International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST21843

Face Liveness Detection : An Overview

Shweta Policepatil, Sanjeevakumar M. Hatture
Department of Computer Science and Engineering Basaveshwar Engineering College (Autonomous), Bagalkot, Karnataka, India

Article Info
Volume 8, Issue 4
Page Number : 22-29

Publication Issue
July-August-2021

Article History
Accepted : 25 June 2021
Published : 02 July 2021

ABSTRACT

As the world becomes more and more digitized, the threat to security grows at an alarming rate. The mass usage of technology has garnered the attention and curiosity of people with foul intentions, whose aim is to exploit this use of technology to commit theft and other heinous crimes. One such technology used for security purposes is "Facial Recognition". Face recognition is a popular biometric technique. Face recognition technology has advanced fast in recent years, and when compared to other ways, it is more direct, user-friendly, and convenient. Face recognition systems, on the other hand, are vulnerable to spoof assaults by non-real faces. To protect against spoofing, a secure system requires liveness detection. This study examines researchers' attempts to address the problem of spoofing and liveness detection, including mapping the research overview from the literature survey into a suitable taxonomy, exploring the fundamental properties of the field, motivation for using liveness detection methods in face recognition, and problems that may limit the benefits.

Keywords : Face Liveness Detection System, Machine Learning, Deep Learning, Face Detection, Face Spoofing.

I. INTRODUCTION

People are increasingly relying upon technology for the completion of their daily tasks. As the usage of smart devices increases, there is a need for securing these devices against people with malicious intentions. The threat to security is high and the consequences are dire if unauthorized access is gained to such systems. Personal data, organizational sensitive information, high risk information is secured in such systems. Hence, properly securing these systems is essential. Face verification has become the most widely used approach for this purpose, however it is prone to a variety of spoofing attacks. Face liveness identification, that is referred to as face spoofing identification, has been devised to defend against spoofing attack.

The emergence of machine learning, deep learning, and computer vision tools have made face liveness detection efficient and feasible for general purpose use. Here we have mentioned few approaches which

have helped us in solving this security problem. Biometrics is a multidisciplinary field that involves measuring and mapping certain biological qualities, such as fingerprints, face, palm veins, and other features, in order to create an individualised recognition code [1]. Physical qualities, such as those listed above, and behavioural traits, such as signatures, voice, and keystrokes, are two types of biometric attributes. A wide range of technologies rely on biometrics. However, one of the most significant challenges facing biometric recognition systems is fake identity, sometimes known as a spoofing assault. In general, there are two sorts of attacks: indirect and direct strikes. Indirect assaults are carried out within the system by hackers or intruders, for example, by tampering with the feature extractor (i.e. matcher) or making changes to the template database. Anti-virus software, firewalls, encryption, and intrusion detection are just a few of the techniques that can help against indirect attacks. Direct attacks, on the other hand, are carried out at the sensor level beyond the system's digital limitations, hence no digital protective mechanisms can be utilised to prevent them. The process of checking whether the biometric being collected by the recognition system is real (i.e. alive) or has been mimicked by intruders to gain illegal access to the biometric system is known as liveness detection. The relative relevance of facial liveness detection has been a topic of debate in the research on liveness detection. We present an overview of the most up-to-date anti-spoofing detection approaches for facial biometrics in this post. Face anti-spoofing systems necessitate the presence of a genuine photograph, recorded video, or dummy evidence at the sensor, among other things (i.e. camera).

A survey of the most interesting face liveness detection methods is offered in the next section. Following that, a discussion of the benefits and drawbacks of several face liveness detection algorithms is offered. After then, a conclusion is reached.

II. Literature Review

Following figure 1 shows the various techniques used in face liveness identification.

