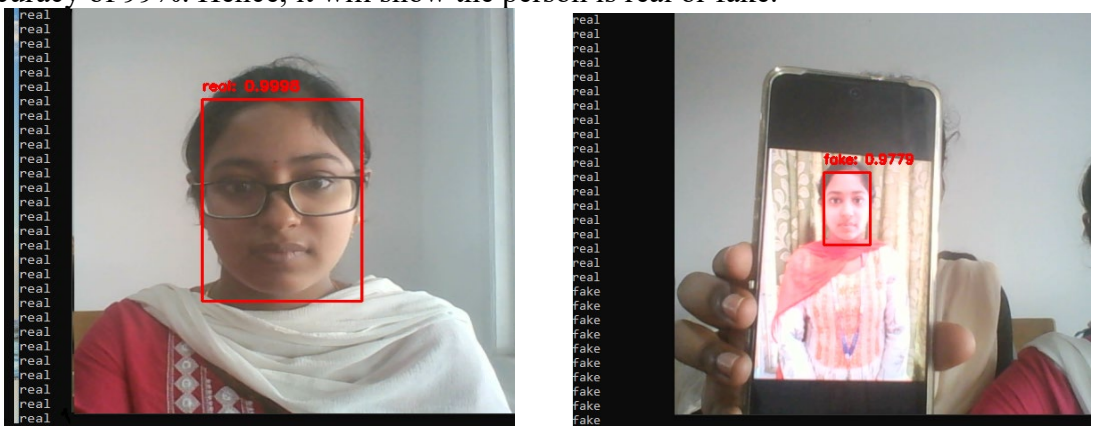
By estimating the diffusion speed, we extract the information characteristics from the picture surface as given in (5).

$$I(x,y) = |\log(I_0(x,y)+1) - \log(I_1(x,y)+1)| \quad (5)$$

Where I_0 is the original picture and Il is the diluted image. As demonstrated the true picture surface in Figure 2 has rather sharp edges (e.g., nose and cheek). The borders of the bogus photos, on the other hand, are smoother. To retrieve the information features, all prior techniques employed hand-crafted features such as the LBP. This method has certain drawbacks, such as the inability to extract complicated characteristics. As a result, deep learning using gradient descent is employed in this study to extract discriminative and greater characteristics from the diffused picture.

8. Results and Discussion

This work proposes a specialized deep convolution neural network that can extract the complex features of the input diffused image to differentiate between a fake and real face. Our CNN has proven to be powerful in extracting not only the edges, but also the textures of the faces. These images are shown in Figure 4. We have achieved the highest reported accuracy of 99%. Hence, it will show the person is real or fake.



(a) The true face which is a Real face. (b) The Fake face which is a forgery.

Figure 4. Diffused images of real and fake faces

9. Conclusion

With such a lot of gadgets the use of facial reputation biometric authentication, the want for face anti-spoof is an absolute must. This paper proposes the use of the CNN evaluation version for photo enter mixed with the face liveness detection module. Based at the effects of module checking out indicates first rate effects to save you diverse kinds of face spoof assaults. We take a look at diverse spoof face assaults examined protected static assaults including masks, image posters or virtual photos, and dynamic assaults including video replays. Further studies can discover parallel programming strategies that could accelerate the time for facial reputation programs.

References

11.1. Journal Article

[1] *J. Wayman, A. Jain, D. Maltoni, and D. Maio, An Introduction to Biometric Authentication Systems, Biometric Systems: Technology, Design and Performance Evaluation, 2005, 1-20.*

[2] *J. Maatta, A. Hadid, and M. Pietikainen, Face spoofing detection from single images using micro-texture analysis, 2011 International Joint Conference on Biometrics (IJCB), 2011.*

[3] *Z. Guoying, and M. Pietikainen, Dynamic Texture Recognition Using Local Binary Patterns with an Application to Facial Expressions, IEEE Transactions on Pattern Analysis and Machine Intelligence, 29 (2007), 915-928.*

[4] *I. A. Gomaa, G. I. Salama, and I. F. Imam, Biometric OAuth service based on finger-knuckles, 2012 Seventh International Conference on Computer Engineering & Systems (ICCES), 2012, 170-175.*

[5] *L. Weiwen, Face liveness detection using analysis of Fourier spectra based on hair, 2014 International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR), 2014, 75-80.*

[6] *N. Kose and J. L. Dugelay, Countermeasure for the protection of face recognition systems against mask attacks, 2013 10th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG), 2013, 1-6.*

[7] *N. Erdogmus and S. Marcel, Spoofing Face Recognition With 3D Masks, IEEE Transactions on Information Forensics and Security, 9 (2014), 1084-1097.*

[8] *D. A. Socolinsky and A. Selinger, A comparative analysis of face recognition performance with visible and thermal infrared imagery, 16th International Conference on Pattern Recognition, textbf4 (2002), 217-222.*

[9] *M. Pietik¨ainen and A. Hadid, Texture features in facial image analysis, Advances in Biometric Person Authentication,Springer, 2005, 1-8.*

[10] *T. Choudhury, B. Clarkson, T. Jebara, and A. Pentland, Multimodal person recognition using unconstrained audio and video, International Conference on Audio-and Video-Based Person Authentication Proceedings, 1999, 176-181.*

[11] *A. Anjos, M. M. Chakka, and S. Marcel, Motion-based counter-measures to photo attacks in face recognition, Biometrics, IET, 3 (2014), 147-158.*

[12] *P. Gang, S. Lin, W. Zhaohui, and L. Shihong, Eyeblink-based Anti-Spoofing in Face Recognition from a Generic Webcamera, IEEE 11th International Conference on Computer Vision, 2007, 1-8.*

[13] *I. Chingovska, A. Anjos, and S. Marcel, On the effectiveness of local binary patterns in face anti-spoofing, 2012 BIOSIG - Proceedings of the International Conference of the biometrics Special Interest Group (BIOSIG), 2012, 1-7.*

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

[15] *J. Weickert, B. M. T. H. Romeny, and M. A. Viergever, Efficient and reliable schemes for nonlinear diffusion filtering, IEEE Transactions on Image Processing, 7 (1998), 398-410.*

[16] *Y. Jianwei, L. Zhen, L. Shengcai, and S. Z. Li, Face liveness detection with component dependent descriptor, 2013 International Conference on Biometrics (ICB), 2013, 1-6.*

[17] *K. Wonjun, S. Sungjoo, and H. Jae-Joon, Face Liveness Detection From a Single Image via Diffusion Speed Model, IEEE Transactions on Image Processing, 24 (2015), 2456-2465.*

[18] *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, Springer, 2010, 504-517.*

[19] *B. Peixoto, C. Michelassi, and A. Rocha, Face liveness detection under bad illumination conditions, 2011 18th IEEE International Conference on Image Processing (ICIP), 2011, 3557-3560.*

[20] *Lin and Su (2019) developed a face anti-spoofing and liveness detection system using CNN [23]. The image is resized to 256 * 256, and RGB and HSV color spaces are used.*