VFAST Transactions on Software Engineering
https://vfast.org/journals/index.php/VTSE@ 2024, ISSN(e): 2309-3978, ISSN(p): 2411-6246
Volume 12, Number 2, April-June 2024 *pp:85-94*

A Robust Hybrid Texture Descriptor (HTD) and a parallel score based fusion for face verification and liveness detection system

Sajida Parveen [1*], **Sharifah Mumtazah** [2], **Nadeem Naeem** [3], **Imtiaz Ali Halepoto** [1], **Shamashad Lakho** [4]

[1]Department of Software Engineering, Quaid-e-Awam university of Engineering, Science and Technology, Nawabshah, Pakistan.; [2]Department of Computer and Communication Systems Engineering, Universiti Putra Malaysia (UPM), Serdang, Malaysia.; [3]Department of Electronic Engineering, Quaid-e-Awam university of Engineering, Science and Technology, Nawabshah, Pakistan.; [4]Department of Information technology, Quaid-e-Awam university of Engineering, Science and Technology, Nawabshah, Pakistan.

Keywords: *face verification, texture analysis, liveness detection, score fusion*

Journal Info:
Submitted:
April 25, 2024
Accepted:
May 19, 2024
Published:
June 15, 2024

Abstract

Currently, most of the biometric recognition systems are based on face verification are susceptible to the spoof attacks. Video replays, printed photographs and 3D mask attacks provoke false acceptance lest some necessary counter-measures are employed. We focus on still face spoof attacks considered as one of the most easily generated attacks and challenging for modern face verification systems. To detect face spoofing, most of existing countermeasures focus on designing discriminative features to analyze the textural properties of facial skin. To improve the texture discriminating properties and get advantages from other texture descriptor, in this paper, a novel Hybrid Texture Descriptor (HTD) is proposed and models the joint performance of face verification and liveness detection by score fusion method, for which the multi-modeling is well recognized. Numbers of experiments are carried out on UPM face spoof and one public domain Replay attack databases as standalone countermeasure in addition to the consolidation with verification system by means of fusion of score. The potential of proposed method demonstrate the out-performance throughout the experiments.

***Correspondence author email address:** sajidaparveen@questedu.pk
DOI: 10.21015/vtse.v12i2.1828

1 Introduction

In spoofing attacks, a fake biometric is used for authentication as a legitimate user. Typically, this happens by introducing a fake sample of biometric to the system that does not actually belongs to the person that presents fake biometric or this can also be defined as that person who claims an identity that is not his own

[1].

Presently spoofing is considered as a more serious type of attack for biometric systems. This is because of the fact that the assailant should not necessarily need skills in programming like for indirect attacks neither it need any exertion to carry on for such attacks[2]. Attacker can easily get biometric trait such as voice, finger prints, face, iris etc to masquerade as someone else. In order to maliciously gain the authentication of a system, the attacker can try to present a mask, photograph, or a video recording, showing the facial image of a legitimate client to the camera. Such type of attacks is known as face spoofing attack. Currently there are a number of companies in the market which are providing security solutions based on face biometric authentication technologies. For instance, Lenovo, Asus and Toshiba Laptops launched in the market with embedded face recognition system with built-in webcams. Moreover various computer vision and biometric based technique can distinguish people without artifacts [3]. But unfortunately all these laptops defeated with more than nothing but simply with the users photographs. Concerning the attacks through facial spoof, the present solution are based on designing discriminative features for texture analysis. In this paper, we continue the quest for robust texture descriptor with more discriminative properties from all the prior work. In this regard, we use the advantages of two texture descriptor i.e Complete Local Ternary Pattern (CLTP) [4] and Dynamic Local Ternary Pattern [5] and proposed a new Hybrid Texture Descriptor (HTD) which over the limitations and increase the performance of face verification system under spoofing attacks. The remainder of this paper is organized as follows. In Section 2, related work is discussed on texture based face liveness detection methods. In Section 3, the proposed methodologies are stated. Experimental results are depicted and the details are discussed in Section 4. Finally, conclusion is made and provided in Section 5.