X. Zhu, S. Li, X. Zhang, H. Li and A. C. Kot at el in [1] creates a general classifier that can recognise facial photos by faking medium contours (termed as SMCs for simplicity). To this aim, the problem of face anti-spoofing is defined as the detection of SMCs in an image. For detection, they propose and train a Contour Enhanced Mask R-CNN (CEM-RCNN) model. Their approach incorporates the contour object-ness, which assesses how probable an object is to contain SMCs, to detect their presence. The experimental results show that the CEM-RCNN is very general for detecting face images with SMCs, and that it outperforms the state-of-the-art in a cross-database scenario.

R. Cai, H. Li, S. Wang, C. Chen and A. C. Kot in [2] proposed a novel framework based on the Convolutional Neural Network (CNN) and the Recurrent Neural Network (RNN) for the face anti-spoofing problem, which is inspired by the philosophy used by humans to determine whether a presented face example is genuine or not, namely, to look at the example globally first and then carefully observe the local regions to gain more discriminative information (RNN). Authors uses deep reinforcement learning to describe the behaviour of discovering face-spoofing-related information from picture sub-patches in particular. They also describe a recurrent technique that uses an RNN to learn representations of local information progressively from the examined sub-patches. Finally, authors combine the local information with the global information, which learned from the original input image using a CNN. Furthermore, they conduct comprehensive experiments on multiple public databases, including

ablation study and visualisation analysis, to evaluate the proposed architecture.

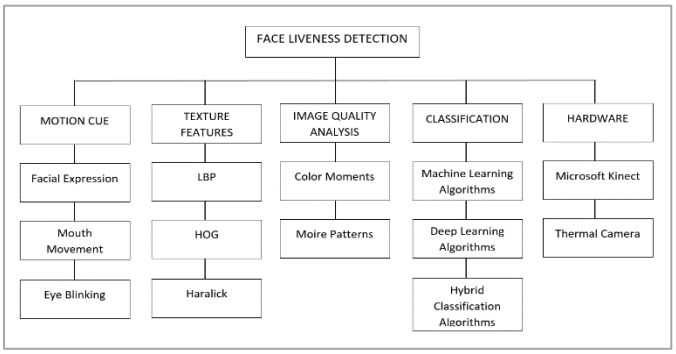

Figure 1. Face Liveness Detection Techniques

W. Sun, Y. Song, C. Chen, J. Huang and A. C. Kot at el in [3] proposes Fully Convolutional Network (FCN) for face spoofing attack detection on pictures, movies, and 3D masks. Face spoofing detection, also known as face anti-spoofing, face liveness detection, or face presentation attack detection, is a difficult issue in practise for protecting face verification systems. An advanced face spoofing detection system based on a depth-based FCN is revisited in their research. Different supervision techniques are thoroughly studied, including global and local label supervision. For local tasks with insufficient training samples, such as the face spoofing detection task, a generic theoretical analysis and related simulation are offered to demonstrate that local label supervision is more suitable than global label supervision. The Spatial Aggregation of Pixel-level Local Classifiers (SAPLC), which is made of an FCN portion and an aggregation part, is proposed as a result of the investigation. The pixel-level ternary labels, which contain the real foreground, faked foreground, and undecided background, are predicted by the FCN component. The labels are then combined to produce an accurate image-level judgement. Experiments on the CASIA-FASD, Replay-Attack, OULU-NPU, and SiW datasets are also carried out to statistically test the proposed SAPLC. The proposed SAPLC outperforms representative deep networks, such as two globally supervised CNNs, one depth-based FCN, two FCNs with binary labels, and two FCNs with ternary labels, and achieves competitive performance close to some state-of-the-art method performances under various common protocols, according to the experiments. Overall, their findings experimentally validate the suggested pixel-level local label supervision scheme's benefit.

