International Journal of Engineering Technology and Applied Science
(ISSN: 2395 3853), Vol. 9 Issue 9 September 2023

Face Anti-Spoofing Detection using Machine Learning Algorithm

Ms. Bhavana Parmar[1], Prof. Chetan Gupta[2]
chingaparmar25@gmail.com[1], chetangupta.gupta1@gmail.com[2]
M.Tech Research Scholar, Dept. of CSE[1], Asst. Prof., Dept. of CSE[2]
SIRTS, Bhopal[1], SGI, Bhopal[2]

Abstract: -Face spoofing detection is one of the most well-studied problems in computer vision. Face recognition has become a widely adopted technique in biometric authentication systems. In face recognition based authentication techniques, the system first recognized the person to verify the legitimacy of the user before granting access to the system resources. The system must be able to determine the liveness of the person in front of the camera, for example, by recognizing the face and denying the types of face presentation attacks related to photographs, videos and the 3D mask of the targeted person. Attackers try to directly or indirectly, masquerade the biometric system as another person by forging biometric traits and get unauthorized access. This work studies computer vision-based feature extraction techniques for real and spoof face imaging and combines different features in the area of face anti-spoofing.

Keywords: - Face Spoofing, Face Recognition, Machine Learning (ML)

I. INTRODUCTION

Every day we come across biometric systems for authentication and many other purposes. The biometrics includes the face, iris, and fingerprint and palm recognition. But the criminals very accurately stimulate the biometrics of the genuine users to access their private systems and this process is called a spoofing attack. It is comparatively easy for the criminals to spoof iris, fingerprint and palm to face spoofing [1, 2]. Face recognition is universally used to ensure authenticity. Mobile unlocking, to safe deposit, locker unlocking exercised face recognition technology. However, hackers or the criminals pretend to pose as a genuine user in three peculiar ways for instance photo attacks, replay video attacks and 3-D mask attack. Presenting themselves as a real user by the way of using printed photo face is entitled as photo attacks [3].

To prohibit impostors from this attack, highlight removal method, User interaction method had been formalized. However, impostors find a way to avail the resources. They exploit motion picture and video replay attacks, 3-D mask attacks to beneficially acquire the user's possessions. Hence, various states-of -art methods have been evolved to retard the imitators. The existing methodologies include Face liveliness detection, Texture analysis, User Interaction (Eye and head movements), Image Quality Assessment, Image Distortion Analysis, Depth sensing, Convolutional neural networks [4, 5]. The success of machine learning in computer vision provides a strong hope of its use in biometrics for the face ant spoofing and other similar applications. With these neural architectures, it is easy for us to solve complex solutions with better performance and features. They work with high-level features and are self-trained from the training dataset. The machine learning is able to deal with digital images with better performances. Many kinds of research are done with neural layers to achieve more accuracy and increase its performance [6].

II. LITERATURE REVIEW

Wanling Zhang et al. [1],a face against mocking procedure by utilizing DWT (Discrete Wavelet Transform), LBP (Local Binary

Pattern) and DCT (Discrete Cosine Transform) with a SVM classifier to assess whether a video is legitimate. First and foremost, the DWT highlights are delivered by deteriorating some chosen outlines into various recurrence parts at the multi-goal blocks. Besides, the DWT-LBP highlights are produced to address spatial data of the squares by interfacing LBP histograms of the DWT blocks in each edge on a level plane. Then, at that point, the DWT-LBP-DCT highlights with the fleeting data of a video document are accomplished by performing DCT procedure on the DWT-LBP elements of those chose outlines upward. Accordingly, these took advantage of DWT-LBP-DCT highlights have the ability to address the recurrence spatial–fleeting data of a video. At last, the SVM classifier with RBF piece is prepared for face against mocking. Contrasted and past phenomenal works, exploratory outcomes on two benchmark information bases (REPLAY-ATTACK and CASIA-FASD) have shown the proposed approach has better discovery execution.

