International Conference on Intelligent Computing and Explainable AI (ICICEA) – April 2026

RESEARCH ARTICLE OPEN ACCESS

Smart Anti-Spy Camera Detection System Using Dual-Mode and Anomaly Analysis

Ms.G .Rajalakshmi*, Nithiyashree Murali**, Baddiga Lasyanjali**

*Assistant Professor, **UG Students - Dept.of Computer Science and Engineering
Prince Shri Venkateshwara Padmavathy Engineering College Chengalpattu, India

***Abstract*— Surveillance gadgets, including hidden surveillance equipment and spy cameras, are a major threat to personal privacy and security in public and personal spaces. Traditional surveillance systems rely on conventional methods, including manual inspection and single-mode sensing. However, these methods are less reliable and limited in scope.This paper proposes a Smart Anti-Spy Camera Detection System based on dual-mode sensing,including infrared reflection analysis and radio frequency signal anomaly detection. The proposed system uses infrared reflection analysis based on retro reflection principles to detect spy cameras. It also utilizes radio frequency signals to detect wireless transmission from spy cameras. An Isolation Forest-based anomaly detection algorithm is used to analyze the radio frequency signals and identify abnormal transmission patterns. The proposed system is based on an embedded platform using the ESP32 module, which ensures portability, low power consumption, and high performance. Experimental results show the reliability,effectiveness,and efficiency of the proposed system.**

***Keywords*—Hidden camera detection,Infrared retro reflection, RF signal analysis, Isolation Forest, Anomaly detection, Embedded systems, Privacy protection, ESP32.**

I. Introduction

Hidden surveillance equipment has become more common owing to rapid technological advancements in miniaturized electronics and wireless communication systems. Modern spy cameras are compact, inexpensive, and can be hidden in everydayobjectssuchassmokedetectors,poweradapterplugs, clocks, and decorative items.

Thepresenceofsuchhiddensurveillanceequipmentcreates asignificantthreattoindividuals'personalprivacy and security, especially in areas such as hotels, changing rooms, offices, hostels,andhomes.Theincreasingmisuseofhiddencameras emphasizestheneedforaneffectiveandreliablehiddencamera detection solution.Existing hidden camera detection techniques include manual detection and simple infrared lens reflectiontools.WhileIR-basedtoolscandetectcameralenses by reflecting IR light, they can be affected by lighting conditions and material types. Moreover, simple RF signal scanners can detect RF signals, but they are not able to distinguish between normal Wi-Fi activity and suspicious camera activity.

ApartfromtheseopticalandRF-basedtechniques,advanced systemshavealsoadoptedvision-basedtechniquesusingdeep learning algorithms. Although these systems provide high accuracy for detecting hidden cameras, they demand more computational power. Moreover, these systems are not appropriateforlow-costportablesystems.Inaddition,mostof the existing commercial systems use single-sensing technology, which is not appropriate for detecting both wired and wireless hidden cameras.

Anotherproblemwiththeexistingsystemsfordetectinghidden cameras is the dynamic nature of the wireless network. In the presence of multiple communication devices such as smartphones, routers, and Bluetooth devices, it is difficult to identify the suspicious communication.

Most of the existing RF-based systems do not have intelligent signalanalysistechniques.Theysimplyusethesignalstrengthfor detecting the presence of the hidden camera. However, this technique is not appropriate for identifying the spy camera.

In order to overcome the above problems with the existing systems for detecting hidden cameras, this paper presents the design of the Smart Anti-Spy Camera Detection System using dual-sensing technology, namely infrared lens reflection and RF signal analysis. The proposed system also employs an artificial intelligence-based anomaly detection algorithm for RF signal analysis.

By integrating optical sensing, RF monitoring, and intelligent signal processing, the proposed system promises to deliver an efficient, portable, and cost-effective solution for enhancing privacy protection against concealed surveillance detection in real-time environments.

