International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Face Liveness to Identify Between Actual Face and Spoof Face

Lovely Pal[1], Renuka Singh[2]

Department of Computer Science and Engineering, ABSS Institute of Technology, Meerut UP, India
lovelypal182[at]gmail.com

Department of Computer Science and Engineering, ABSS Institute of Technology, Meerut UP, India

Abstract: ***Biometric systems are commonly used mostly for face detection and recognition security purposes such as fingerprint or retinal detection and signature verification. Face detection is a process that analyses human faces in digital images and is used in a wide range of applications like facial motion tracking, eye movements, and facial identification. Facial recognition software technology has improved dramatically in recent years in current and developed security solutions. Face recognition, like some of the other biometric systems, can easily fooled. A person's picture and video (character, personality) are freely accessible via the internet or even a social media website***.

Keywords: Face Detection, Retinal Detection, Signature Verification

1. Introduction

Typically, spoof methods are classed based on proof given verification systems, like a stolen video or image from the internet or social media. To protect against spoofing, a secured system requires a liveness detection monitor. The facial liveness detection approach is the greatest strategy for safeguarding the system and avoiding spoof assaults on our network. There are several methods for facial identification accessible; nevertheless, face recognition systems are dangerous, inadequately guarded, and easily tricked. Many advanced ways exist in modern tech to trick such systems utilizing spoofing. Face liveness monitoring is suggested to prevent spoofing from insecure face recognition.

The requirement for massive identity management, their usefulness rely on the precise derivation of a person's identification on the basis of multiple applications, has increased the relevance of biometrics in contemporary society. Distributing networked system resources, allowing access to the nuclear installations, executing remote monetary operations, and boarding a commercial flight are some illustrations of these uses. A security system's primary purpose is to verify an individual's identification. The key purpose for this is to keep imposters from gaining access to secured resources. Passcodes or ID card methods are common security approaches, however these identity procedures can easily forgotten, impeded, or stolen, undermining the desired security. A biometric authentication can provide better protection for such a security system utilizing the biological and physical attributes of humans.

In recent times, liveness detection has emerged as a prominent study area in the fingerprint identification and eye detection sectors. However, options to dealing with this difficulty in facial recognition software are severely limited. This act of distinguishing between live and non - living image features is referred to as liveness. Constant attempts will be made by impostors to load the system with fake biometrics. Using detection and tracking tools may greatly improve a biometric system's efficiency. Spoofing resistance in biometric security systems is a crucial and complex issue. There are several possible categories for face recognition - based attacks. The categorization is based on the confirmation proof presented to the face authentication scheme, like a stolen picture, stolen face pictures, video recording, 3D face modeling capable of blinking and extending their lips, 3D face models capable of displaying varied moods, and so forth. Before facial recognition systems may be widely used in our daily lives, the anti - spoofing problem must be thoroughly resolved.

2. Literature Review

Face Liveness Detection employs a variety of methodologies. Some of the more intriguing liveness detecting algorithms are explained in this section.

Gang Pan et al. (2004) developed a nonintrusive consistent liveness finding approach to validate picture parodying in face recognition by observing eyeblinking. Eye straining is an exceedingly perplexing structure to grasp. The goal of such a face liveness localization approach is to counter the caricaturing attack in a non - intrusive way using only a generic camera. The physiologic function of eye blinking is to instantly shut and open the eye lids, which helps to disseminate tears throughout the face and eliminate irritants. Humans normally blink 15 - 30 times per minute, which means they blink about once two to three seconds and have a blink period of almost 205 millisecond. As a result, a basic camera may readily capture facial footage at more over 15 frames a second, with a latency between frames of no over than 70 milliseconds. The cameras can then take two or more shots while the subject is staring into the camera. It provides a hint to employ eye blinking for face spoofing.

Jukka et al. (2006) suggested a strategy for detecting face spoof attacks using microscopic texture analysis. The idea is to emphasise the contrasts in micro texture in the higher dimensional space. The authors accepts local binary patterns to describe micro texture and geographical information (LBP). This tool's vector is then transmitted into an SVM or

support vector machine classifier, which determines if the micro texture patterns are fake or real.