2 Related Work

For detecting the liveness in face, texture of skin plays very important roll. In order to explore the information from skin texture, numerous LBP and its extended version based texture descriptor have been introduced in the literature and became more popular among the researchers because of its simplicity and efficiency. While, in order to generalize the impact of face liveness detection for face verification system, limited work has been done in this domain. In general, face liveness detection counter-measure is not designated to operate as a stand-alone system [6]. Its purpose is to provide additional guard checks to a biometric system. This additional security layer of an anti-spoofing system increases the robustness of overall biometric system. In order to evaluate and compare the impact of embedded system of liveness detection to a biometrics, it is necessary to calculate the performance of the systems in fusion mode. To identify spoofing attack by combining the result of two separate technique i.e head 3D properties along with the eye blink. In the literature, for joint operation of face verification and face anti-spoofing [7], The two fusion techniques decision and score level were adopted to combine the face verification and anti-spoofing. In order to test the fusion, four rules have been set for fusion strategies: AND, SUM, Logistic Regression (LR) and Polynomial Logistic Regression (PLR).

The performance of the embedded system was reported by the standard HTER and spoof false acceptance rate SFAR that means spoof attacks which passes the system successfully. The reported results shows that fusion reduces the ratio of SFAR form 91.54% for face verification system. SUM fusion rule created the most successful in rejecting spoofing attacks, but at the worst in terms of verification performance. The PLR fusion scheme performed almost perfectly for verification capabilities of the baseline system, and also achieved good safeguard to spoofing attacks. A multi-modal presentation attack detection through PAD has been proposed with score fusion of two weighted level i.e sun and wight product with combination of speech and mouth motion [8]. Various score fusion research is done in other biometric traits and domain such as fingerprint matching and liveness detection has been obtained via UNNS and Slim-ResCNN respectively to test fingerprint from legitimate user[9]. Recently, face anti-spoofing method

based on color texture, machine learning, artificial intelligence and multi-scale assessment deployed for checking and identified various spoof attacks [10–14]. There is still a gape to investigate the best strategy for implementation of face liveness detection with facial biometrics in terms of error rates and flexibility of incorporating.

3 Proposed Methodology

In this work, face liveness detection model is designed to use as a security layer for face verification system to protect from spoof attacks. The overall system's architecture block diagram is represents the combined operational scenario of both model by proposed texture descriptor as a feature extractor in all training and testing phases in Figure 1. Mainly, the system is divided into two models: Face Liveness and another one is face verification model. In order to make a decision either accept or reject, the obtained scores from both models are joined together in fusion strategy method.

3.1 Hybrid Texture Descriptor

Correspondence attempt of hybrid approach is to take advantages from recently proposed texture operators which actually increase the robustness of texture descriptor and overcome the limitations that posses as an individual texture descriptor. Basically in this hybrid approach we utilized two texture operator (i.e DLTP and CLTP) . DLTP is adopted because of its dynamic adoption of threshold value and from CLTP, sign-magnitude transform is adopted to make the feature descriptor more informative in terms of texture for face liveness and verification system. Hybrid Texture Descriptor (HTD) is used as a feature extractor in both face liveness to distinguished between live and spoof face images and face verification system for genuine and imposter attempt. The DLTP texture descriptor is defined as:

$$DLTP = \sum_{p=0}^{p-1} a(z_p - z_c) \times 3^p, \times 3^p, \tag{1}$$

$$a(x) = \begin{cases} 1 \; if & p_i > c + \tau \\ 0 \; if & c - \tau \leq p_i \leq c + \tau \\ -1 \; if & p_i < c - \tau \end{cases} \tag{2}$$

Where z_c is a central pixel and $z_p(p = 0, 1, \ldots p-1)$ is circularly and evenly spaced neighbours. The local difference vector ($DLTP(a) = [a_0, \ldots, a_{p-1}]$) characterizes the image local structure at into three levels. The value of threshold in DLTP is adopted dynamically by using Weber's law which makes it robust. It is seen that DLTP actually uses only the sign component of difference vector and the central gray value is removed. Apparently, this may lead to some incorrect matches. Thus we need to extract the distinct and stable features from $DLTP(a) = [a_0, \ldots, a_{p-1}]$ to robustly recognize the texture patterns for the liveness detector. In this regard, we combined the sign-magnitude transformation with DLTP and decompose the descriptor into two transforms and represent the image with its center gray level. Where $sign(DLTP) = DLTP$, and

$$a(x) = \begin{cases} 1 \; if & p_i > c + \tau' \\ 0 \; if & c - \tau' \leq p_i \leq c + \tau' \\ -1 \; if & p_i < c - \tau' \end{cases} \tag{3}$$