II. LiteratureReview

ThesystemmonitorsWiFicommunicationsignalsgenerate dby surveillance cameras connected to a network. By analyzing parameterssuchasReceivedSignalStrengthIndicator(RSSI) and applying the Nilsimsa hashing algorithm, the system identifies suspicious camera transmissions and estimates their approximate location.Thismethodenablesreal-timedetectionofmultiplet ypes of WLAN spy cameras in indoor environments. [1]

The method utilizes IR sensors to detect infrared emissions generatedbyhiddencameras,particularlythoseoperatinginni ght-vision mode. When abnormal IR radiation is detected, the system triggers an alert mechanism such as a buzzer notification to warn the user. This approach provides a simple and cost-effective solution for identifying hidden cameras in indoor environments. [2]

The work [3] monitor these traffic behaviors through smartphone-based systems, hidden cameras can be detected even when the transmitted data is encrypted. This technique demonstratestheusefulnessofnetworktrafficanalysisin

identifyingcovertsurveillancedevices.[3]

The system detects electromagnetic leakage produced by covert cameras using an FM radio receiver. By analyzing electromagnetic signals emitted by surveillance devices, the modulecanidentifythepresenceofhiddencameras.Thisdesign offers a low-cost and portable solution for detecting hidden cameras using electromagnetic signal monitoring. [4]

ConvolutionalNeuralNetworks(CNNs)aretrainedtodetect hidden cameras by analyzing Photo Response Non-Uniformity (PRNU) patterns produced by camera sensors. These unique sensornoisepatternsallowidentificationofsurveillancedevices based on their hardware characteristics. This approach demonstrates the effectiveness of deep learning models in hidden camera recognition. [5]

Thesystemidentifiescharacteristictransmissionpatternsthat differentiate camera data from normal network traffic. By analyzing these behaviors through mobile devices, hidden camerascanbedetectedevenwhenoperatingwithinencrypted wireless networks. [6]

The study identifies weaknesses in authentication mechanismsandcommunicationprotocolsusedbysurveillance cameras. These vulnerabilities may allow unauthorized access or exploitation through device identifiers or weak security configurations, highlighting privacy risks associated with hidden camera technologies. [7]

The system utilizes a CNN-BiLSTM architecture to analyze CSIpatternsandidentifyabnormalsignalbehaviorproducedby hidden cameras.

By applying machine learning techniques, the approach enables accurate real-time detection of covert surveillance devices. [8]

The system captures infrared-reflected light from objects in theenvironmentandprocessestheimagesto identifyreflective patterns of camera lenses. Since camera lenses exhibit distinctive retroreflective properties, the system can detect concealed cameras in real time using infrared imaging techniques. [9]

Deep learning-based framework for wireless spy camera detection is introduced to enhance privacy protection. The system employstheCOCO-SSDobjectdetectionmodelwithin a convolutional neural network architecture to identify both visibleandconcealedcamerasincapturedimages.Byanalyzing visual features of the environment, the method provides an intelligent approach for detecting surveillance devices without requiring additional hardware components. [10]

Althoughseveralexistingapproacheshavebeenproposedfor hidden camera detection, many systems rely on a single detection technique such as wireless traffic analysis, infrared sensing, or image processing. These approaches may face limitations in complex environments where cameras may not continuously transmit signals or may operate without visible indicators.Toovercometheselimitations,theproposed system integrates IR sensor-based lens reflection detection, RF signal monitoring,andAI-basedanomalydetectionusingtheIsolation Forest algorithm on an ESP32 platform, providing a portable and multi-sensor solution for real-time hidden spy camera detection

RELATEDWORK

Existing hidden camera detection systems are mostly centered around the analysis of wireless network traffic and signal-based detection. Various research studies have been conducted on the detection of WLAN-enabled spy cameras by analyzing RSSI, network traffic patterns, and wireless signals [1][8]. These systems are capable of detecting cameras that transmit data over a WiFi network and are able to provide an approximate location of the camera. However, they are fundamentally limited in that they cannot detect cameras that store data locally and do not transmitdatawirelesslythattransmitdataoveranetworkandar e unabletodetectcamerasthatstoredatalocallyanddonottrans mit data.