Kollreider et al. (2001) describe a movement - based counter - measures that uses an optical stream area to verify the connectivity between different parts of the face. The data is deemed fake in this manner if the optical streaming field upon that focus point of face and also the main focus of the ears have a comparable direction. The research was evaluated using the XM2VTS database component 'Head Rotation Shot, ' wherein real access was the records of this set, and thus the assaults were made using printouts of that information. Using this unavailable database, an equivalent error rate of 0.5percent was calculated.

The authors have proposed that analysing the 2D Fourier spectrum of the source images is an efficient strategy for live facial recognition. As the equivalent frequency descriptors, they estimated the ratio of power of high - frequency elements to that of all frequency content. The researchers assume that a higher - frequency descriptors of the living face ought to be greater than a suitable threshold T_{fd}. Most high frequency elements of a picture are those with frequencies larger than two - thirds of the image's greatest radius frequency as well as magnitudes higher than just a threshold T_f. The studies found that when an extremely clear and large photo is utilized to mislead the program, the aforementioned strategy would be beaten. To address this issue, motion pictures were used for live face recognition. Observing temporal variations in facial structure over time, wherein facial appearance was represented by such an energy value specified in frequency response, is therefore an excellent method for live face identification. To overcome this challenge, the researchers have devised a three - step approach. The first stage is to create a subset by selecting a picture from just an input image sequence every 4 photos. With in second phase, a sustainable value t is generated for each picture in such selection. For the depiction of temporal variation with in face, the frequency dynamics descriptor or FDD, which corresponds to the standard error of the resultant flag value, is computed. In comparison to prior studies that seek 3 - D depth data of head, the suggested technique has several advantages, including ease of computation.

Table 1: Live face detection Experimental results

Image Sequence		Frequency Dynamics Descriptor			High Frequency Descriptor		
		Mean	Min.	Max.	Mean	Min.	Max.
Live Face	200 images	960	718	1490	0.7197	0.4011	2.0544
Fake Face	40 images (48 x 33 mm)	286	233	376	0	0	0
	50 images (76 x 55 mm)	260	186	364	0.0913	0	0.1376
	90 images 124 x 84 mm)	175	91	282	0.3535	0	0.5514
	20 images (600dpi)	249	237	260	0.2803	0	0.3917

Variable Focused base analysis

Sooyeon Kim et al. (2009) developed the approach of facial liveness detection utilising variable focusing. The fundamental strategy is to employ pixel value fluctuation by focusing among two photos acquired in various focuses consecutively, which is among the camera functionalities. Considering that there isn't any significant change in movement, the researchers attempted to figure out the differences in focus levels between actual and fake faces whenever two consecutive photos (in/out focus) of each participant were gathered. Because of the abundance of data, certain features of real faces may be seen whereas others are hidden. Photos taken from various focal lengths of such a printed face show very little variation from one another since the differences are so small. This method relies on the difference in Depth of Field (DoF), which measures how much individual pixels shift in and out of focus between successively captured images. Depth of field (DoF) refers to the range between whatever is in sharp focus to whatever is out of focus. It was determined that a smaller depth of field (DoF) would improve the efficiency of liveness detection, thus the researchers worked to increase the out focusing effects. Sum Modified Laplacian is utilized to assess focus intensity in this approach. The SML displays degrees of concentrating in pictures as a converted 2nd - order divergent filter.

Movement of eye analysis

Hyung - KeunJee et al. (2001) described an eye tracking - based embedded face detection systematic approach. The experts proposed recognizing eyeballs in subsequent input photographs, trying to calculate the variance of every eye area, and deciding whether the specified face is fake or real. The central premise seems to be that large structure fluctuations in human vision must occur as a result of blinking and unexpected pupil movements. Within input facial picture, the first center point both of eyeballs is recognized. Face areas are normalized and eye areas are retrieved using the identified both eyes. After binarizing retrieved eye regions, variance is determined for each binarized eye area. If the outcome is above the threshold, then input picture is identified as a live face; otherwise, it is differentiated as a picture. The researchers utilized the fact that perhaps the intensity of the eye area is below that of the rest of the facial image if the picture is treated as a 3D curve to identify the eye areas. On determine the eye area, first apply Gaussian fiInput image is recognized as a real person if the result is greater than the threshold; else, it is classified as an image. To do this, they took use of the fact that, if the image is seen as a 3D curve, the luminosity of the eye region may be lower compared to the remaining of the face image. ltration to the facial picture to produce a smoothed 3D curve. By using gradient descent approach, we extract each of the local minimum standards in the curve. The eye predictor, which is developed using Viloa'sAdaBoost training techniques, is used to minimize the number of invalid eye options. Following that, the original image is normalized by a size as well as rotation using the central point of eyes because of input face might have different sizes and rotation. Self Quotient Image (SQI) is used to reduce the influence of