Where τ' is the mean value of the whole image. Furthermore, the original image is represented as its center gray level, expressed as:

$$Center - Gray(DLTP) = \sum_{p=0}^{p-1} a(z_p - z_c) \times 3^p, \tag{4}$$

$$a(x) = \begin{cases} 1 \; if & p_i > c + \tau'' \\ 0 \; if & c - \tau'' \leq p_i \leq c + \tau'' \\ -1 \; if & p_i < c - \tau'' \end{cases} \tag{5}$$

Where τ'' is the average gray level of the whole image. The dimensionality of the DLTP histogram is very large because of 3^p bins. Thus we adopted the split code into positive and negative $Sign(DLTP)$, $Magnitude|DLTP|$ and $Center - Gray(DLTP)$. Finally, the hybrid texture descriptor is expressed as:

$$HTD = Sign(DLTP(a)) + Magnitude|DLTP(a)| + Center - Gray(DLTPbig(a)). \tag{6}$$

The *HTD* descriptor depicts the feature of the facial image by combining $Sign(DLTP)$, $Magnitude|DLTP|$ and $Center - Gray(DLTP)$ operators.

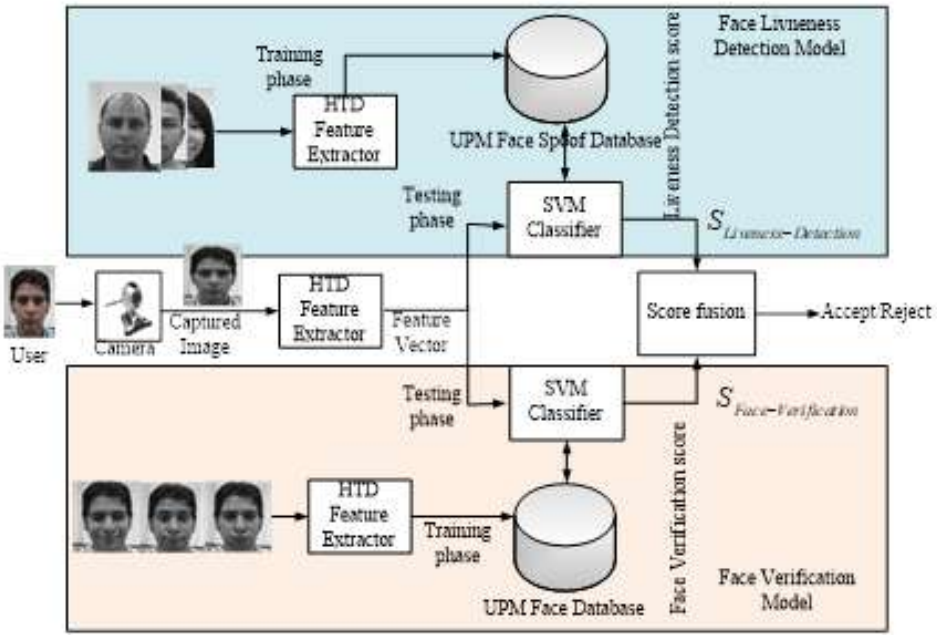

Figure 1. Overall system architecture

3.2 Standalone Face Verification System

During the standalone face verification system (FVS) for each authorized test T, two possibilities are computed: either T is presented by the authorized user \ genuine (x), or it is not authorized user or imposter $(\bar{x})$. Usually the score of the system is the log-likelihood ratio between the probabilities of both possibilities:

$$S_{FVS} = logp(T|x) - logp(T|\bar{x}) \quad (7)$$

In this paper we consider HTD based face verification system and this score would be calculated from the verification model.

3.3 Standalone Face Liveness Detection system

A binary classification method is employed in face liveness detection that separate the spoof attacks from natural zero effort (both genuine and imposter) attempts. Every test T compute two possibilities: either T is an original facial skin (I) or it is not $(\bar{I})$. In this research, the liveness detection is performed using HTD and classified via support vector machines (SVM) with linear kernel.

$$S_{LD} = logp(T|I) - logp(T|\bar{I}) \quad (8)$$

3.4 Score Fusion

Score level fusion is one of most popular method in multi biometrics to combine the results in order to make a decision that is also adopted in this research work. The outputs scores that comes from two modules are combined by a "fusion rule", which produces a final match score that is used to accept or reject the claimed identity. Score fusion aims at combining the output scores from both FV and LD systems. In this approach, the FV system compares positive test possibility $T(x,I)$ against negative test possibility$T(\bar{x},I)$ and the LD system compares positive test possibility $T(x,I) \cup T(\bar{x},I)$ against negative test possibility $\overline{T(x,I)}$. The positive possibility for the joint system is the intersection of the positive test possibilities for both subsystems $T(x,I)$. In the fusion approach, individual maching scores from FV and LD subsystems are combines to generate a single score which is then used for making the final decision. In our case the scores from both modalities are homogeneous (same classification method i.e. SVM).

