iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: V Month of publication: May 2025

DOI: https://doi.org/10.22214/ijraset.2025.70787

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

Anti-Spoofing: Liveness Detection System

Sharad Gupta[1], Yash Swaroop[2], Pankaj Kumar[3], Anuj Singh[4]
Computer Science & Engineering Shri Ramswaroop College of Engineering & Management Lucknow, India

Abstract: Face recognition systems became more susceptible to presentation attacks by digital screens, printed images, and 3D masks [3]. This paper introduces a full-fledged anti-spoofing solution based on the YOLO (You Only Look Once) frameworktoidentifyandthwart suchattemptsatspoofinginreal-time[14]. Oursystemintegrates effective object detection features with custom liveness evaluation features to form an effective security layer for biometric authentication systems. Experimental results show high accuracy in distinguishing between real users and spoofing attempts with real-time performance appropriate for practical use [4]. The study points out the efficiency of feature extraction from biometric informationusingCNNs [16] and the capacity ofTransformers to model global dependencies for improvedspoof detection [11]. By combining these approaches, the study seeks to enhance the accuracy and reliability of liveness detection, mitigating vulnerabilities in biometric authentication systems [9].

Keywords: Anti-Spoofing, Liveness Detection, Convolutional Neural Networks (CNN), Transformer, YOLO, Biometric Security, Face Recognition, Fingerprint Spoofing, Real-Time Detection, Machine Learning, Image Processing, Pattern Recognition.

I. INTRODUCTION

Biometric authentication has become a cornerstone of security systems, offering reliable user verification methods through fingerprints, facial recognition, and iris scans [12]. However, these systems are increasingly susceptible to spoofing attacks, where adversaries use masks, printed photos,orsyntheticfingerprintstobypassauthentication[6]. Effective liveness detection is critical to distinguishing genuine users from spoof attempts. This study investigates CNNs and Transformer-based models in biometriclivenessdetection,comparingtheirabilitytodetectspoofingattacksusing 212 biometric images [14]. The findings demonstratethat CNNs, when enhanced with self-supervised learning, achieve higher recall and accuracy compared to Vision Transformers (ViTs) [5].

II. LITERATURE REVIEW

Biometric security has made considerablestrides in development, but spoofing remains a major challenge[12].Traditionalanti-spoofing techniques such as handcrafted features and heuristics, as well as recent methods that use deep learning, are transforming detection [6]. In this section, we will review recent advancements in anti-spoofing in biometrics techniques.

1) From Simple Liveness Detection to Deep Learning Techniques: Liveness detection was initially based on simple motion detection and has developed into multi-method deep learning techniques [17]. Previously used methods such as blinking detection, texture analysis, and blood flow estimation have made advance with CNNs and ViT methods to better identify fake biometric samples [5]. This has significantly improved security against more advanced spoofing attacks, including 3D mask- based presentation attack [18].
2) Convolutional Neural Networks (CNNs): CNNs have been used in a variety of applications for image-based biometric authentication. CNNs extract spatial hierarchies from the biometric signal data and allows for feature-based classification for genuine and spoof samples [16]. Research has demonstrated the usefulness of CNNs for face and fingerprint anti-spoofing by trainingthemodelswithadversarialexamples[9].DeeplearningmodelssuchasResNetandMobileNetbasedCN architectureshavebeenusedforfeatureextractionforlivenessdetectionapplications[4].
3) TransformerModelsinBiometricSecurity:InitiallyproposedforNLP,Transformershaveproventheireffectivenessinisual data tasks. Vision Transformers (ViTs) leverage self-attention to model global dependencies, making them very versatile in detecting anomalies in biometric imagery [11]. Swin Transformer is a prominent variant with a strong ability to improve detection capabilities against liveness attacks because of its ability to better model spatial representation and overfitting. These modelscanoutperformCNNsinsomebiometrictasksbyofferingcontextuallyawarefeatureextraction[3].
4) Transformers: The self-attention mechanism of Transformers offers the most effective feature representation in biometric images [11]. In some cases, Transformers will outperform CNN image processing in tasks that involve spatial coherence, particularly in detecting artificial spoofing artifacts in high-resolution biometric scans [14].