light. Following the normalization of the face region, eye areas are extracted depending on the center of the eyes. Then, to use a threshold, ocular areas are binarized to also have pixel values of 0 and 1. The threshold is calculated using the average pixel value of every eye area. The shape of eye regions acquired from genuine faces varies more than regions produced from synthetic ones. The Hamming distance method is employed to determine the liveness score from each eye area. The Hamming distance seems to be the pixel count that do not share the same value when two sorted lists of images are compared. Whereas if average liveness value is higher than threshold, then input picture is identified as a live face; otherwise, it is identified as an image.

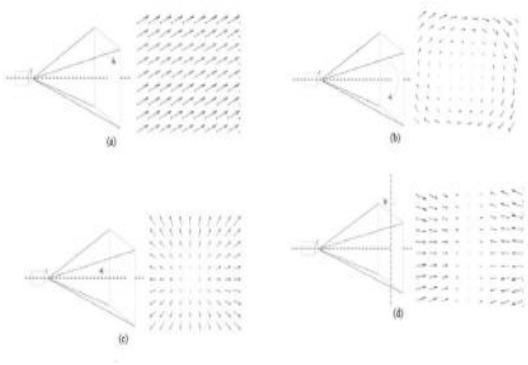
Table 2: Obtained hamming distance
Hamming Distance of Eye Regions

	Hamming Distance		
	Mean	Min	Max
Live Face	30	18	47
Fake Face	17	10	22

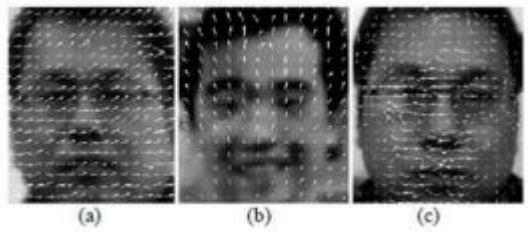
Analysis based Optical Flow

Bao et al. (2012) first proposed the optical flow field approach. It evaluates the differences and similarities between the optical flow generated by three - dimensional things and that produced by two - dimensional surfaces. The optical flow field has four possible motions: translation, rotation, forward motion, and lateral swing. Study discovered that now the optical flow fields produced by the first 3 groups seem to be roughly equivalent in both 2D and 3D pictures. Differences in the optical flow field are controlled by the fourth kind. They use a method predicated on the idea that optical flow field of a 2D object may be understood in terms of an anticipated transformation. It is possible to determine whether or not the testing zone is flat by computing the area of application, which is made possible by the optical flow.

To do this, we need to find out how much of a difference there is between the optical flow fields. This variation serves as a cutoff point for authenticating facial features. There were three types of data samples used in the study. The very first group included 100 printable face pictures that have been interpreted and randomly repositioned before the experiment, the second group included 100 images from group 1 that have been folded as well as curled just before experiment, and thus the third group included real faces of people undertaking gestures like trying to swing, rattling, and so on. The trial lasted 10 seconds, according to the experts. The camera sampled at the rate of 30 frames each second.



Types of the optical flow fields



Examples of group a, b, c

Table 1: Experimental Results

Group	T			
	0.2	0.4	0.6	0.8
1st	0.54	0.83	0.86	0.92
2nd	0.45	0.80	0.85	0.89
3rd	1.00	1.00	0.94	0.86

3. Results

As demonstrated in Fig., the percentage of successful detection increases as the threshold increases. However, the experts did not indicate any incorrect acceptance rates, so the proportion may reduce at some time. Another issue is that because the approach is predicated on exact estimation of the optical flow field, changes in lighting will have a detrimental impact on the outcomes. This approach will fail if such fake face isn't really planar, i.e. 3D objects. As a result, the report recommends combining this technique with some other liveness detection systems.