Infrared-based camera detection systems are another type of camera detection solution that has been extensively researched andemployedforthedetectionofnightvisioncameras[2][9].T he existing systems are capable of detecting cameras that transmit data in infrared and are relatively simpler and cost-effective solutions. However, the existing systems are limited in that the accuracyofthesolutionisaffectedbyenvironmentalfactors,a nd the presence of infrared sources may cause false positives in camera detectionsystemsthatare basedon infrared retroreflectionimage processing systems.

TableI.ComparisonofExistingHiddenCameraDetection Methods

Recently, new research has been conducted on the use of electromagneticleakage,andtheapplicationofdeeplearninghas beenintroduced[4][5][10].TheuseofFM-based,CSI-based,and CNN-basedmethodsisbasedontheanalysisofthecharacteristics of the wireless signals or images, and the classification is conducted accordingly, providing a hardware solution for the detectionofharmonicemissionsfromcameracircuits.Theabove methods are based on the analysis of the characteristics of the signalsorimages,andtheclassificationisconductedaccordingly.

Even though significant research has been conducted on the improvement and introduction of new methods for the detection ofhiddencameras,allexistingsystemsarebasedonasingletype of detection mechanism and are limited to specific types of camerasoroperatingconditions.Theabovelimitationsneedto be overcome, and a more robust and adaptive detection framework must be provided, improving the accuracy and minimizing false detections, and providing a better solution for privacy protection in real-world scenarios.

III. PROPOSEDMETHODOLOGY

A. SystemOverview

The proposed system is based on the idea of developing a multi-modal hidden camera detection system, which will be helpful in enhancing privacy protection in various indoor locations,includinghotelrooms,hostels,washrooms,changing rooms,offices,and rentalrooms,etc.Duetotheincreasedrisk of unauthorized surveillance, there is a need to develop detection mechanisms to reduce the risk of hidden camera usage. The proposed system will be helpful in solving the problembyintegratingvarioussensing andintelligentanalysis techniques.

The overall system architecture is based on the idea of integrating various interconnected modules, including data acquisition, signal processing, feature extraction, and intelligent decision-making. Unlike existing systems, the proposedsystemisbasedontheideaoffusinghybriddetection techniques,includinginfraredandradiofrequencymonitoring.

The system will be able to scan the environment and detect suspicious signals, indicating the usage of hidden cameras. Various stages of signal filtering will be performed to reduce the impact of noise and interference. After completing the preprocessing stage, the signals will be passed to the feature extraction module, where meaningful patterns will be identified. Then, the IsolationForestalgorithm willbeapplied to the signals, enabling real-time detection and classification.

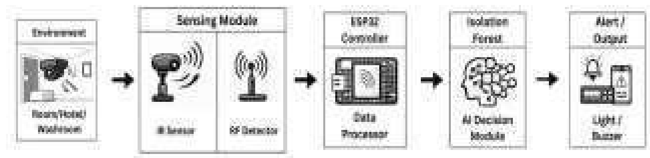


Fig.1.SystemArchitectureoftheProposedSmartAnti-Spy Camera Detection System

B. OperationalEnvironmentInterface

The operational environment interface represents the physical deployment space where the detection system operates. This includes environments such as hotel rooms, hostels,washrooms,offices,andotherprivateindoorlocations wherehiddencamerasmaybeinstalled.Thesystemisdesigned tofunctionseamlesslyintheseenvironmentswithoutrequiring any structural modifications or specialized installation procedures.

This module is responsible for capturing environmental context information, including lighting conditions, reflective surfaces, and ambient wireless activity. These environmental factors significantly influence sensor behavior and detection accuracy. For instance, reflective surfaces may cause false IR reflections, while background wireless signals may introduce RF noise. Therefore, understanding the environment is essential for reliable detection.

By continuously interacting with the surrounding environment, the system adapts its sensing and detection mechanismstoreal-worldconditions.Thisensuresthatthe detectionprocessremainseffectiveevenincomplexenvironmentswithvaryinglightingandsignalinterference.