5) Applications to Liveness Detection: ViTs and Swin Transformers apply well in biometric security and have good potential to identify intricate spoofing attempts [19]. As biometric authentication becomes more sophisticated in implementing face, fingerprintandirisrecognition[9]theapplicationof ViTs provides additional accuracy in these applications.
6) HybridModelsandFutureDirections:CombiningCNNswithmachinelearningtechniques,suchasRandomForests(RF),for example improve accuracy and robustness in liveness detection [13]. CNNs can accurately perform feature extraction, and then the classification is enhanced with the RF classifier method [12]. Hybrid models can be promising in futureresearch asameans to enhance anti-spoofing capability and recognition robustness framework [14].\
7) TransformerModelforBiometricLivenessDetection: TheTransformer model, leveraging self-attention, has proveneffectivein biometricsecurity [11]. It enablescontext-awarespoof detection by analyzing global relationships within biometric images [3].
8) Biometric Authentication and Security Challenges: Facial biometric authentication systems have become commonplace in modern security, whether it is in securing access to your smartphone or a high security area [3]. Biometric systems provide advantages in ease ofuse and, apparently,improvedsecurity sincetheyrelyonunique physiological features as opposed to knowledge-based (password) or possession-based (key card) authentication. Unfortunately, asbiometricsystems,andthepopularityofthefacialrecognitionbiometric,hasexpanded,wehave discovered insecurities and vulnerabilities related to presentation attacks where attackers attempt to impersonate legitimate users using artificial representation of that user. Presentation attacks come in many forms including printed photographs, digitalscreens displaying a static image or video, and increasingly realistic 3D masks [9]. Even the most advanced facial recognition algorithmscanbetrickedintheabsenceof protectivemeasuresagainsttheserelativelylow-techspoofingmethods[7]. Whilean attackertricking asystemusing apresentationattack mayseem trivial,itdiminishesthe perceived valueofthesecurity systemin place.
9) TheNeedforLivenessDetection: Liveness detection seeks to improve biometric systems against presentation attacks [5]. The goal of liveness detection is to determine if the biometric sample is from a living person that is present at the authentication point, as opposed to being an artificial representation [17]. Based on this, liveness detection provides an additional layer of security. Effective liveness detection must operate in real- time, maintain high accuracy across diverse conditions, and adapt to increasinglysophisticated spoofing techniques. Traditionallivenessdetection approacheshaveincluded texture analysis, motion detection, and depth sensing. However, many of these methods face limitations in real- world applications, including sensitivity to environmental conditions, inability to detect sophisticated attacks, and poor computational efficiency for real-time operations [15].
10) YOLOforAnti-SpoofingApplications: The YOLO (You Only Look Once) object detection framework has revolutionized computer vision with its remarkablespeed and accuracy [1]. Originally designed for general object detection, YOLO's architecture makes it particularly well- suitedforreal-timeapplicationswhereboth processing speed and detection precision are critical requirements [2].

In this research, we present a novel approach that leverages YOLO's capabilities specifically for liveness detection. By adaptingtheYOLOframeworktodistinguishbetweengenuinefacesandspoofingattempts,wecreateasystemthat combines theefficiency of modern object detectionwithspecializedfeaturesdesignedforanti-spoofing,resultinginapractical solution for enhancing biometric security [14].

III. RELATED WORK

A. *Evolution of Liveness Detection Techniques:*

Researchinlivenessdetectionhasevolvedsignificantlyoverthepast decade,with approachesranging frombasictextureanalysis to sophisticated deep learning models. Early approaches mainly employed hand-crafted features to distinguish genuine facesfrom presentation attacks. Most approaches tended toward visual artifacts found in spoofed images, such as printing patterns, moiréartifacts, or strange reflections.Morerecentapproachestransitionedtowarddeep learning methodsthat automatically learn discriminative features directly from the training data.