The $S_{face\_verification}(x,\bar{x})$ and $S_{face\_liveness}(I,\bar{I})$ are the output scores from FV and LD respectively. Both systems FV and LD score is fused parallel, with reference

to the bimodal that is based on face verification and liveness detection. In a verification setting, each user presents his/her face to the respective camera sensor, and claims his/her identity. In each sub system, SVM then separately compares the presented trait with the corresponding template for checking of the claimed identity and liveness. The matching scores for $S_{face\_verification}$ and $S_{face\_liveness}$ are produced by face verification and face liveness detection respectively.Finally, these matching scores are fused through a decision fusion rule $f(S_{face\_liveness}, S_{face\_verification})$. If the fused score S is equal or greater than a predefined threshold S*, then user is accepted as genuine, otherwise it is rejected as spoof and imposter. Figure 22 illustrates the architecture of parallel fusion model of system.

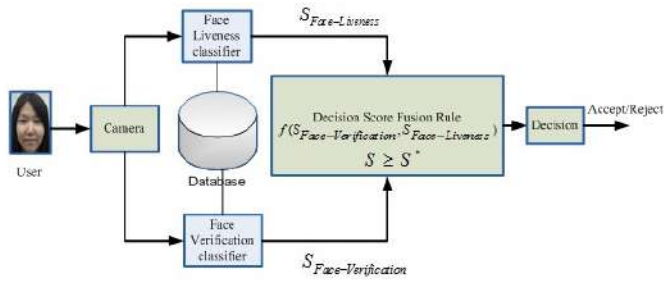

Figure 2. Parallel score fusion modal of face verification and face liveness detection

The sum rule is applied in parallel fusion operation mode which is expressed in equation

$$f(S_{face\_liveness}, S_{face\_verification}) = S_{face\_liveness} + S_{face\_verification} \quad (9)$$

Where, $S_{face\_Verificaiton}$ is the score generated by the face verification classifier and $S_{face\_liveness}$ is the score produced by face liveness detection classifier.

3.5 DATABASES

In this research, the main goal is to evaluate the performance of face verification under the spoof attacks includes verification and spoofability assessment of the system. Therefore, there is a need of a database which satisfies certain criteria. For face biometric verification system, database need to be provide protocols of genuine samples to enroll user in the system. similarly, to enable spoofability assessment, it need to provide face spoofing attacks as well. Currently, the databases from the litrature [15,16,17] mostly used for spoofablity assessment. Meanwhile, they are found to be limited in terms of texture variations. Therefore, for texture analysis there is a need of a databases that should be rich interms of texture based face spoof attacks. there are two different types of database namely self collected UPM and public domain Replay attack database are utilized in this paper for the analysis of face verification under the spoofing attacks.

A UPM Face Spoof Database (UPM-FSD) contained various types of textures for spoofing attacks. the database is consists of 30 subjects and fake faces are recaptured on various forms which include four different types of paper and three different digital display devices: A4, laminated, un-laminated, matt, mobile, laptop and tab screen. Moreover, for evaluating the combined operation of face liveness detection with face verification system, an additional imposter attempts introduced. All images were collected using a high precision camera. This database provides a more realistic and challenging platform for combined operation of face liveness detection and face verification system[18, 19]. Similarly, Replay attack database consists of 50 subjects which includes print, digital photo and video attacks. The diversity of attacks is provided in terms of two kind of support for attacks: hand and fixed along with two conditions: controlled and adverse. Besides spoof attacks, the replay-attack also provides real access samples which are designated for verification purpose. Such an evaluation is not possible for the spoofing attacks in NUAA and CASIA-FASD databases. The training and evaluating protocols were set as licit and spoofed protocol and are utilized to evaluate the performance of face verification model, face liveness detection/ spoofability assessment and joint operation of both models. The details of licit and spoofed protocols are shown in Table 1.

Table 1. Details of database protocols

Database		UPM-FD	Replay Attack
Genuine sample	training	9000	22497
	testing	10000	29791
Spoof attacks	training	15000	69686
	Testing	20000	93,686
Imposter	training	6000	10000
	testing	10000	30000

4 Results and Discussions

The performance evaluation of the proposed texture descriptor and combined operation of face liveness detection with verification detection were carried out using the UPM face spoof and UPM face verification database. The comparison analysis is made with one public domain Replay attack database which also provide the protocols for joint operation. It is worth nothing that for both databases the features extraction and performed evaluation of fusion methods undergo exactly the same procedure in all three experiments.