Theoperationalinterfacethusservesasthefoundationforreal-time sensing and monitoring, enabling accurate detection of hidden cameras in practical scenarios.

C. Multi-SensorAcquisitionUnit

Themulti-sensoracquisitionunitisresponsibleforcollecting raw environmental data using multiple sensing technologies. Itconsistsof an IRLED, anIRphotodiode sensor,and anRF detector module, each playing a crucial role in detecting hiddencameras.Theintegrationofmultiplesensorsallowsthe systemtocapturedifferenttypesofsignals,therebyimproving detection reliability.

The IR LED emits infrared light at a specific

Method	Mode	En
IR Retro	Optical Lens Reflection	N/
CamFirm (FM)	RF Harmonics	YE
Traffic Pattern	Wi-Fi Traffic analysis	NO

wavelength into the environment. When this light encounters a camera lens, it produces retroreflection due to the curved and reflective properties of the lens surface. The reflected IR signal is captured by the photodiode sensor, and its intensity is measured. Higher reflection intensity may indicate the presence of a camera lens, especially in low-light conditions where such reflections are more prominent.

Atthesametime,theRFdetectormodulesearchesforsignals in the radio frequency band to detect the signals being transmittedwirelesslybythespycamera.TheRFmodulealso picksupthesignalstrengthandvariations.Thisinformationis then analyzed to check for unusual patterns. Information gathered by both IR and RF sensors creates a comprehensive picture of the surroundings and is sent to the processing unit.

D. EmbeddedControlandSignalConditioning Unit

The embedded control and signal conditioning unit is the central processing unit of the system. It is implemented as a microcontroller platform, such as the ESP32, capable of real-timedataprocessingandcontrol.Theunitprocessesrawsensor data from the IR and RF module.

The main role of this module is to condition the signals, including removing noise, interference from the environment, and normalizing the signals. The environment, including ambient light, reflections from non-camera objects, and background wireless signals, may interfere with the signals. The conditioning ensures that only significant and relevant information is extracted from the signals.

Further, the module also converts the analog signals from the sensorintoadigitalformat,whichcanbeeasilyprocessedand analyzed. At the same time, it also carries out preliminary checks based on thresholds and organizes the data into a structuredformat,referredtoasfeatures.Thisstageisalsovital inenhancingtheaccuracyofthedetectionsystem,eliminating false positives, and ensuring that the data used is clean and reliable.

E. IsolationForestDecision-MakingEngine

The decision-making part of the system utilizes the IsolationForestalgorithm,which isanunsupervised machine learning approach for anomaly detection. This approach is differentfromsupervised machinelearningapproachesinthe sensethatitdoesnotneedlabeleddatafortrainingthemachine learning models and is thus appropriate for real-world applications,especiallywhenitisdifficulttodefineabnormal patterns.

The Isolation Forest algorithm utilizes multiple decision trees randomly generated and the isolation of data points according to the values of the features. The normal data points need more splits to be isolated by the decision tree, while the anomalous data points, such as abnormal IR reflectionsandRFsignalspikes,arequicklyisolatedbythe decision tree and thus have higher anomaly scores.

Initially, the model is trained using baseline data collected in a camera-free environment, establishing a normal behavior profile. During real-time operation, incoming feature vectors—such as IR reflection intensity, RF signal strength, RF variance, and spectral entropy—are evaluated by the model. If the computed anomaly score exceeds a predefined threshold, the system classifies the observation as a potential hidden camera detection, enabling accurate and automated decision-making.