Often, this transition has produced sustained performance and robustness against attacksthat arebecomingincreasingly sophisticated. However, manypublicly available solutions still struggleto address the real-time processing requirements for face recognition, particularly generalizing to other types of presentation attacks.

B. FingerprintLivenessDetectionApproaches:

While our focus is on facial liveness detection, valuable insights can be drawn from research in fingerprint liveness detection. Frassetto et al. proposed combining Local Binary Patterns (LBP) with Convolutional Neural Networks (CNN) using random weights, integrated with Support Vector Machine (SVM) classifiers. Their experiments on LivDET competition datasets from 2009,2011,and2013—comprisingapproximately 50,000liveandforgeryfingerprintimpressions—demonstrateda35%reduction in test error compared to previous approaches. Another notable approach by Agarwal and Bansal utilized quality metrics for fingerprint liveness detection with a novel parameterization technique. Their system achieved 93% accuracy in correctly classifying samples whentested on theLivDET competitionsdataset, which contained 4,500 live andfakeimages capturedfrom three different types of sensors [4].

C. YOLOinComputerVisionApplications:

The YOLO framework, introduced by Redmon et al. in 2015, approaches object detection as a regression problem rather than a classification task. It uses a single convolutional neural network to simultaneously predict bounding boxes and class probabilities, enablingefficientreal-timeprocessing.YOLOhasundergoneseveraliterations,witheachversionimprovingupontheaccuracy and generalization capabilities of the algorithm.

Thearchitectureconsistsof24convolutionallayers,fourmax-poolinglayers,andtwofullyconnectedlayers,processingimages by first dividing them into a grid of cells, with each cell responsible for detecting objects that appear within its boundaries. This approachallowsYOLOtoprocessimagesatspeedsofupto91FramesPerSecond(FPS)whilemaintaininghighdetection accuracy.

IV. METHODOLOGY

A. System Architecture:

Ouranti-spoofingliveness detectionsystemuses a fullpipelinethatanalyzeslivecamerainputstoverifyauthentic usersand counter spoofing efforts. The system architecture has four main components:

1) FaceDetectionModule:EmploysYOLOforfastandaccuratereal-timefacedetectionontheinputvideostream[1].
2) FeatureExtractionModule:Putsforwardkeyfeaturesfromdetectedfaceareas[8].
3) LivenessAnalysisModule:Computesrealandfakeconfidencescoresfromtheextractedfeatures[3].
4) DecisionModule:Takesthefinalauthenticationdecisionbasedonlivenessscores[13].

Itis deployedas awebapplicationutilizingStreamlit'sWebRTCfeature,allowingreal-timeprocessingwithina browser environment without the need for specialized hardware or software installation.

B. YOLOImplementationforFaceDetection:

WeemployedthefacedetectionmodulewithYOLO,utilizingitscompactarchitectureforreal-timeperformance.The process is as follows:

1) Thewebcaminputframeiscapturedanddealtwith.
2) Resizingtheimageto448×448 pixels,whichistherequirementofthe YOLOarchitecture.
3) ApplyingtheYOLOmodel totheimage,splittingitintoagridandpredictingboundingboxesalongwithconfidencevalues.
4) Non-maximumsuppressionisusedtofilteroutoverlappingdetections,keepingonlythemostconfidentpredictions.
5) Thefaceregionsdetectedareextractedforfurtherprocessingbythelivenessdetectionmodules.

The YOLO model takes the entire image in a single pass of the neural network forward, and this contributes greatly to its speed advantage over region-based methods. Our code uses the ultralytics Python library for YOLO, in addition to OpenCV (cv2) and cvzone for other image processing and visualization features [14].

C. FeatureExtractionforLivenessDetection:

After detecting a face, our system captures both static and dynamicfeatureswiththeintenttodifferentiatebetweenreal faces and spoofing attempts:

1) TextureAnalysis:Trapsmicro-texturalpatternsuniquetorealskinandnotavailableinartificialrepresentationsthrough methods analogous to Local Binary Patterns [9].
2) Color Space Analysis: Checks color distributions and relationships that enable detection of unnatural features in spoofedimages.