4.1 Results of standalone Face verification system

In this experiment, the evaluation of standalone face verification is performed by using HTD. The model is trained and test by using two protocols of UPM and Replay attack database: (1) Licit (genuine as positive and imposter as negative samples) and (2) Spoofed (genuine and spoofed of genuine as positive and imposter as negative samples). The obtained results on of face verification on both databases are shown in Table 2, whereas Figure 3 and Figure 4 illustrate ROC plots for both databases. Firstly, these results clearly shown that proposed HTD is more robust for face verification. Secondly, the results on both Licit and spoofed protocols does not shows much variation in FAR which exhibit that without countermeasure of liveness detection, spoof attacks easily deceived the system around 90%.

Database	protocol	HTER	FAR	Accuracy
UPM-FD	Licit	4.19	4.607	94.98
	Spoofed	4.62	4.89	98.32
Replay-Attack	Licit	5.2	4.4	90.2
	Spoofed	4.7	4.2	93.5

Table 2. Performance of standalone face verification system %

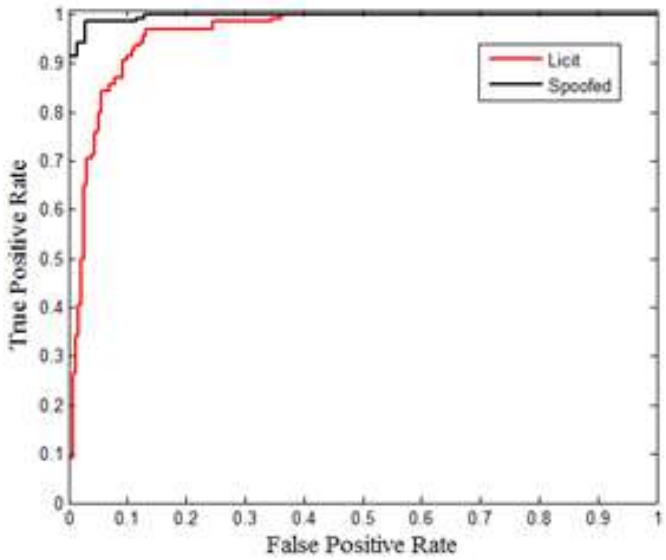

Figure 3. Roc curve of face verification on licit and spoofed protocols on UPM FD

4.2 Results of standalone Face Liveness detection system

To evaluate the robustness of the HTD based face liveness detection system against the face spoof attacks; in this experiment spoof protocol is utilized in which the system is trained with genuine samples as positive and different types of face spoof attacks as negative samples. The results are obtained and represented in Table 3 and the performance of the system is depicted in Figure 5 in terms of Receiver Operating Characteristic (ROC). Clearly, the HTD texture descriptor is robust to detect all kind of face spoof attacks which alterna-

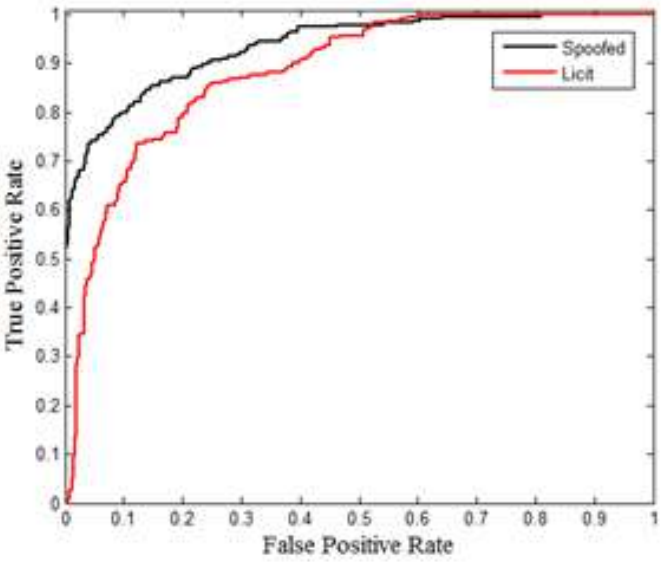

Figure 4. Roc curve of face verification on licit and spoofed protocols on Replay Attack