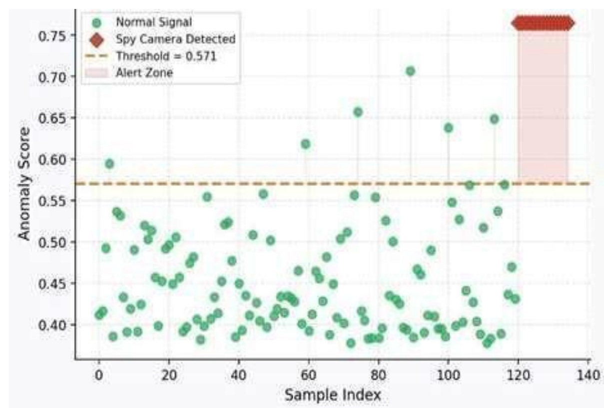


Fig.2.AnomalyScoreperSample—Isolation Forest Output

Thealgorithmisfirsttrainedonbaselineenvironmentaldata collected in a camera-free environment to establish the normalsignalprofile.Duringreal-timeoperation,incoming sensor feature vectors—comprising IR reflection intensity, RF signal strength, RF signal variance, and spectral entropy—are passed to the trained Isolation Forest model. An anomaly score is computed for each sample, and if this scoreexceedsthepredefineddetectionthresholdthesample is classified as indicative of a hidden camera presence.

F. AlertandNotificationSystem

The alert and notification system is responsible for providing feedback to the user in real-time upon the detection of a potential hidden camera by the Isolation Forest model.

Themoduleconsistsofacombinationofvisualandauditory alert systems, such as the LED and buzzer alarm systems. ThemoduleconsistsofagreenLEDforasafeenvironment and a red LED for a potential detection environment. The buzzeralarmsystemprovidesareal-timenotificationtothe user even without visual attention to the device

Furthermore, the system utilizes the ESP32's Wi-Fi capabilitytosendreal-timenotificationstoamobilepplication for increased user convenience and remote monitoring.Oncethealertcycleiscomplete,thesystemresets and continues with the monitoring process for uninterrupted operation and increased security against potential hidden camera devices.

IV. ExperimentalSetup

The proposed system for the detection of hidden cameras has been implemented in a hardware form using an ESP32 microcontroller that works as a central embedded system for real-time data acquisition and processing. The hardware components of the system include an Infrared (IR) sensor module for detecting retroreflective lens activity and an RF detector module for detecting wireless signal activity. Other auxiliarycomponentslikeLEDsandabuzzerarealsoinclu ded for immediate notification of detected camera activity.

TheIRsensingmoduleoperatesbyemittinginfraredlighti nto theenvironmentandmeasuringthereflectedintensityusi nga photodiode sensor. Hidden camera lenses exhibit characteristic retroreflection properties, which result in noticeablespikesinIRintensitywhenpresent.Inparallel,t he RF detector continuously scans the surrounding frequency bands (primarily 2.4 GHz and 5 GHz) to capture wireless transmissionsfromactivespycameras.Thesensoroutput sare collectedasanalogsignalsandprocessedbytheESP32,w here they are conditioned, digitized, and converted into feature vectors for further analysis.

Toevaluatesystemperformance,experimentswerecondu cted in controlled indoor environments simulating real-world conditions,suchasahotelroomsetup.Multiplehiddenca mera types were used during testing, including Wi-Fi-enabled cameras and IR-based night vision cameras, to ensure comprehensive validation. The experiments were designed undervaryingenvironmentalconditions,includingchan gesin lightingintensity,presenceofreflectivesurfaces,anddiff erent levelsofbackgroundwirelessactivity.Thisapproachensu res that the system is tested under realistic scenarios where environmental noise and interference may affect detection accuracy.

The performance of the proposed system was assessed by analyzingtemporalvariationsinIRreflectionintensityan dRF signal strength. During normal conditions (i.e., absence of hiddencameras),thesensorreadingsremainedwithinasta ble baseline range. However, when a hidden camera was introduced into the environment, a significant increase in IR reflection intensity and RF signal fluctuations was observed. These variations were captured over time and plotted to visualize detection patterns.

ThisisevidentinthegraphicalrepresentationinFig.3,whi ch showsspikesforthepresenceofhiddencameras.Thesespi kes confirm the efficacy of the proposed approach for acquiring data using multiple sensors for identifying abnormal environmental conditions. The use ofbothIRand RFsensors allows for the detection of both active and inactive cameras.

