Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 11, No. 3, November : 2023

FACE SPOOFING DETECTION WITH LOCAL BINARY PATTERN

Er. Poonam Devi, Research Scholar, Dept. of CSE, SVIET.
Mr. Prince Sood, Assistant Professor, Dept. of CSE, SVIET.
Dr. Sourabh Sharma, Professor and Dean, Dept. of CSE, SVIET.

Abstract
The face spoof technique was proposed to identify and detect the spoofed and non-spoofed images. The DWT technique is used to analyze the textual features present within the test images. There is a possibility that some exceptional disturbances are available like geometric disturbances and the artificial texture disturbances. The camera and the illumination subordinates are mostly responsible for such disturbances. A perfect camera with no defects should be used just to notice the difference between the geometric, the illumination and the texture-based disturbances. To detect the whether the image is spoofed or non-spoofed already existed technique SVM classifier is used. The SVM based technique is proposed in the previous work for the detection of face spoof. The face spoof detection techniques are based on two steps, the first step is of feature extraction and second is of classification. The eigan based technique is applied for the feature extraction and SVM classifier is applied for the classification. To improve accuracy of the face spoof detection SVM classifier will be replaced with the hybrid classifier. The hybrid classifier will be the combination of decision tree and random forest classifier.

1. Introduction

Applications that require authentication can benefit from the strong and useful solution provided by biometrics. Nowadays, academia and industry are paying more and more attention to biometrics authentication thanks to deep learning because of its advancements in security compared to more conventional authentication techniques (such passwords, secret questions, and token codes) [1]. The most common biometric modalities are voice, iris, face, and fingerprints. Of them, "face" is the most widely used because it doesn't require any extra hardware resource and almost all smartphones come with a front-facing camera. Despite the effectiveness of face recognition, it is still susceptible to presentation attacks because of the prevalence of social media, where it is simple to obtain facial photos.As an illustration, a presentation assault can capture a person's facial information by printing (printing attack), replaying on a screen (replay attack), or even forging the face using 3D masking and VR, which poses highly difficult security challenges [2]. Numerous studies for face spoofing detection have been prompted by security issues with face recognition systems. A number of methods attempt to recover the distortion information that may be present in spoof face samples from the perspective of evaluating the disturbance information put into the spoofing media. Common spoofing artefacts include those related to texture, motion, and image quality. The facial recognition system may be tricked by imitating genuine faces.Before detecting facial photos, anti-spoofing technologies must be put in place to thwart these attacks. The security of the facial recognition system must be ensured [3]. If spoof attack attempts are made on an ordinary face recognition system that lacks intentional and concrete anti-spoofing features (as is the case with many face recognition systems in use), the system is likely to fail. Respondents provide the face recognition system with their facial features, which it then compares to the information in the base library ID. The system will regard the respondent as "real" and grant access to the main system if the comparison result score is less than the threshold. Even while the facial recognition technology has made great progress, it occasionally still confuses real faces with fraudulent ones [4]. A generalised depiction of a face recognition system is shown in Fig. 1.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 11, No. 3, November : 2023

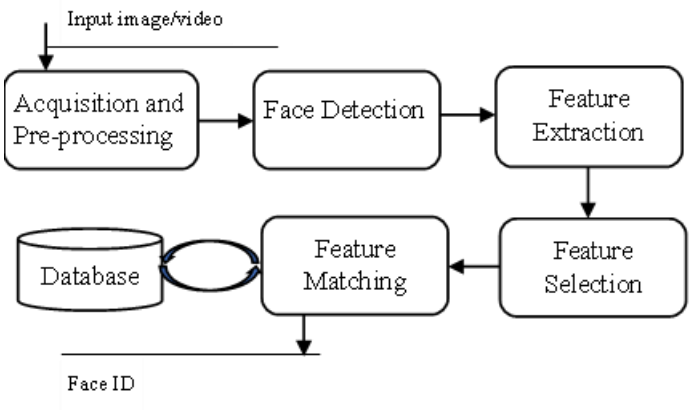

Figure 1: Pipeline of a Face Recognition System

Image capture and pre-processing are the first stages taken by every picture processing system for features extraction and image understanding. The input source, which can be either static images or streaming video, is used to generate the target images. Image processing systems must include picture pre-processing in order to achieve accurate results while also minimizing noise [5]. Systems in this condition must confront a wide range of challenges that could obstruct the entire process, especially in an unconstrained environment. These issues could include, among other things, variations in the image background, attitude, ageing, illumination, and expressions. Given that it has an impact on how well feature extraction functions, pre-processing a picture is always recommended as one of the first processes [6].Post-processing of data might be considered for the removal of noise from the given image in the case of an uncontrolled environment where learning is influenced by external variables. Facial detection is the process of locating and isolating the face region from the surrounding area. It is a further critical step in the overall facial recognition process and has undergone substantial research in the field of machine vision. Early face recognition techniques were able to swiftly recognise facial features in input photographs [7]. It eventually became a vibrant study area and a fundamental part of any framework for understanding faces visually.