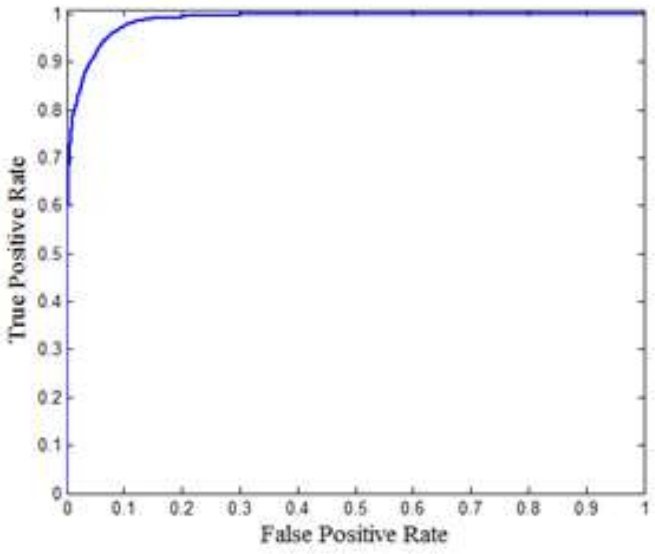

Figure 5. Roc curve of Face liveness detection on UPM-FSD

Database	protocol	HTER	FAR	Accuracy
UPM-FD	spoofed	2.34	0.86	97.8
Replay-Attack	spoofed	3.32	1.67	96.12

Table 3. Performance of Face Liveness Detection %

Database	HTER	FAR	Accuracy
UPM-FD	2.423	1.062	97.57
Replay-Attack	4.96	2.38	91.4

Table 4. Performance of score fusion system of FV and FLD %

tively increase the security for face verification system. In contrast, as illustrated in Figure 6, Reply attacks little bit harder to detect. The reason behind this is that HTD is robust for texture that why face spoof attacks of UPM are easily detected while Reply attack exhibit variability in terms of illumination.

4.3 Parallel score fusion method

In order to investigate the performance of FVS with the joint operation of FLD, parallel score fusion method is implemented. The empirical analysis of parallel score fusion method on UPM and Replay attack databases are presented in Table 4. To compare parallel fusion method using their vulnerability to spoofing as a criteria, look at the FAR and ROC curve in Figure 7, it is notice that there are lower value of FAR i.e. 1.062% and 2.38% with performance of 97.57% and 91.4 of UPM and Replay attack DB respectively. Thus, achieved result with parallel score fused model shows that face liveness detection successfully protect the face verification against vulnerability of face spoof attacks by reducing the acceptance of spoof attacks as genuine (FAR). The result is also plotted in Figure 8, which shows that ROC curve of parallel score fusion of FLD with FVS performed well by reducing the acceptance ratio of face spoof attacks FAR up to 87.92%. Since the positives scores of the FV and FLD systems are same, so it does not affect the FRR in both of the individual systems.

Additionally, for well-formatted manuscripts, we recommend that you let LaTeX handle figure/table placement for you as much as possible, so please avoid specifying strenuous float instructions like '[h!]'

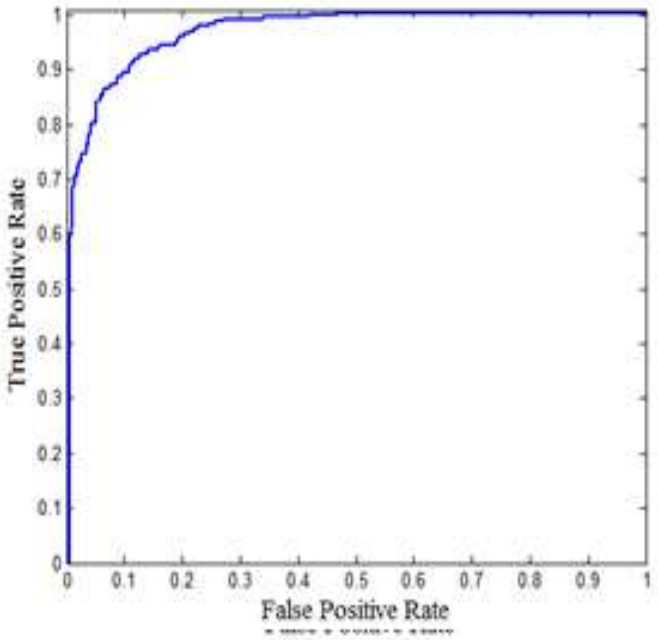

Figure 6. Roc curve of Face liveness detection on Replay Attack

and '[H]' as much as possible.