Z. Wang et al. [2], face against ridiculing is basic to the security of face acknowledgment frameworks. Profundity directed learning has been demonstrated as one of the best techniques for face against mocking. Notwithstanding the extraordinary achievement, most past works actually define the issue as a solitary casing perform multiple tasks one by just enlarging the misfortune with profundity, while dismissing the nitty gritty fine-grained data and the exchange between facial profundities and moving examples. Conversely, we plan another way to deal with recognize show assaults from numerous edges dependent on two experiences: 1) nitty gritty discriminative pieces of information (e.g., spatial angle extent) among living and mocking face might be disposed of through stacked vanilla convolutions, and 2) the elements of 3D moving appearances give significant insights in distinguishing the ridiculing faces. The proposed technique can catch discriminative subtleties through Residual Spatial Gradient Block (RSGB) and encode spatio-worldly data from Spatio-Temporal Propagation Module (STPM) effectively. Also, an original Contrastive Depth Loss is introduced for more precise profundity oversight. To survey the adequacy of our strategy, we likewise gather a Double-modular Anti-ridiculing Dataset (DMAD) which gives genuine profundity to each example. The investigations show that the proposed approach accomplishes best in class results on five benchmark datasets including OULU-NPU, SiW, CASIA-MFSD, Replay-Attack, and the new DMAD.

S. Zhang et al. [3], face against mocking is fundamental to keep face acknowledgment frameworks from a security break. A significant part of the advances have been made by the accessibility of face against caricaturing benchmark datasets lately. Notwithstanding, existing face against mocking benchmarks have set number of subjects ($\leq$170) and modalities ($\leq$2), which thwart the further improvement of the scholarly local area. To work with face against caricaturing research, we present an enormous scope multi-modular dataset, in particular CASIA-SURF, which is the biggest openly accessible dataset for face hostile to satirizing as far as the two subjects and visual modalities. In particular, it comprises of 1,000 subjects with 21,000 recordings and each example has 3 modalities (i.e., RGB, Depth and IR). We additionally give an estimation set, assessment convention and preparing/approval/testing subsets, fostering another benchmark for face hostile to satirizing. Also, we present a new multi-modular combination strategy as standard, which performs highlight re-weighting to choose the more enlightening channel highlights while smothering the less valuable ones for every modular. Broad investigations have been led on the proposed dataset to check its importance and speculation ability.

X. Yang et al. [4], Face against mocking is a significant errand in full-stack face applications including face discovery, check, and acknowledgment. Past approaches construct models on datasets which don't recreate this present reality information well (e.g., little scale, immaterial difference, and so on)

Existing models may depend on helper data, which keeps these ant spoofing arrangements from summing up well by and by. In this paper, we present an information assortment arrangement alongside an information amalgamation strategy to reenact advanced medium-based face satirizing assaults, which can undoubtedly assist us with getting an enormous measure of preparing information well mirroring these present reality situations. Through taking advantage of a clever Spatio-Temporal against Spoof Network (STASN), we can push the exhibition on open face hostile to mocking datasets over state of-the-workmanship strategies by a huge degree. Since the proposed model can naturally take care of discriminative locales, it makes breaking down the practices of the organization conceivable. We direct broad investigations and show that the proposed model can recognize parody faces by extricating highlights from an assortment of locales to search out unobtrusive confirmations like boundaries, moire examples, and reflection antiques, and so on.

J. Zhang et al. [5], face biometrics have accomplished exceptional execution over the previous many years, yet unforeseen caricaturing of the static faces represents a danger to data security. There is an expanding interest for steady and discriminative organic modalities which are difficult to be copied and misled. Discourse driven 3D facial movement is an unmistakable and quantifiable conduct signature that is promising for biometrics. In this paper, we propose a clever 3D behavior metrics structure dependent on a "3D visual password" got from discourse driven 3D facial elements. The 3D facial elements are mutually addressed by 3D-keypoint-based estimations and 3D shape fix highlights, extricated from both static and discourse driven powerful districts. A group of subject-explicit classifiers are then prepared over chosen discriminative highlights, which considers a discriminant discourse driven 3D facial elements portrayal. We build the primary freely accessible Speech-driven 3D Facial Motion dataset (S3DFM) that incorporates 2D-3D face video in addition to sound examples from 77 members. The exploratory outcomes on the S3DFM show that the proposed pipeline accomplishes a face distinguishing proof pace of 96.1%. Definite conversations are introduced, concerning hostile to satirizing, head present variety, video outline rate, and pertinence cases. We additionally give examination with different baselines on "profound" and "shallow" 2D face highlights.