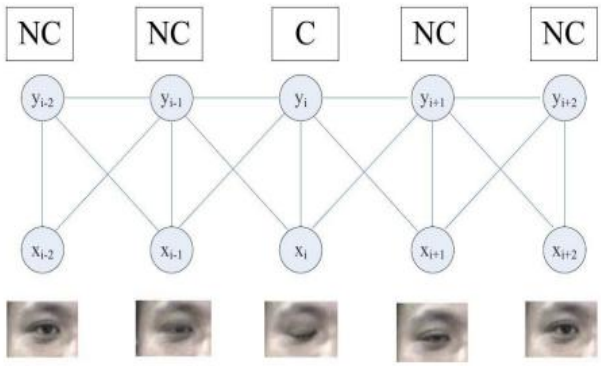
Kollreider et al. (2001) proposed a combination of face components detection and optic flow field estimates for face liveness detection. This method can distinguish between mobility of points and movement of lines. The researchers provide a method for analyzing the trajectories of individual portions of a live face. The data obtained can be utilized to determine the extent to which a printed picture was used.

For detecting face components, this method employs a model - based Gabor deconstruction and SVM. The essential notion behind this approach is that a 3D face creates a 2D motion which is greater in centre facial regions than in outside face parts like ears. As a result, pieces farther away change direction than portions closer to the camera. A picture, on the other hand, causes continual motion on various facial areas. It is possible to evaluate how quickly the face pieces are in relationship to each other using the

knowledge about their locations and velocity. This data is necessary to distinguish a live face from such an image.

Blinking based analysis

Lin Sun et al. (2010) pioneered the blinking - based technique for liveness identification utilizing Conditional Random Fields or the CRFs. The paper employs CRFs to represent blinking behaviors in order to account for long - term dependence on the input pattern. The CRF model was then compared to a discriminative model including AdaBoost as well as a generative model such as HMM. CRFs are deterministic models for efforts have been exerted and labeling sequence data that are primarily utilized in natural language analysis due to their ability to accommodate long - range dependence on the output sequence. Blinking activities usually represented by a picture sequence that includes images with close as well as non - close states.



Graphic structure of CRF - based blinking model

Binary Classification based analysis

Tan et al. (2005) proposed the anti - spoofing issue approach as nothing more than a binary problem of classification. The researchers' main point is that a real human face varies from a photograph of a human face. A real face is 3D, whereas a photograph is only 2D. The surface quality of a photograph differs from the appearance of a genuine face. The studies discovered a real - time and non - intrusive way to solve a problem using individual pictures from a basic web camera. Even though the deductions of positive and negative numbers in input space are substantially overlapping, the job is composed as a binary categorization problem, so an adequate representation space is critical. They offered two ways for extracting the critical details about distinct surface qualities of a real life human face or an image in regards of latent samples that use the Lambertian model. Using these findings, two novel additions to the sparsely logistic model were used to detect spoofs quickly and accurately. To increase generalization capability under high - dimensional and short sample size circumstances, the basic sparse logistic regression classifiers was expanded both nonlinearly as well as spatially. The findings revealed that nonlinear sparse prediction model enhances anti - photo spoofing performance significantly, but spatial extension results in a dense relatively low level bilinear regression model. The authors gathered a public information huge photograph - imposter database including over 50K picture images from 15 people to assess their strategy. Preliminary tests on this database reveal that the authors' suggested technique provides good detection accuracy, with the benefits of real - time screening, non - intrusion, and the lack of additional hardware. They also provided highly successful findings in their work, although the authors disregarded the issue of poor lighting circumstances. Peixoto et al. (2008) expanded their approach to cope with photos even in low - light settings, whether via a laptop screen or elevated printed photographs. The fundamental idea is that even the brightness of an image collected from an LCD panel influences the image in a manner that high - frequency regions becoming prone to "blurring" because of pixels with increasing values illuminating their surroundings. As a result, the phoney photos have less boundaries than the original facial image. By examining such data, the authors were able to determine if a picture was a fake or not. They began by analyzing the picture with the Difference of Gaussian (DoG) filter, which employs two Gaussian filters with distinct degrees of separation as boundaries. The authors' fundamental aim was to preserve the high - middle - frequencies to recognize the boundaries and reduce the noise. However, under poor lighting circumstances, DoG filtering fails to identify the boundaries. The authors utilised a Sparse Logistic Regression Model identical to the model used only by Tan et al. (2004), for the classification phase. To reduce the impact of poor lighting, the picture was pre - processed to homogenize it and make the lighting changes more regulated. The contrast - limited adaptive histogram equalization was utilized by the researchers.