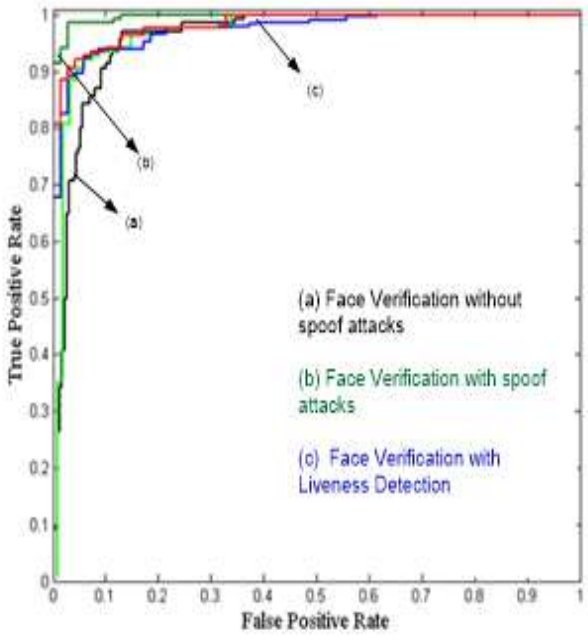

Figure 7. ROC curve of score fusion of FV with FLD on UPM DB

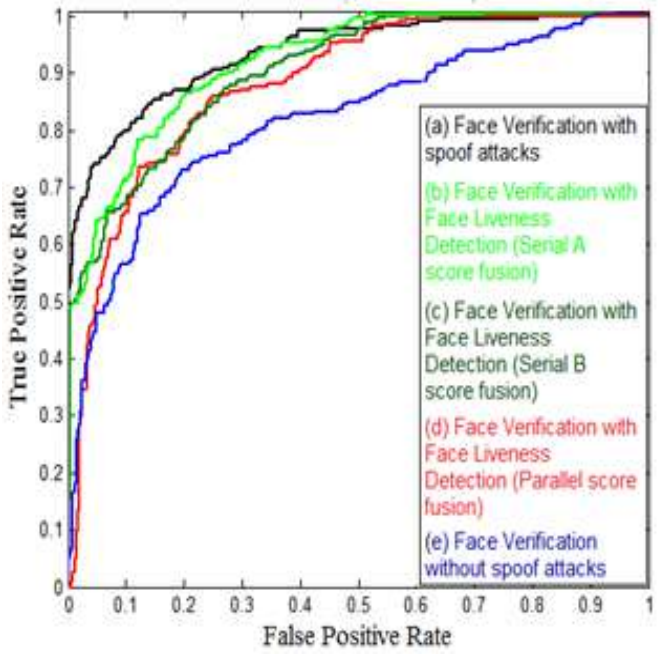

Figure 8. ROC curve of score fusion of FV with FLD on Replay attacks

5 conclusions

To look forward for the best texture descriptor in face liveness detection, the expectation is to find only one approach that has capabilities to discriminate the mediums of spoof attacks from the genuine skin. In this paper, the novel texture descriptor named as Hybrid Texture Descriptor (HTD) was proposed. A comprehensive evaluation of the performance in face liveness detection was performed on self-collected UPM-FSDB and one publicly available Replay attack database. UPM-FSDB basically rich in texture based face spoof attacks while Replay attack database have diversities in terms of illumination conditions. From the obtained results, robustness of proposed texture descriptor is concluded in every aspect on both databases. Technically, face liveness detection is designed to protect the authentication systems from spoofing attacks. In order to evaluate the performance of face liveness detection as a security layer to the face verification system, parallel score fusion methods is applied. Thus, for evaluating the combined operation of both models, three operational modes have been tested: Face verification without spoof attacks, face

verification with spoof attacks , face verification with face liveness detection in parallel score fusion method. The performance of tested protocols was portrayed in ROC graphs and results are reported in FAR, HTER and accuracy in percentages. The mutual operation of systems proved that fusion strategies protected the system against face spoof attacks by reducing FAR from 89.89% up to 0.9524%. This prominent margin shows the worth of the HTD based face liveness detection system in face verification.

Author Contributions

Sajida Parveen: Writing original draft preparation **Sharifah Mumtazah**: supervision **Nadeem Naeem**: Data collection **Imtiaz Ali Halepoto**: Editing **Shamshad Lakho**: Software, Validation.