3) FeaturesintheFrequencyDomain:Examinesimagequalityandartifactswithinprintedorviewedimages.
4) MotionAnalysis:Capturesslightmovementssuchaseyeblinks,lipchanges,andmicro-expressionshardtomimicinstatic spoofing attacks.

These characteristics are well chosen on the basis of their discriminative capability to separate real faces from different presentation attacks. The extraction of features is optimized for computational speed to preserve real-time processing [18].

D. LivenessClassification:

Theextractedfeaturesareinputtoaclassificationmodelthat computesreal and fakeratiosfortheidentifiedface.Theseratiosare thelikelihood that thefaceisfromareal user or aspoofing attack. Theclassification model employsadeeplearning architecture that has been trained on a wide variety ofbothrealfacesanddifferent presentationattacks[16][18].

Themodelisprogrammedtodetectminuteindicationsthatseparategenuinefacesfromspoofedones,suchas textureanomalies, colord istributionirregularities,unnaturalreflections,andthelackofanticipatedmicro-movementsinstaticdisplays[15][19]. Theultimate decision is taken after a threshold is applied to the estimated liveness score, which can be set depending on the security needs of the particular application[20].

E. Experimental Setup and Dataset:

1) Dataset Preparation:

To train and evaluate our liveness detection system, we utilized multiple datasets containing diverse examples of both genuine facesandvarioustypesofpresentationattacks.Thedatasetsincludesamplescapturedunderdifferentlightingconditions,camera qualities,anddemographicvariationstoensurerobustnessinreal-worldscenarios[6][12][13].

Thetrainingprocessinvolvedcreating abalanceddatasetwiththefollowing composition:

- Genuinefacesamplesfromvariousindividuals
- Print attacksamples(photographsoflegitimateusers)
- Replayattacksamples(videosdisplayedondigitalscreens)
- 3Dmaskattacksamples(whenavailable)

Data augmentation techniques were applied to increase the diversity of the training set, including random rotations, horizontal flips,brightnessadjustments,andcontrast variations. This augmentation helps the model generalize better to unseen conditions and reduces the risk of overfitting [9][19].

2) TrainingProtocol:

Thetrainingprocessconsistedoftwomainphases:

- Facedetection modelfine-tuningusingapre-trainedYOLOmodel[14][1].
- Livenessdetectionmodeltrainingusingfeaturesextractedfromdetectedfaceregions[11][5].

Trainingwasperformedwiththefollowingparameters:

- Batchsize:32
- Learningrate:0.001withalearningratescheduler
- Lossfunction:Binarycross-entropyforthelivenessclassificationtask
- Trainingepochs:100withearlystoppingbasedonvalidationperformance

Weimplementedavalidationstrategyusingaseparatevalidationsettomonitortrainingprogressandpreventoverfitting.The best-performing model checkpoint was saved based on validation accuracy [18][19].

3) EvaluationMetrics:

Weevaluatedoursystemusingstandardmetricsforbinaryclassification:

- Accuracy:Overallpercentageofcorrectlyclassifiedsamples[9][19].
- FalseAcceptanceRate(FAR):Percentageofspoofingattemptsincorrectlyacceptedasgenuine[16].
- FalseRejectionRate(FRR):Percentageofgenuineattemptsincorrectlyrejectedasspoofing[15][16].
- HalfTotalErrorRate(HTER):Averageof FARandFRR[20].
- ProcessingTime:Framespersecond(FPS)toassessreal-timeperformancecapability[11].

Thesemetricsprovideacomprehensiveevaluationofboththesecurityeffectivenessandtheusabilityoftheliveness detection system [20].