W. Sun, Y. Song, H. Zhao and Z. Jin in paper [4] proposes the Fully Convolutional Network with Domain Adaptation and Lossless Size Adaptation (FCN-DA-LSA) as a face spoofing detection method. The FCN-DA-LSA contains a lossless size adaptation preprocessor followed by an FCN-based pixel-level classifier with a domain adaptation layer, as the name implies. The FCN local classifier fully exploits the pervasive and repeated qualities of face spoof distortion. The domain adaptation (DA) layer promotes cross-domain generalisation. The face restoration procedure causes a lot of spoof clues, thus the lossless size adaptation (LSA) saves these. Both the DA and the LSA are required for high-accuracy face spoofing detection, according to the ablation study. Among the state-of-the-art approaches, the FCN-LSA achieves competitive results. The FCN-DA-LSA enhances performance and surpasses previous approaches by using small-sample external data in the target domain (2/50, 2/50, and 1/20 subjects for CASIA-FASD, Replay-Attack, and OULU-NPU, respectively).

Patil Rashmi, Bellary Sreepathi in paper [5] proposes melanoma skin cancer using image processing and deep learning classification. Authors used Similarity Measure for Text Processing (SMTP) as loss function to improve the performance of convolutional neural network (CNN) Classification. Two approaches for classifying melanoma cancer stages are presented in this research. Their results with various loss functions were displayed and compared to the proposed SMTP loss function. The suggested technique outperforms a number of different loss functions created expressly for classification problems.

H. Chen et al in paper [6] proposes Face anti-spoofing region-based convolutional neural network

(FARCNN). Face-based biometric systems are commonly utilised in person authentication applications since the human face is the most accessible from our daily lives and contains the most information. Authors build a method to prevent face spoofing that combines the face detection stage and the face spoofing detection stage. FARCNN is designed in this paper using the upgraded Faster region-based convolutional neural network (R-CNN) framework. Face spoofing detection is a three-way classification that distinguishes actual face, fake face, and background, and is motivated by face detection. We improve several key tactics, such as roi-pooling feature fusion and adding the Crystal Loss function to the original multi-task loss function, to extend the conventional Faster R-CNN scheme. In addition, a new Retinex-based LBP for face spoofing detection is described, which can handle diverse lighting circumstances. Finally, these two detectors are cascaded and produce promising results on the CASIA-FASD, REPLAY-ATTACK, and OULU-NPU benchmark databases. Furthermore, they also conduct cross-database tests to check the suggested cascade detector's generalisation capacity.

In [7] offers a novel feature learning technique for learning discriminative deep dynamic textures for 3D mask face anti-spoofing by R. Shao, X. Lan, and P. C. Yuen. A unique joint discriminative learning technique for learning the spatial and channel discriminability of deep dynamic textures is included in the learning model. Their proposed joint discriminative learning technique may be utilised to adaptively weight the discriminability of the learned feature from different spatial regions or channels, guaranteeing that more discriminative deep dynamic textures play a bigger role in face/mask categorization. The authors' proposed technique is effective in both intra- and cross-data set scenarios, according to experiments on a range of publically available data sets.

Authors A. Şengür et al in paper [8] uses of deep learning based models in face liveness detection systems. According to them very few works have made the use of convolutional neural network (CNN) for working on face liveness detection systems and those which have used CNN have used various fine-tuning approaches as well as different dataset for the purpose of training. The approach used in paper [8] is based on transfer learning, making use of some pre-trained CNNs architectures which are well-known, for the purpose. Various deep features are studied and compared on the common ground for face liveness detection in videos. After performing experimental analysis on well-known, publicly available databases such as NUAA and CASIA-FASD, it is observed that the methodology proposed gives satisfying results which can be compared with the same of other methods.

Alotaibi, A. in [9] proposes deep CNN architectures which has been applied in some recent work in face liveness detection because they provide superior liveness detection accuracy than the previous machine learning approaches. author uses a combination of diffusion of the collected image and a simple three-layer CNN architecture in their suggested study.