Moreover,thefeaturesextractedusingtheproposedappro ach were analyzed using the Isolation Forest algorithm.

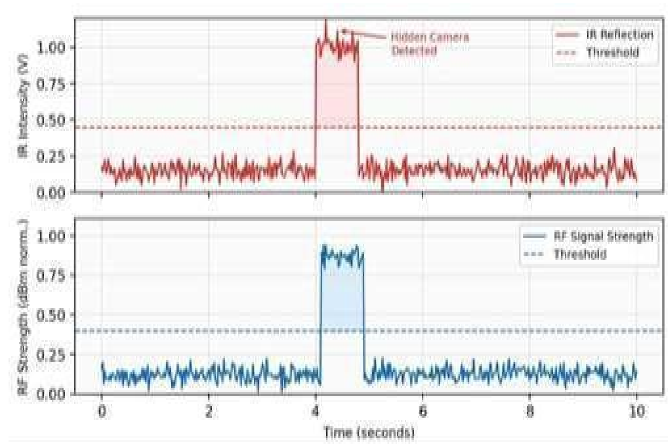


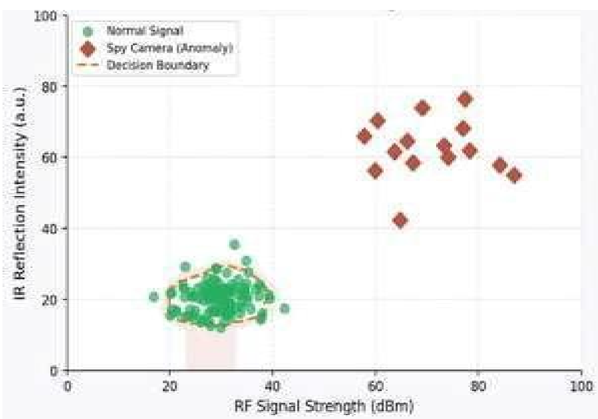
Fig.3.TemporalVariationofIRReflectionIntensityandRF Signal Strength During Hidden Camera Detection

component,itcaneffectivelydetecthiddencameras.

AsshowninFig.3,asuddenspikeinIRreflectionintensity and RF signal strength above predefined threshold levels clearlyindicatesthepotentialpresenceofahiddensurveillance camera, triggering an immediate alert. Comparative performanceevaluationagainstexistingmethods,illustratedin Fig. 5 and Fig.6,demonstratesthe superiority of theproposed system in terms of both detection accuracy and portability.

.

The features were visualized in the RF vs. IR feature space, and the decision boundary plot is shown in Fig. 4. The plot indicatesthat normal environmental data pointsare separated from abnormal data points representing hidden camera presence.



Fromthevisualization,it isclearthatthedecisionengine basedontheIsolationForestapproachisabletodifferentiate between normal and abnormal signals, even in different environmental conditions. The anomaly score for the data pointsindicatingthepresenceofthehiddencameraishigher in the model, thereby classifying the data with minimal errors.

Fromtheexperimentalresults,itisclearthattheproposed system for the detection of hidden cameras is effective in providingreal-timeresultswiththehelpofmachinelearning approaches and multi-sensor data acquisition systems. The system is consistent in different environmental conditions.

V. Result

The IR detection component detects infrared signals emitted by a hidden camera, which is used for night vision. The RF detection component detects suspicious RF signals emittedbyahiddencamera.Bycombiningthesesignalsand processingthemthroughtheintelligentdecision-making

Fig.5.DetectionAccuracyvsFalsePositiveRateComparison

WhiletheproposedsystemeffectivelyintegratesIRsensing, RF analysis, and Isolation Forest-based anomaly detection on an embedded platform, future enhancements may explore advanced hybrid AI frameworks that combine unsupervised anomaly detection with deep neural architectures trained on large-scalesurveillancesignaldatasets.Suchintegrationwould require high computational resources, extensive labeled datasets, and optimized edge-AI acceleration hardware.