Compliance with Ethical Standards

It is declare that all authors don't have any conflict of interest. It is also declare that this article does not contain any studies with human participants or animals performed by any of the authors. Furthermore, informed consent was obtained from all individual participants included in the study.

References

[1] Z. Wu, Y. Cheng, S. Zhang, X. Ji, and W. Xu, "Uniid: Spoofing face authentication system by universal identity," in *Proceedings of Network and Distributed System Security Symposium (NDSS)*, 2024.

[2] M. Sebastien, M. Nixon, and S. Li, *Handbook of biometric anti-spoofing: trusted biometrics under spoofing attacks*. 2014.

[3] S. Sharma, I. Dhall, S. Nayak, and P. Chatterjee, "Reliable biometric authentication with privacy protection," in *Advances in Communication, Devices and Networking: Proceedings of ICCDN 2021*, pp. 233–249, Springer Nature Singapore, 2022.

[4] K. Alalayah, R. Irshad, T. Rassem, and B. Mohammed, "A new fast local laplacian completed local ternary count (fll-cltc) for facial image classification," *IEEE Access*, vol. 8, pp. 98244–98254, 2020.

[5] M. Ibrahim, M. Efat, H. Shamol, S. Khaled, M. Shoyaib, and M. Abdullah-Al-Wadud, "Dynamic local ternary pattern for face recognition and verification," in *International Conference on Computer Engineering and Applica-tions*, vol. 1012, 2014.

[6] I. Chingovska, A. Anjos, and S. Marcel, "Anti-spoofing in action: joint operation with a verification system," in *Proceedings of the IEEE conference on computer vision and pattern recognition workshops*, pp. 98–104, 2013.

[7] L. Li, Z. Yao, S. Gao, H. Han, and Z. Xia, "Face anti-spoofing via jointly modeling local texture and constructed depth," *Engineering Applications of Artificial Intelligence*, vol. 133, p. 108345, 2024.

[8] C. Chou, "Presentation attack detection based on score level fusion and challenge-response technique," *The Journal of Supercomputing*, vol. 77, no. 5, pp. 4681–4697, 2021.

[9] Y. Zhang, C. Gao, S. Pan, Z. Li, Y. Xu, and H. Qiu, "A score-level fusion of fingerprint matching with fingerprint liveness detection," *IEEE Access*, vol. 8, pp. 183391–183400, 2020.

[10] Y. Moon, I. Ryoo, and S. Kim, "Face antispoofing method using color texture segmentation on fpga," *Security and Communication Networks*, vol. 2021, no. 1, p. 9939232, 2021.

[11] Z. Yu, Y. Qin, X. Li, C. Zhao, Z. Lei, and G. Zhao, "Deep learning for face anti-spoofing: A survey," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 45, no. 5, pp. 5609–5631, 2022.

[12] M. Rusia and D. Singh, "A color-texture-based deep neural network technique to detect face spoofing attacks," *Cybernetics and Information Technologies*, vol. 22, no. 3, pp. 127–145, 2022.

[13] P. Jaswanth and M. Ramprasad, "Deep learning based intelligent system for robust face spoofing detection using texture feature measurement," *Measurement: Sensors*, vol. 29, p. 100868, 2023.

[14] R. Raghavendra and R. Kunte, "A novel feature descriptor for face anti-spoofing using texture based method," *Cybernetics and Information Technologies*, vol. 20, no. 3, pp. 159–176, 2020.

[15] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," in *Computer Vision–ECCV 2010: 11th European Conference on Computer Vision, Heraklion, Crete, Greece, September 5-11, 2010, Proceedings, Part VI 11*, pp. 504–517, Springer Berlin Heidelberg, 2010.

[16] A. Anjos, M. Chakka, and S. Marcel, "Motion-based counter-measures to photo attacks in face recognition," *IET Biometrics*, vol. 3, no. 3, pp. 147–158, 2014.

[17] S. Parveen, S. Ahmad, M. Hanafi, and W. Adnan, "The design and compilation of a facial spoof database on various textures," in *2014 4th International Conference on Artificial Intelligence with Applications in Engineering and Technology*, pp. 182–186, IEEE, 2014.

[18] S. Praveen, S. Rehman, N. Naeem, J. Devi, and M. Ahmed, "Improved complete dynamic local ternary pattern texture descriptor for face spoof attacks," *International Journal of Computer Science and Network Security*, vol. 18, no. 12, pp. 102–110, 2018.