Boulkenafet et al. in [10] perform the analysis of luminance data from images of face which has been a major focus of research about non-intrusive software based face liveness detection systems, and this disregards the color component which can give vital information when detecting face liveness. This paper introduces a unique and fresh approach in face spoofing detection methodologies by making use of color texture analysis. The method proposed in this text focuses on obtaining complementary low level feature data from various color spaces. This information is then utilized in the form of joint color and texture data from the luminance and chrominance channels. To be more precise, feature histograms are calculated for each image band, differently. The paper states that the result of varied experiments performed on three standard datasets, specifically the CASIA Face Anti-Spoofing Database,

the Replay-Attack Database and MSU Mobile Face Spoof Database have been excellent. The paper states that the method proposed produces stable performance over all three datasets. The encouraging results imply that under unfamiliar circumstances, facial color texture representation is more reliable than the gray-scale one.

Authors Parveen S, Ahmad, S.M.S., Abbas, N.H., Adnan, Hanafi, Naeem at el in paper [11] proposes many approaches for determining the liveness of a captured static image by extracting elements from a 2D image and passing them to a classifier. Extraction of variants of Local Binary Patterns and use of a Support Vector Machine (SVM) classifier to determine whether the face is real or fake are two examples. authors proposed the Dynamic Local Ternary Pattern (DLTP), a texture descriptor in which the textural features of facial skin were investigated using dynamic thresholding and an SVM with linear kernel for classification.

Authors Y. Li, Y. Li, Q. Yan, H. Kong, and R. H. Deng at el in [12] captures the movement of a specific portion of the face, such as the lips or the eyes, might be an indicator of liveness; eye state and mouth state are two primary signs to be considered in life sign identification algorithms, which were developed in [12].

Andrea Lagorio et al in [17] offer a unique liveness detection approach based on the 3D structure of the face. Their proposed method allows a biometric system to distinguish between a real face and a photograph, hence minimising vulnerability. The proposed approach, according to the authors, can be used in two scenarios: as an anti-spoofing tool in conjunction with 2D face recognition systems, or as part of a 3D face recognition system for early detection of spoofing attempts. The suggested algorithm uses the 3D properties of the acquired face data to identify whether or not there is a live face in front of the camera. The lack of surface variation in the scan is one of the primary indicators that the acquisition is from a 2D source, according to the scientists. It has a very low curvature on the surface. A simple and fast approach is created to compare the two 3D scans based on the estimation of the surface's mean curvature. The primary components of the Cartesian coordinates within a specified neighbourhood are used to calculate an approximation of the actual curvature value at each place. After that, the mean curvature of the 3D points on face surface is calculated. Two experiments were devised by the authors. They employed FS and GVS sets in the first one. The False Rejection Rate (FRR) was computed as zero after separating the distributions of the mean curvature values for the two sets. They employed the FS and Bosforus sets in the second experiment. They run numerous experiments with values ranging from 4 to 20 to determine the algorithm's sensitivity. For different values of radius, the value of FRR at rank 1 is always equal to zero.

To handle dynamic face spoofing attacks and determine liveness of a video sequence, various ways have been proposed. Wang T. et al. in paper [14] suggested a detection method based on the analysis of sparse structural information in 3D space. From the given face footage, facial landmarks were recognised, and key frames were chosen from which the sparse 3D facial structure was restored. Following that, structures were aligned, and structure features were retrieved for classification utilizing an SVM classifier.

Authors G. Kim et al. in paper [15] has the main goal of to distinguish between a real face and an artificial face (two-dimensional paper masks) in terms of shape and detail. For distinguishing real faces from 2-D paper masks, a single image-based fake face identification approach based on frequency and texture studies is suggested. The authors used a power spectrum-based frequency analysis method that takes advantage of both low-frequency and high-frequency information. Furthermore, for assessing the textures on the given facial photos, a description approach based on Local Binary Pattern has been devised. They attempted to distinguish the live face image from 2-D paper masks using frequency and texture information.