The first task of any face recognition system is feature extraction. It has a significant impact on the system's overall effectiveness. There are different varieties of feature extractor models, such as SIFT, SVM, STIP, and STISM. A variety of criteria have been used to categorise feature extraction techniques, including global vs. local [8], hand-crafted vs. learning-driven, and 2D vs. 3D features extraction schemes. Feature extractors or descriptors commonly generate a large feature space for a single image when attempting to identify a person in a streaming video. The huge feature space is then further processed using a variety of techniques in order to narrow down the most crucial features and lessen dimensionality.This enhances system performance by lowering total expenses and making better use of the system period for recognition [9]. The primary features are taken from the input facial image and then iteratively matched to meet the goal objective. Face recognition that is iterative is a process. The identifier is just taken out of the database by the system. Researchers have proposed a substantial number of remedies in the research as a result of the recent increase in interest in face spoof detection [10]. Three different face spoofing detection techniques are briefly discussed in this section: texture-based techniques, motion-based techniques, and picture quality and reflectance-based techniques. Since the bulk of face recognition systems only employ RGB cameras, integrating texture information has been an obvious approach for preventing face spoofing.Numerous texture-based features are researched in this domain to prevent face faking. CNN-based features and handcrafted features can be readily divided from two categories [11]. ConvNet-conditioned features or ConvNets have been used in face anti-spoofing in multiple recent attempts as a result of deep learning's success in resolving a wide range of computer vision issues. The majority of research techniques approach anti-spoofing as a straightforward binary classification issue with softmax loss. To defend against

display and picture attacks, motion-based approaches use facial movements such moving lips, blinking eyes, and other facial expressions [12]. By replicating the varying stages of eye blinking, eye movement is used as an effective cue for face anti-spoofing.The detection of spoofing attacks also makes use of mouth movement in tandem with eye blinking. The approaches based on image quality and reflectance are reviewed in the literature since the recovered picture and video may result in a loss of image quality and variations in reflectance. These methods extract specular reflection, blurriness [13], chromatic moment, and colour variety from the liquid crystal display (LCD) screen to explain the changes in surface reflection between the real and fake faces [14]. Numerous researches use optical flow features and image-quality features to distinguish real faces from fake faces. Furthermore, the elements that are most useful for spotting face spoofing can be extracted by analysing the noise information in phoney face photographs using the Fourier spectrum [15].These reflectance- and image-based approaches defend against low-resolution attacks well, but they may fall short when faced with spoof artefacts that are incredibly convincing [16].

2. Literature Review

Yaman Akbulut,et.al (2017) studied that the identity as well as liveness of the input of face can be known through a reliable face-based access system [17]. Thus, several feature-based spoof face detection techniques have been proposed by different researchers. For detecting the liveness of a face, a series of processes are applied on the input image. A deep-learning based face spoof detection approach is proposed in this paper by using two various deep learning methods. The local receptive fields (LRF)-ELM and CNN are known to be these two methods. For increasing the speed of processing of a model, LRF-ELM was introduced lately in which a convolution and pooling layer was included. There are a series of convolution and pooling layers, however, present within CNN. NUAA and CASIA are the two common face spoof detection databases on which the experiments were conducted to evaluate the performance of proposed approach. The performance of LFR-ELM approach was known to be better within both the databases as per the comparisons made towards the end.

YasarAbbas Ur Rehman, et.al (2018) proposed an efficient mechanism to train the deep CNN classifiers to detect the face liveness [18]. When the CNN classifiers are to be trained on small scale face anti-spoofing database, the continuous data-randomization is utilized as small mini-batches. There is reduction in the training time along with reduction in the HTER as per the experimental results achieved when implementing the proposed approach. Further, on the intra-database and cross-database face liveness detection tests, efficient results are achieved by the proposed technique. Thus, an overall improvement is achieved by the proposed mechanism.

Shervin Rahimzadeh, et.al (2017) presented a study related to the issues faced when detecting the face spoof [19]. It is possible to include new means of spoofing attackers as per the various observations made. The image sensor inter-operability issue and the minimal size of a sample are few of the issues that have come forward within this work. This paper initially proposed a new evaluation protocol through which the effects of unseen attack types could be known on the basis of certain existing factors. From the training set, the samples that were of similar to that of a test sample were excluded as per the novel mechanism. For accounting the variability of imaging conditions, both inter and intra database experiments were performed by applied the proposed mechanism. This paper proposed a novel and highly realistic formulation of the spoofing detection issue with respect to the conceptual innovations. To train the systems, only the positive samples were needed by the new formulation. Towards the end, the experiments conducted showed that there was still the need to improve the detection rates since the performance of both the schemes was not up to the mark.