Scenic Clues based analysis

Yan et al. (2014) pioneered the approach of detecting facial liveness by examining several scenic indicators. For dependable and effective face liveness recognition, the study presents a system that integrates three scenic clues: non - rigid movement, face backdrop consistency, and image band effect. A relatively low level matrix deconstruction based picture alignment technique is used to extract the non - rigid motion cue, which signals face movements such as blinking. The face - background continuity clue posits that the movement of the face and backdrop is high for false face pictures and low for legitimate faces, and that this continuity can serve as an effective liveness indication. The project designed a motion detection approach based on GMM for face - background uniformity. The image bands effect represents imaging quality problems induced in the false face replication, which the researchers detected using wavelet transform.

Context based analysis

Komulainen et al. (2009) developed this innovative context - based face anti - spoofing approach. The research follows the attack - specific spoofing approach to detect and engaged in face spoofing situations where scene information may be utilized. They are attempting to identify spoofing by showing a phoney face in front of cameras in the offered perspective. The fundamental idea was that when detecting spoofing, humans rely heavily on scene as well as contextual cues; the proposed algorithm aims to mimic people's behaviour and uses scenic cues to assess whether or not a phoney face is positioned in front of the cameras. The cascades of upper - body (UB) and spoofed medium (SM) sensors of oriented gradients (HOG) descriptors, along with

linear support vector machines is used in the proposed technique (SVM).

The researchers claim that researchers, the method may be used to either a single picture sequence or a video clip. The researchers suggested a technique for identifying close - up fake faces by cascading two HOG descriptor - based detectors. The projection medium's existence was determined by assessing the alignment of the face as well as the upper region of the torso with just an upper - body detector and a specific detector trained on actual face spoofing instances. The upper - body detector, which would be part of the human posture assessment pipeline, is used to determine proper head and shoulder alignment. For testing, they employed the CASIA Face Anti - Spoofing Dataset, which contains many false face assaults of varied natures and are under varying settings and image capabilities. The suggested technique outperforms the CASIA Face Anti - Spoofing Database, with an error rate ranging from 3.3% to 6.8%.

Combination of Standard Techniques based analysis

Kollreider et al. (2012) proposed an approach that integrates established techniques in 2D facial biometrics. They investigated the issue using real - time methodologies and adapted them towards real - life spoofing situations in such an indoor setting. First, the algorithm begins for faces, and if one is found, a timer is initiated to specify the duration for gathering evidence. The evidence is therefore gathered in order to determine the liveness of the features. During non - interactive modes, 3D attributes or eye - blinking or the mouth movement are examined for liveness identification. If no corresponding response is discovered, responses are randomly solicited and verified. The following are the variations between asynchronous as well as synchronous: Because async is multi - threaded, actions or programmes can operate in parallel. Although Sync is single - threaded, only one action or programme may operate at the same time. Because Async is non - blocking, it may send numerous requests to such a server.

4. Discussion

Liveness detection methodologies are classified below in accordance with the type of liveness indication employed to aid in the identification of liveness in faces. Movement, texture, and live sign indications were the most often employed. The primary function of motion analysis is to differentiate between the motion patterns of 3D and 2D faces. It takes use of the fact that flat objects move in quite different ways from three - dimensional human faces. To analyse motion, optical flow is often approximated from videos. System dynamics does not need human input, is not reliant on texture, and is very difficult to fake using a 2D image of the face. Video is necessary for motion analysis, however it's challenging to use dynamic simulation on footage with weak motion. High - quality photographs are necessary, and the technique is vulnerable to being spoofed by 3D sculptures.