The frequency information is used for two purposes, according to the authors. The first is the difference in presence of 3-D shapes that results in a difference in low frequency areas connected to lighting component created by the overall shape of a face. Second, discrepancy in detail information between the live faces and the masks causes a disparity in high frequency information.. Texture information is obtained because, when compared to photos acquired from 3-D objects, images taken from 2-D objects (specifically the illumination components) tend to lose texture information. Frequency-based feature extraction, Texture-based feature extraction, and Fusion-based feature extraction are all being used for feature extraction. The authors used a 2-D discrete Fourier transform to convert the face image into the frequency domain in order to extract frequency information. The altered product is then divided into many groups of concentric rings, each representing a frequency band region. Finally, the average energy values of all the concentric rings are combined to form a 1-D feature vector. They employed Local Binary Pattern (LBP), one of the most prevalent ways for representing the texture information of images, for texture-based feature extraction. The authors use a Support Vector Machine (SVM) classifier for learning liveness detectors using feature vectors created by power spectrum-based and LBP-based approaches in the final one, fusion-based feature extraction. The fusion-based method generates a feature vector by combining the SVM classifier's decision value. Power spectrum-based feature vectors are used to train SVM classifiers, while LBP-based feature vectors are used to train SVM classifiers. For their experiments, the authors employed two databases: the BERC Webcam Database and the BERC ATM Database. The false faces (non-live) were obtained from printed paper, magazine, and caricature photos, and all of the images in the webcam database were taken under three distinct lighting situations. When images are collected from prints and caricatures, the suggested approach's experimental results reveal that the LBP-based method outperforms the frequency-based method. Overall, the fusion-based method produced the greatest results, with an error rate of 4.42 percent, compared to 5.43 percent for frequency-based methods and 12.46 percent for LBP-based method.

Lin Sun, Gang Pan, Zhaohui Wu, Shihong Lao at el in [16] presented the blinking-based approach for liveness detection utilising Conditional Random Fields (CRFs). To account for long-range dependencies on the observation sequence, the authors used CRFs to represent blinking behaviours. The CRF model was then compared to a discriminative model such as AdaBoost and a generative model such as HMM. CRFs (conditional random fields) are probabilistic models for segmenting and labelling sequence data. They're commonly employed in natural language processing since they can accommodate long-range dependencies on the observation sequence. The action of blinking is represented by an image sequence consisting of pictures in near and non-close states.

B.G. Nalinakshi et al. [17] proposed system for identifying the user with face modality and detecting liveness utilising differences in facial eye, lip, chin, and forehead movements, the suggested model provides security to biometric systems. The suggested model provides security in two phases, namely authentication and liveness checks. This technique is tested on a group of 50 people who have a wide range of poses and expressions. Face recognition accuracy with the Indian face database is approximately 87 %, while face recognition accuracy with the own database is around 86 %, and liveness detection performance for verified users is around 88 %.

III. Conclusion

The goal of this study was to gain a better understanding of face liveness detection by updating and taxonomizing the literature. Another important aspect is that new researchers in this field will have a clear understanding of what face liveness detection is

and what opportunities there are to develop new methods, adopt new technologies, and explore specific directions and research gaps without wasting time on irrelevant research. In this paper we also discussed the various approaches a face liveness detection system can be based on, by focusing on the types features extracted from the image or video.

IV. REFERENCES

[1]. X. Zhu, S. Li, X. Zhang, H. Li and A. C. Kot, "Detection of Spoofing Medium Contours for Face Anti-Spoofing," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 31, no. 5, pp. 2039-2045, May 2021, doi: 10.1109/TCSVT.2019.2949868.

[2]. 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.

[3]. W. Sun, Y. Song, C. Chen, J. Huang and A. C. Kot, "Face Spoofing Detection Based on Local Ternary Label Supervision in Fully Convolutional Networks," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3181-3196, 2020, doi: 10.1109/TIFS.2020.2985530.

[4]. W. Sun, Y. Song, H. Zhao and Z. Jin, "A Face Spoofing Detection Method Based on Domain Adaptation and Lossless Size Adaptation," in IEEE Access, vol. 8, pp. 66553-66563, 2020, doi: 10.1109/ACCESS.2020.2985453.