X. Li et al. [6], face biometric frameworks are helpless against spoofingattacks. Such assaults can be acted in numerous ways, includingpresenting a falsified picture, video or 3D cover of a substantial user.A broadly involved methodology for separating certified appearances fromfake ones has been to catch their intrinsic contrasts in (2Dor 3D) surface utilizing neighborhood descriptors. One impediment of thesemethods is that they might fall flat assuming an inconspicuous assault type, for example ahighly reasonable 3D veil which looks like genuine skin surface, isused in spoofing. Here we propose a strong enemy of spoofing methodby recognizing beat from face recordings. In view of the way that apulse signal exists in a genuine living face however not in any maskor print material, the strategy could be a summed up solutionfor face liveness recognition. The proposed strategy is evaluatedfirst on a 3D cover spoofing information base 3DMAD to demonstrate its viability in recognizing 3D veil assaults. More importantly,our cross-data set analysis with great REAL-F masksshows that the beat based technique can recognize even thepreviously inconspicuous veil type while surface based strategies failto sum up past the improvement information. At long last, we proposea powerful course framework joining two corresponding assault specific parody indicators, for example use beat location against printattacks and shading surface investigation against video assaults.

L. Feng et al. [7], numerous characteristic explicit countermeasures to confront satirizing assaults have been created for security of face validation. In any case, there is no better face

against satirizing strategy than manage each sort of caricaturing assault in shifting situations. To further develop the speculation capacity of face hostile to ridiculing approaches, an extendable multi-signs incorporation structure for face against satirizing utilizing a progressive neural organization is proposed, which can intertwine picture quality signals and movement prompts for liveness discovery. Shear let is used to foster a picture quality-based liveness highlight. Thick optical stream is used to remove movement based liveness highlights. A bottleneck include combination technique can coordinate diverse liveness includes adequately. The proposed approach was assessed on three public face hostile to caricaturing information bases. A half all out blunder rate (HTER) of 0% and an equivalent mistake rate (EER) of 0% were accomplished on both REPLAY-ATTACK information base and 3D-MAD data set. An EER of 5.83% was accomplished on CASIA-FASD information base.

Table 1: Summary of Literature Review

S. No.	Author	Year of publication	Technique	Results
1.	Wanling Zhang and Shijun Xiang	Elsevier, 2020	Face anti-spoofing detection using DWT-LBP technique	EER-dev=0.026, HTER-test = 0.061, EER-test = 0.064, Accuracy = 92.738
2.	Z. Wang, Z. Yu, C. Zhao, X. Zhu, Y. Qin, Q. Zhou, F. Zhou, Z. Lei	IEEE 2020	Face anti-spoofing using deep spatial gradient and temporal depth learning	Accuracy = 90.693, Precision = 84%, Recall = 76%
3.	S. Zhang, X. Wang, A. Liu, C. Zhao, J. Wan, S. Escalera, H. Shi, Z. Wang, S.Z. Li	IEEE 2019	Face anti-spoofing using multi-model technique	Accuracy = 88.784, Precision = 83%, Recall = 72%
4.	X. Yang, W. Luo, L. Bao, Y. Gao, D. Gong, S. Zheng, Z. Li, W. Liu	IEEE 2019	Face anti-spoofing detection using DWT technique	EER-dev=0.022, HTER-test = 0.057, EER-test = 0.061, Accuracy = 87.73
5.	J. Zhang, R.B. Fisher	IEEE 2019	Face anti-spoofing detection using LBP technique	Accuracy = 86.084, Precision = 81%, Recall = 69%
6.	X. Li, J. Komulainen, G. Zhao, P.C. Yuen, M. Pietikainen	IEEE 2017	Face anti-spoofing using curvelet transform	EER-dev=0.019, HTER-test = 0.057, EER-test = 0.056, Accuracy = 84.73
7.	L. Feng, L.M. Po, Y. Li, X. Xu, Y. Fang, C.H. Cheung, K.W. Cheung	IEEE 2016	Face anti-spoofing using DCT technique	Accuracy = 83.33, Precision = 76%, Recall = 69%

III. PROBLEM IDENTIFICATION

The facial recognition frameworks are highly vulnerable to spoofing attacks and this vulnerability generates an effective security concerned issues in biometric domain.

- Moreover, some of the earlier proposed approaches have attained attractive results with intra test evaluation done to detect the face spoofing attack.
- However, this impact is considered as a major difficulty in the highly focused biometric anti-spoofing research domain.
- A biometric recognition system that is used to recognize the genuine entries, extracts the

features among a set of users input image [7, 8].

- The person's identity is established by comparing the extracted feature set against a set of feature sets in the database.
- The object is to increase accuracy and to decrease the false positives occurred in the preceding papers.
- To decrease the complexity in the cases of high dimensional data.Also make data sets available for face spoofing attack while suppressing the features with increase detection [9].