ZinelabidineBoulkenafet, et.al (2016) presented that the analysis of luminance information of the face images is a major focus for the non0intrusive software based face spoof detection approaches [20]. Therefore, to differentiate the fake faces from genuine ones, the chroma component is discarded here.

To detect the face spoof using color texture analysis, a novel and appealing approach is proposed in this paper. The complementary low-level feature descriptions are extracted from various color spaces for exploiting the joint color-texture information from various channels. Individually, over each image band, the feature histograms are calculated. Highly efficient results were achieved in comparison to the earlier methods as per the experiments conducted on the most challenging datasets. Also, across all three benchmark datasets, the proposed approach is most likely to achieve highly efficient results, which was difficult to the traditional approaches. The stability of facial color texture representation was known to be higher in comparison to the gray-scale regions as per the results achieved after the evaluations.

XiaoleiLiu, et.al (2017) presented that by providing the printed or downloaded images or candid videos to the sensor, the legal identity authentication can be achieved by impostors to develop face recognition systems [21]. For recognizing whether the face map is real or fake, an improved face local binary feature (ELBP) of a face map is extracted through this paper. The proposed method is known to be convenient and effective as compared to the other static or dynamic approaches proposed previously. Upon the NUAA datasets, around 95% of correct recognition rate is achieved here. The performances of proposed algorithm are known to be better with the help of comprehensive analysis as well as comparisons made amongst the proposed and existing algorithms.

XiaochaoZhao, et.al (2017) presented a study related to representing and recognizing the dynamic textures of input images [22]. Aspatio-temporal descriptor is proposed on the basis of LBC. The neighboring pixels are thresholded with the central pixel present within the local volume by the proposed descriptor similar to the VLBP mechanism. However, only the numbers of 1s are counted by the VLBC approach and the local structure is abandoned. The information related to the local contrast and central pixel intensity is involved within the completed VLBC version due to which the performance of the system is also enhanced. Further, from these codes, the histograms are also extracted. For representing a DT sequence, a joint 3D histogram is utilized here. For the DT classification, the negative log-likelihood distance-based NN classified is applied to conduct experiments. Comparisons of proposed and existing methods are done on various databases which show that the DT classification provides highly effective results by applying the proposed descriptor. Upon three databases as well, the applied CVLBC for 2D face spoofing detection provides better results. Thus, the variations in motion and appearance amongst the facial videos of the users can be characterized properly by the application of proposed mechanism.

Haoliang Li, et.al (2018) proposed an unsupervised domain adaptation mechanism which is an anti-spoofing approach to be applied in facial images [23]. The training samples present within the different source environment are used for proposing this approach. Particularly, depending upon the source and target domain data, initially an embedding function is imposed. To the new space in which the distribution similarity can be measured, the data is mapped through this function. There is reduction of Maximum Mean Discrepancy amongst the latent features present within the source and target domains so that it is possible to learn a classifier that is more generalized. For knowing the capability of features that are both hand-crafted and involve deep neural network learning, these features are utilized within the proposed framework. Further, a new database that includes more than 3000 face samples is generated for face spoof detection. An improved generalization capability is achieved within the cross-domain environments thus improving the performance of anti-spoofing as per the simulation results achieved by performing experiments on the new database.

FeiPeng, et.al (2018) proposed guided scale space for reducing the influence of redundant noise contamination [24]. The redundancy of original facial texture is minimized and highly powerful facial edges have been extracted. For the extraction of liveness detection features, two guided scale texture descriptors have been proposed which are dependent on the guided scale space. The edge preservation property of guided scale space is applied by the guided scale based local binary pattern (GS-LBP). For

encoding the neighboring relationships of the original face as well as the guided scale face, the local guided binary pattern (LGBP) is applied. No additional features are utilized to identify this relationship. The linear support vector machine classifier is applied along with the guided scale texture features to detect the presentation attack. On various databases, the experiments are conducted which show that the proposed approach is more effective, in comparison to previously proposed techniques. Keyurkumar Patel, et.al (2016) presented a study on the smartphone unlock systems that are today very popular within several mobile phones and also within the systems that include mobile payments [25]. An unconstrained smartphone spoof attack database (MSU USSA) that includes not less than 1000 subjects is generated here. Using the front as well as rear camera of a smartphone, the images of print and replay attacks are gathered. Various intensity channels, image areas, as well as feature descriptors are used for analyzing the image distortion of print and replay attacks. The Android smartphone is used to develop an efficient face spoof detection approach. As per the experiments conducted it is seen that to detect the face spoofs of both, cross-database and intra-database testing environments, the proposed approach provided effective results. There were around 20 participants included within the evaluations which showed that the performance of proposed approach within real applications was very good.