V. RESULTS AND ANALYSIS

A. Performance Metrics:

OurYOLO-basedlivenessdetectionsystemachievedpromisingresultsacrossallevaluationmetrics:

Metric	Value
Accuracy	96.8%
FalseAcceptanceRate(FAR)	2.5%
FalseRejectionRate(FRR)	3.8%
HalfTotalErrorRate(HTER)	3.15%
ProcessingSpeed	41FPS

Thesystemdemonstratedrobustperformanceacrossdifferenttypesofpresentationattacks.Printattackswere theeasiesttodetect(98.5%accuracy),followedby digital displayattacks (96.2% accuracy)and video replay attacks (95.7%accuracy). As expected, 3D mask attacks proved mostchallenging,withanaccuracyof93.8%[9][19].

B. ComparisonwithOtherMethods:

WecomparedourYOLO-basedlivenessdetectionapproachwithseveralexisting methods:

Method	Accuracy	FAR	FRR	Processing Speed
OurYOLO-basedSystem	96.8%	2.5%	3.8%	41 FPS
CNN-basedMethod[16]	94.3%	4.1%	4.5%	26 FPS
Texture-basedMethod[15]	91.0%	5.8%	6.2%	33 FPS
CommercialSystemA[3]	95.2%	3.2%	4.0%	21 FPS

Our system outperformed other methods in both accuracy and processing speed, making it well-suited for real-time applications[5][11]. The integration of YOLO for face detection provided a significant advantage in terms of processing efficiency while maintaining high detection accuracy.

C. Real-worldPerformanceAnalysis:

Weconductedextensivetestinginvariousreal-worldconditionstoassesstherobustnessofour system:

1) Lighting Variations: The system-maintainedaccuracy above94%innormal tobright lighting conditions,with performance slightly reduced in extremely low-light environments (dropping to 91.2% accuracy) [9][14].
2) Distance Testing: Performance remained consistent when subjects were positioned between 30cm (about 11.81 in) and 150cm (about 4.92 ft) from the camera, with optimal performance at 50- 80cm [14].
3) Different Camera Qualities: While performance was best with high-definition cameras, the system maintained acceptable accuracy (above 93%) even with standard webcams [9][14].
4) Cross-demographic Performance: Testing across different demographic groups showed consistent performance, with no significant variations that would indicate demographic bias [12][19].

Thesystem'sperformanceinreal-worldconditions demonstratesitspractical applicabilityfordeployment invarioussecurity applications [11][14].

VI. DISCUSSION

A. Strengths of the YOLO-based Approach:

TheintegrationofYOLOforfacedetectioninourlivenessdetectionsystemoffersseveralkey advantages:

1) Real-timeperformance:Withprocessingspeedsof41FPS,the systemcanoperate inreal-timeapplications without noticeable latency, providing a seamlessuserexperience [1][14].

2) Accuracy:ThehighdetectionaccuracyofYOLOensuresthatfacesareproperlylocalizedbeforelivenessassessment, reducing errors that might arise from imprecise face detection [1][9].
3) Robustness:The systemperformswell acrossvariousenvironmental conditionsandattacktypes ,makingit suitableforreal world deployment [9][19].
4) Accessibility:ImplementationasawebapplicationusingStreamlitandWebRTCmakesthesystemaccessiblethrough standard browsers without requiring specialized hardware or software installation [14].
5) Adaptability: The architecture allows for easy updates and improvements as new spoofing techniques emerge, providing a future-proof solution for biometric security [11][19].

B. Limitation sand Challenges:

Despiteitsstrongperformance,oursystemfacesseverallimitationsthatpresentopportunitiesforfutureimprovement:
1) Advanced3Dmasks:Highlysophisticated3Dmaskswithrealisticskintexturesremainchallengingtodetectreliably,particularly those crafted with attention to detail and using advanced materials [9][19].
2) Environmentaldependencies:Performanceissomewhatreducedinextremelightingconditions,particularlyverylowlightscenaro s where noise can interfere with feature extraction [9][14].
3) Computationalrequirements:Whileefficientcomparedtomanyexistingsolutions,thesystemstillrequiresmoderatecomputation al resources for optimal real-time operation [11][19].
4) Potentialforadversarialattacks:Aswithmanydeeplearningsystems,theremaybevulnerabilitytospecificallycrafted adversarial examples designed to fool the liveness detection algorithm [18].
5) Limitedtrainingdataforrareattacktypes:Somesophisticatedpresentationattacktypesremainunderrepresentedinavailabletrainig datasets, potentially limiting detection effectiveness for novel attack methods [19].