IV. CHALLENGES OF FACE RECOGNITION

Pose/Viewpoint: - It is a particular attitude or instance, especially with the hope of impressing others and to present one insincerely. It is a movement in which the dancer steps, in any desired position,from one foot to the other and it is a straight knee onto the flat foot.

Facial Expression: -A facial expression is one or more motions or positions of the muscles beneath the skin of the face. According to one set of controversial theories, these movements convey the emotional state of an individual to observers. Facial expressions are a form of nonverbal communication.

Occlusion: -Occlusion occurs when a portion of the picture visible on one image is occluded in the other by the scene itself or, a section of the scene near the image boundary moves out of the field of persuasion on the other picture.

Image Orientation: -The image-orientation property allows us to rotate an image in multiples of 90 degree. Values like 47 degree are rounded to the nearest multiple of 90.

Spoofing: - The word "spoof" means to trick, or deceive. Therefore, spoofing refers tricking or deceiving computer systems or other computer users. This is typically done by hiding one's identity or faking the identity of another user on the Internet.

Spoofing Attack:- It is a situation in which one person (or) program successfully masquerades as another by falsifying data, thereby gaining an illegitimate advantage.Some of the methods that are used for spoofing facial recognition system are by presenting fake faces with mask,Printed photos,Videos etc.

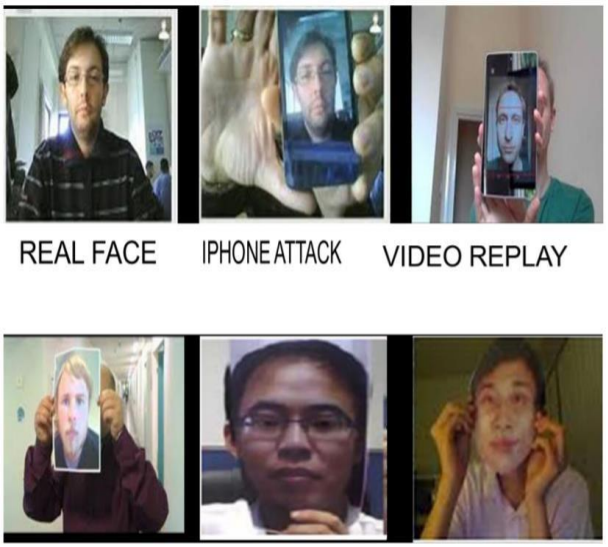

Figure 1: Types of Spoofing Attack [10]

V. FACE ANTI-SPOOFING DETECTION USING MACHINE LEARNING

Spoof detection is able to provide generalized performance and be able to be utilized in improving the effectiveness of the system particularly when working with noisy images.The anti-spoofing community should also consider engaging in new fundamental research regarding the biological dimension of biometric traits, in order to break with the current popular trend embraced by many of the latest research where some well-known sets of features are extracted from images in public databases and passed through a classifier. Classification plays again a vital role in recognition,some of the optimization techniques can be used for enhancing the performance of the system. Spoof detection

measures appear to play an important role in human vision and could be incorporated into feature descriptors in a more general form than the single spatial frequency used by the current descriptors [10, 11].

Machine Learning

Machine Learning is a subset of Artificial Intelligence concerned with "teaching" computers how to act without being explicitly programmed for every possible scenario. The central concept in Machine Learning is developing algorithms that can self-learn by training on a massive number of inputs. Machine learning algorithms are used in various applications, such as email filtering and computer vision, where it is difficult or infeasible to develop conventional algorithms to perform the needed tasks [14]. Machine learning enables the analysis of vast amounts of information. While it usually delivers faster, more precise results to identify profitable prospects or dangerous risks, it may also require additional time and assets to train it appropriately. Merging machine learning with AI and perceptive technologies can make it even more effective in processing vast volumes of information. Machine learning is closely associated with computational statistics, which focuses on making predictions using computers. Machine learning approaches are conventionally divided into three broad categories, namely Supervised Learning, Unsupervised Learning & Semi-supervised Learning, depending on the nature of the "signal" or "feedback" available to the learning system.

Face anti-spoofing (FAS) has lately attracted increasing attention due to its vital role in securing face recognition systems from presentation attacks (PAs). As more and more realistic PAs with novel types spring up, traditional FAS methods based on handcrafted features become unreliable due to their limited representation capacity. With the emergence of large-scale academic datasets in the recent decade, machinelearning based FAS achieve remarkable performance and dominate this area [12][13][15].