References

[1] J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of Fourier spectra," Proc. SPIE, vol. 5404, pp. 296–303, Aug. 2004.
[2] K. Kollreider, H. Fronthaler, M. I. Faraj, and J. Bigun, "Real-time face detection and motion analysis with application in „liveness" assessment," IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 548–558, Sep. 2007
[3] J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection with component dependent descriptor," in Proc. IJCB, Jun. 2013, pp. 1–6.
[4] T. Wang, J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection using 3D structure recovered from a single camera," in Proc. ICB, Jun. 2013, pp. 1–6.
[5] S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, "Computationally efficient face spoofing detection with motion magnification," 2013, in Proc.CVPR Workshops. IEEE Trans. Image Process. vol. 23, no. 2, pp. 710–724
[6] Shailendra Kumar Dewangan, "Human Authentication Using Biometric Recognition", International Journal of Computer Science & Engineering Technology (IJCSET), ISSN: 2229-3345, Vol. 6, No. 4, pp. 240-245, April 2015.
[7] A. Rattani, N. Poh, and A. Ross, "Analysis of user-specific score characteristics for spoof biometric attacks," in Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), Jun. 2012, pp. 124–129.
[8] L. Best-Rowden, H. Han, C. Otto, B. F. Klare, and A. K. Jain, "Unconstrained face recognition: Identifying a person of interest from a media collection," IEEE Trans. Inf. Forensics Security, vol. 9, no. 12, pp. 2144–2157, Dec. 2014.
[9] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in Proc. IEEE BIOSIG, Sep. 2012, pp. 1–7.
[10] N. Erdogmus and S. Marcel, "Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect," in Proc. IEEE BTAS, Sep./Oct. 2013, pp. 1–6.
[11] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in Proc. IJCB, Oct. 2011, pp. 1–7.
[12] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," in Proc. ECCV, Sep. 2010, pp. 504– 517.

[13] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face antispoofing database with diverse attacks," in Proc. ICB, Mar./Apr. 2012, pp. 26–31.
[14] L. Sun, G. Pan, Z. Wu, and S. Lao, "Blinking-based live face detection using conditional random fields," in Proc. AIB, 2007, pp. 252–260.
[15] W. Bao, H. Li, N. Li, and W. Jiang, "A liveness detection method for face recognition based on optical flow field," in Proc. IASP, Apr. 2009, pp. 233–236.
[16] S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, "Computationally efficient face spoofing detection with motion magnification," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), Jun. 2013, pp. 105–110.
[17] YamanAkbulut, AbdulkadirSengur, ÜmitBudak, Sami Ekici, "Deep Learning based Face Liveness Detection in Videos", 2017, IEEE
[18] Yasar Abbas Ur Rehman, Lai Man Po, Mengyang Liu, "LiveNet: Improving features generalization for face liveness detection using convolution neural networks", 2018 Elsevier Ltd. All rights reserved
[19] ShervinRahimzadeh, Arashloo, Josef Kittler, and William Christmas, "An Anomaly Detection Approach to Face Spoofing Detection: A New Formulation and Evaluation Protocol", 2017 IEEE
[20] ZinelabidineBoulkenafet, JukkaKomulainen and AbdenourHadid, "Face Spoofing Detection Using Colour Texture Analysis", 2016, IEEE Transactions On Information Forensics And Security
[21] Xiaolei Liu, Runge Lu, Wei Liu, "Face Liveness Detection Based on Enhanced Local Binary Patterns", 2017, IEEE
[22] Xiaochao Zhao, Yaping Lin, and Janne Heikkila, "Dynamic Texture Recognition Using Volume Local Binary Count Patterns with an Application to 2D Face Spoofing Detection", 2017, IEEE
[23] Haoliang Li, Wen Li, Hong Cao, Shiqi Wang, Feiyue Huang, and Alex C. Kot, "Unsupervised Domain Adaptation for Face Anti-Spoofing", 2018, IEEE Transactions On Information Forensics And Security
[24] Fei Peng & Le Qin & Min Long, "Face presentation attack detection using guided scale texture", 2018, Multimedia Tools and Applications, Volume 77, Issue 7, pp 8883–8909
[25] Keyurkumar Patel, Hu Han, and Anil K. Jain, "Secure Face Unlock: Spoof Detection on Smartphones", 2016, IEEE Transactions On Information Forensics and Security