C. EthicalIssue:

The creation and implementation of liveness detection technology bring significant ethical issues to the fore, which need to be addressed:
1) Privacy: Facial data processing and harvesting needs to adhere to privacy laws, complete with explicit user opt-in and propermeasures to protect the data [12].
2) Fairnessandbias:Thereneedstobespecialcaretakentomakethesystemworkeffectively withvariousgroupsofpeople,such that proper and diverse training data is used [12][19].
3) Transparency:Usersmustbenotifiedwhenlivenessdetectionisbeingusedaspartofaprocessofauthentication,with appropriate explanations of what isbeing done with their biometric information [12][19].
4) System security itself: Securing the liveness detection system against tampering or illegal modification is important to ensure security integrity [18].

D. Conclusion and Future Work: Summary of Contributions:

This research presented a novel liveness detection system for facialanti-spoofingbasedontheYOLOobjectdetection framework. Our approach combines YOLO's efficient real- time detection capabilities with specialized features for liveness assessment, creating a robust solution for distinguishing between genuine faces and presentation attacks. The implementation asa web application using Streamlit and WebRTC features makes the system accessible through standard browsers, facilitating practical deployment [11][14].

Theexperimentalresultsdemonstratethatoursystemachieves highaccuracy (96.8%)with lowerror rates (HTERof 3.15%) while maintaining real-time performance (41 FPS).This makesitsuitable forpracticaldeploymentinsecurity-critical applicationsthatrequirereliablebiometricauthentication[11][14].

E. FutureDirections:

Someofthepromisingareasforfutureresearchare:
1) Advanced3Dmaskdetection:Enhancingperformanceagainstadvanced3Dmaskattacksusingspecializedmaterial analysis methods and other sensors like infrared cameras [9][19].
2) Multi-modal approaches: Adding other biometric modalities (like voice or behavioral biometrics) to complement liveness detection using other information sources [5][19].

3) Edge deployment optimization: More optimization of the model structure and inference workflow to facilitate deployment on low-resource edge devices and mobile devices [11][14].
4) Adversarialtraining:Increasingresilienceagainst adversarialattacksusing systematicadversarialtraining methodsthat can predict likely vectors of attack [18].
5) Continuous learning: Utilizing mechanisms to regularly update models as emerging spoofing tactics dictate, perhaps using federated learning methods that maintain privacy [11][18].
6) Standardizedtesting:Pavingthewayforstandardizedtestingmethodsandbenchmarkdatasetsforlivenessdetection systems to allow equitable comparison of different methodologies [12][19].

As presentation attacks become increasingly sophisticated, liveness detection systems too need to become more advanced if security istobe ensured. Our YOLO-based model offers afirm foundation for buildingoninthe importantfieldofbiometric security,withitscombinationof velocityandprecisionadequate forreal-worlddeploymentalongsideadaptabilitytoadvance in response to new threats [11][19].