Supervised Learning: A model is trained through a process of learning in which predictions must be made and corrected if those predictions are wrong. The training process continues until a desired degree of accuracy is reached on the training data. Input data is called training data and has a known spam / not-spam label or result at one time.

Unsupervised Learning: By deducting the structures present in the input data, a model is prepared. This may be for general rules to be extracted. It may be through a mathematical process that redundancy can be systematically reduced, or similar data can be organized. There is no labeling of input data, and there is no known result.

Semi-Supervised Learning: Semi-supervised learning fell between unsupervised learning (without any labeled training data) and supervised learning (with completely labeled training data). There is a desired problem of prediction, but the model needs to learn the structures and make predictions to organize the data. Input data is a combination of instances that are marked and unlabeled.

VI. CONCLUSION

In this paper, a framework is review with machine learning to detect the spoofed face. The image is given as an input to the machine learning framework. Since we used the strategy of training the fake and real face dataset separately it is easy and efficient for the system to classify the image between real and fake when an input image is given. The flexibility of the neural layers is the main reason for the better performance in detecting the spoofed images.

REFERENCES

[1] Wanling Zhang and Shijun Xiang, "Face anti-spoofing detection based on DWT-LBP-DCT

features", Signal Processing: Image Communication, Elsevier, 2020.

[2] Z. Wang, Z. Yu, C. Zhao, X. Zhu, Y. Qin, Q. Zhou, F. Zhou, Z. Lei, Deep spatial gradient and temporal depth learning for face anti-spoofing, in: The IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2020.

[3] S. Zhang, X. Wang, A. Liu, C. Zhao, J. Wan, S. Escalera, H. Shi, Z. Wang, S.Z. Li, A dataset and benchmark for large-scale multi-modal face anti-spoofing, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2019, pp. 919–928.

[4] X. Yang, W. Luo, L. Bao, Y. Gao, D. Gong, S. Zheng, Z. Li, W. Liu, Face antispoofing: Model matters, so does data, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2019, pp. 3507–3516.

[5] J. Zhang, R.B. Fisher, 3D Visual passcode: Speech-driven 3D facial dynamics for behaviometrics, Signal Process. 160 (2019) 164–177.

[6] X. Li, J. Komulainen, G. Zhao, P.C. Yuen, M. Pietikainen, Generalized face antispoofing by detecting pulse from face videos, in: International Conference on Pattern Recognition, 2017.

[7] L. Feng, L.M. Po, Y. Li, X. Xu, Y. Fang, C.H. Cheung, K.W. Cheung, Integration of image quality and motion cues for face anti-spoofing, J. Vis. Commun. Image Represent. 38 (C) (2016) 451–460.

[8] K. He, X. Zhang, S. Ren, J. Sun, Deep residual learning for image recognition, in:Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition,2016, pp. 770–778.

[9] M. Asim, Z. Ming, M.Y. Javed, CNN Based spatio-temporal feature extraction forface anti-spoofing, in: 2017 2nd International Conference on Image, Vision andComputing (ICIVC), IEEE, 2017, pp. 234–238.

[10] E. Marasco, A. Ross, A survey on antispoofing schemes for fingerprint recognition systems, AcmComput. Surv. 47 (2) (2015) 1–36.

[11] S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, A.T. Ho, Detection of face spoofing using visual dynamics, IEEE Trans. Inf. Forensics Secur. 10 (4) (2015) 762–777.

[12] P. Allan, P. Helio, S. William Robson, R. Anderson, Face spoofing detectionthrough visual codebooks of spectral temporal cubes, IEEE Trans. Image Process.24 (12) (2015) 4726–4740.

[13] S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, A.T. Ho, Detection offace spoofing using visual dynamics, IEEE Trans. Inf. Forensics Secur. 10 (4)(2015) 762–777.

[14] P.L.D. Leon, M. Pucher, J. Yamagishi, I. Hernaez, I. Saratxaga, Evaluation ofspeaker verification security and detection of HMM-based synthetic speech, IEEETrans. Audio Speech Lang. Process. 20 (8) (2012) 2280–2290.

[15] H. Wendt, S.G. Roux, S. Jaffard, P. Abry, Wavelet leaders and bootstrap for multifractal analysis of images, Signal Process. 89 (6) (2009) 1100–1114.