Texture analysis approaches identify assaults primarily by exploiting identifiable texture patterns like print errors and overall picture blur. This method assumes that phoney faces are created on paper, and that the print process as well as paper structure which provide texture characteristics may distinguish those printed pictures from actual face images. In this case, the person's face is printed out on paper and displayed to the cameras for confirmation or authentication. Because the printing process and paper typically have strong textural properties, using textured analysis to detect actual faces is advantageous in such scenarios. Texture analysis - based approaches are simple to develop and do not require user cooperation. Nevertheless, printing and paper textures may vary widely; thus, systems based on texture evaluation must be resistant to varied texture patterns, which need a big dataset. It is also possible that the attack is carried out by projecting a photograph onto a screen, leading to a lack of texture details. Motion analysis will be effective in reducing the dependence on particular texture data.

Although, motion estimation may confront issues if there is minimal motion information. This might arise when the user's behavior varies, resulting in high - noise photos with low resolution. Motion analysis may also fail when spoof assaults are carried out using more complex approaches, such as 3D sculpting face model.

There are two forms of life sign identification. First, some known user interactions are assumed. In this instance, the viewer must perform a specific action to verify the face image's authenticity. This allocation might be a particular action that acts as a response to a challenge or as a moving passcode. Users who successfully perform their jobs are deemed to be authentic. The third category doesn't really assume user interaction and instead relies on certain facial movements, like blinking, as a sign of vitality and, thus, a genuine face. Using 2D face photographs and 3D models, it is very impossible to trick the life sign - based liveness detection system. This method is likewise texture - independent; however it may require user participation. This method is mostly based on detecting facial parts.

5. Conclusions

This paper provides an overview of various ways to detecting facial liveness. It gave a classification based on the approaches utilised and the types of liveness indicator used for facial liveness detection, which aids in comprehending distinct spoof attack patterns and their relationship to the established solutions. A survey of the most intriguing methodologies for detecting liveness was provided. The most typical difficulties reported in various liveness detection systems are the impacts of light change and the consequences of amplified noises on pictures, which destroy the texture features. For continued development of the liveness detection systems dependent on blinking and movements of the eyes, eyes lenses that create reflection arealso studied. Moreover, the datasets, which are essential for the effectiveness of liveness detection methods, must be relevant and diversified in order to replicate the predicted application situations. Non - interactive videos sequences must incorporate interactive segments in which users complete specific tasks. Upcoming attack dataset must take into account threats such as 3D sculpting faces and enhanced textures. Our primary goal is to provide a clear route for

continued development of more safe, user - friendly, as well as efficient ways for detecting facial liveness.

References

[1] Chakraborty, S., & Das, D. (2014). An overview of face liveness detection. *arXiv preprint arXiv: 1405.2227*.

[2] Bao, W., Li, H., Li, N., & Jiang, W. (2009, April). A liveness detection method for face recognition based on optical flow field. In *2009 International Conference on Image Analysis and Signal Processing* (pp.233 - 236). IEEE.

[3] Chan, P. P., Liu, W., Chen, D., Yeung, D. S., Zhang, F., Wang, X., & Hsu, C. C. (2017). Face liveness detection using a flash against 2D spoofing attack. *IEEE Transactions on Information Forensics and Security*, *13* (2), 521 - 534.

[4] Hadiprakoso, R. B., &Setiawan, H. (2020, November). Face Anti - Spoofing Using CNN Classifier & Face liveness Detection. In *2020 3rd International Conference on Information and Communications Technology (ICOIACT)* (pp.143 - 147). IEEE.

[5] Parveen, S., Ahmad, S. M. S., Hanafi, M., & Adnan, W. A. W. (2015). Face anti - spoofing methods. *Current science*, 1491 - 1500.

[6] Lagorio, A., Tistarelli, M., Cadoni, M., Fookes, C., &Sridharan, S. (2013, April). Liveness detection based on 3D face shape analysis. In *2013 International Workshop on Biometrics and Forensics (IWBF)* (pp.1 - 4). IEEE.