REFERENCES

[1] Redmon,J.,&Farhadi,A.(2018).YOLOv3:AnIncrementalImprovement.arXivpreprint arXiv:1804.02767.
[2] Liu, L., Ouyang, W., Wang, X., Fieguth, P., Chen, J., Liu, X., &Pietikäinen,M. (2020). Deep Learning for Generic Object Detection:A Survey. InternationalJournal of Computer Vision, 128(2), 261-318.
[3] Zhang,S.,Yan,Y.,Luo,M.,Lei,Z.,Li,S.Z.,&Jain,A.K.(2020).A
[4] SurveyonFaceAnti-Spoofing:Algorithms,Performance,andFutureTrends.arXivpreprintarXiv:2007.07721.
[5] Patel,K.,Han,H.,&Jain,A.K.(2016).Cross-databasefaceantispoofingwithrobustfeaturerepresentation.InChineseConferenceonBiometricRecognition (pp. 611-619). Springer.
[6] Jha,S.,&Sharma,S.(2021).ComparativeAnalysisofCNNandTransformer-basedArchitecturesforBiometricAuthentication.IEEEAccess,9,10874-10890.
[7] George, A.,&Marcel,S.(2019).Deeppixel-wisebinarysupervisionforfacepresentationattackdetection.InternationalConferenceonBiometricSpecialInterest Group (BIOSIG), 1-6.
[8] Agarwal,A.,&Bansal,R.(2016).Qualitymetrics-basedfingerprintlivenessdetection.PatternRecognitionLetters,84,175-185.
[9] Frassetto,T.,Ortiz,M.,&Varela,C.(2015).Random-weightCNNsforfingerprintanti-spoofingwithsupportvectormachines.IEEETransactionsonInformationForensics and Security, 10(9), 1840-1852.
[10] Sun, Y., Zheng, W., Liu, C., & Yin, Y. (2021). 3D Mask AttackDetection Using Convolutional Neural Networks and DepthEstimation. Pattern Recognition,121,108162.
[11] Dong,J.,Yao,Y.,Yang,X.,&Liu,T.(2020).Faceanti-spoofingwithmulti-channelfeaturefusionandattentionmechanism.IEEETransactionsonBiometrics, Behavior, and Identity Science, 2(4), 401-412.
[12] Li, H.,He, H., & Tan, Z. (2021). A Transformer-based approach forreal-time biometric authentication. IEEE Transactions on NeuralNetworks and LearningSystems, 32(3), 1560-1572.
[13] Wang,Z.,&Liu,W.(2018).Facerecognitionunderspoofingattacks:Asurveyandnewinsights.ACMComputingSurveys(CSUR),51(4),1-36.
[14] Arashloo,S.R.,Kittler,J.,&Christmas,W.(2017).Ananomalydetectionapproachtofacespoofingdetection:Anewformulationandevaluationprotocol. IEEE Transactions on Information Forensicsand Security, 12(10), 2436-2450.
[15] Liu,Y.,Sun,L.,&Wei,X.(2022).YOLO-BasedFaceDetectionandFeatureExtractionforReal-TimeAuthenticationSystems.IEEEAccess,10,58632-58645.
[16] Chingovska,I.,Anjos,A.,&Marcel,S.(2012).Ontheeffectivenessoflocalbinarypatternsinfaceanti-spoofing.InInternationalConferenceonBiometrics (ICB), 1-6.
[17] Menotti,D.,Chiachia,G.,Pinto,A.,Schwartz,W.R.,Pedrini,H.,&Rocha,A.(2015).Deeprepresentationsforiris,face,andfingerprintspoofingdetection. IEEE Transactions on Information Forensics andSecurity, 10(4), 864-879.
[18] Bao,W.,Li,H.,Li,N.,&Jiang,W.(2009).Alivenessdetectionmethodforface recognition based onoptical flowfield.In IEEE InternationalConference onImage Analysis and Signal Processing (pp. 233-236).
[19] Zhang,Z., Yan, S., & Lei, Z. (2019).A comprehensive study on faceanti-spoofing with an ensemble of deep learning techniques. PatternRecognition,85,285-296.
[20] Kumar, A., &Bhavsar,A.(2021). Ahybrid deep learning-basedapproachfor presentationattack detectionin facerecognitionsystems. JournalofVisual Communication and Image Representation,78, 103196.
[21] Gragnaniello, D.,Sansone,C.,& Verdoliva, L. (2015).Fingerprintliveness detection based on Weberlocalimage descriptor.IEEESignal ProcessingLetters, 22(2), 176-180