[5]. Patil, Rashmi & Bellary, Sreepathi. (2020). Machine learning approach in melanoma cancer stage detection. Journal of King Saud University - Computer and Information Sciences. 10.1016/j.jksuci.2020.09.002.

[6]. H. Chen, Y. Chen, X. Tian and R. Jiang, "A Cascade Face Spoofing Detector Based on Face Anti-Spoofing R-CNN and Improved Retinex LBP," in IEEE Access, vol. 7, pp. 170116-170133, 2019, doi: 10.1109/ACCESS.2019.2955383.

[7]. R. Shao, X. Lan and P. C. Yuen, "Joint Discriminative Learning of Deep Dynamic Textures for 3D Mask Face Anti-Spoofing," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 4, pp. 923-938, April 2019, doi: 10.1109/TIFS.2018.2868230.

[8]. A. Şengür, Z. Akhtar, Y. Akbulut, S. Ekici and Ü. Budak, "Deep Feature Extraction for Face Liveness Detection," 2018 International Conference on Artificial Intelligence and Data Processing (IDAP), 2018, pp. 1-4, doi: 10.1109/IDAP.2018.8620804.

[9]. Alotaibi, A.; Mahmood, A. Deep face liveness detection based on nonlinear diffusion using convolutional neural network. SIViP 2017, 11, 713–720; doi:10.1007/s11760–016–1014–2.

[10]. Boulkenafet, Zinelabidine & Komulainen, Jukka & Hadid, Abdenour. (2016). Face Spoofing Detection Using Colour Texture Analysis. IEEE Transactions on Information Forensics and Security. 11. 1-1. 10.1109/TIFS.2016.2555286.

[11]. Parveen, S.; Ahmad, S.M.S.; Abbas, N.H.; Adnan, W.A.W.; Hanafi, M.; Naeem, N. Face Liveness Detection Using Dynamic Local Ternary Pattern (DLTP). Computers 2016, 5, 10.

[12]. Y. Li, Y. Li, Q. Yan, H. Kong, and R. H. Deng, “Seeing Your Face Is Not Enough: An Inertial Sensor-Based Liveness Detection for Face Authentication,” in CCS 15: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015, pp. 1558–1569.

[13]. Andrea Lagorio, Massimo Tistarelli, Marinella Cadoni, Liveness Detection based on 3D Face Shape Analysis, Biometrics and Forensics (IWBF), 2013 International Workshop on Page(s): 1-4, 2013

[14]. Wang, T.; Yang, J.; Lei, Z.; Liao, S.; Li, S.Z. Face Liveness Detection Using 3D Structure recovered from a single camera. In proceedings of the 2013 International Conference on Biometrics (ICB), Madrid, Spain, 4– 7 June 2013; pp. 1–6, doi:10.1109/ICB.2013.6612957.

[15]. G. Kim, S.Eum, J. K. Suhr, D. I. Kim, K. R. Park, and J, Kim, Face liveness detection based on texture and frequency analyses, 5th IAPR International Conference on Biometrics (ICB), New Delhi, India. pp. 67-72, March 2012

[16]. Lin Sun, Gang Pan, Zhaohui Wu, Shihong Lao, Blinking-Based Live Face Detection Using Conditional Random Fields, ICB 2007, Seoul, Korea, International Conference, on pages 252-260, August 27-29, 2007.

[17]. BG Nalinakshi, Sanjeevakumar M Hatture, Manjunath S Gabasavalgi, Rashmi P Karchi, “Liveness detection technique for prevention of spoof attack in face recognition system”, nternational Journal of Emerging Technology and Advanced Engineering, vol 3, issue 12, pages. 627-633, 2013.

Cite this article as :

Shweta Policepatil, Sanjeevakumar M. Hatture, "Face Liveness Detection : An Overview", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 8 Issue 4, pp. 22-29, July-August 2021. Available at doi : https://doi.org/10.32628/IJSRST21843
Journal URL : https://ijsrst.com/IJSRST21843