Fig.6.PortabilityScorevsOfflineCameraDetection Comparison

VI. FutureWork

Further research may involve real-time RF spectrum fingerprinting and channel state information (CSI) analysis to detect ultra-low-power or encrypted covert cameras that operate with minimal transmissionsignatures. Implementing such techniques would demand specialized signal processing modulesandadvancedwirelessanalysisinfrastructurebeyond

thescopeofthecurrentprototype.

Additionally, large-scale deployment studies across diverse architectural environments could be conducted to develop generalized adaptive environmental modeling systems.Thiswouldinvolvecomplexcalibrationalgorithms and extensive field validation under controlled and uncontrolled interference scenarios. These enhancements would further strengthen detection robustness but require substantial research, infrastructure, and computational support.

VII. Conclusion

This work proposes an integrated Smart anti-spy camera detection system, which utilizes multi-sensor data acquisition,signalprocessing,andsmartdecision-makingto provide enhanced personal privacy and security. In recent times,duetotheproliferationandmisuseofspycameras,the detectionofthesedeviceshasbecomeasignificantproblem. Conventional camera detection techniques, where a human observer identifies the camera or utilizes single-sensor camera detection, are no longer sufficient. In this work, we propose a camera detection system that utilizes infrared reflection and radio frequency signal detection to identify bothpassiveinfrared-basedcamerasandactivewirelessspy cameras in indoor environments.

The integration of multi-sensor data within a unified framework provides improved camera detection reliability and robustness. In this work, the infrared sensor utilizes the retroreflective characteristics of camera lenses, whereas the radio frequency sensor utilizes abnormal radio frequency transmission patterns to identify spy cameras. Such multi-modal camera detection ensures the camera detection system's reliability in different environments, including varying lighting conditions, presence of reflective surfaces, and radio frequency transmission. Such a multi-modal approach provides improved camera detection accuracy compared to conventional camera detection systems.

TheuseofESP32intheformofanembeddedcontrolunit ensures real-time signal acquisition, conditioning, and processing. This ensures efficient system performance with minimal computational overhead. Moreover, the use of the Isolation Forest algorithm enhances the system's capability to detect anomalies in the signals.

ByusingfeatureslikeIRintensityandRFsignalchange ,the system can identify normal environmental conditions and abnormal activities with high confidence. This eliminates the need to constantly monitor the environment.

The alert and notification feature ensures that the user becomesawareofthesituationinrealtime.Thisfeatureutil izes visual, audio, and wireless notifications to alert the user. The system's compact and portable design ensures that it can be implemented in a variety of privacy-concerned environments. Some of these environments include hotel rooms, hostels, offices, and washrooms. The autonomous capability of the system enhances its usability.

Overall, the proposed work shows that the problem of spy camera threats can be effectively addressed by a multi-sensor AI-based detection framework. This work also shows that the proposed system can provide a good trade-off in terms of accuracy, cost-effectiveness, portability, and real-time performance.Therefore,thisworkhassignificantimplica tions for the development of intelligent surveillance detection techniques. This work also provides a foundation for future research in secure, automated, and user-centric privacy protection.

References

[1] HyeyoungAn;etal.,"WirelessSpyCameraSpotteSystemWithReal-timeTraffic Similarity Analysis And wifi Signal Tracing", IEEE,2024.
[2] EleniAthanasiadaou; et al., "Camera Recognition With Deep Learning",Forensic Sciences Research,IEEE ,2018.
[3] QianruLiao;etal.,"CamFirm:ACompactFM-BasedModule ForHiddenCamera Detection, IEEE, 2025.
[4] Dinhnguyen Dao; et al., "DeepDeSpy: A Deep Learning -Based WirelessSpy Camera Detection System, IEEE, 2021.
[5] VaishaliKoul;etal.,"HiddenCameraDetection",InternationalJournalOfAdvance Research In Science And Engineering, IEEE, 2017.
[6] ShaikRuksana;etal.,"IOT-EnabledCovertSurveillanceCamera Identification Through IR Sensor, IEEE, 2024.
[7] Yushicheng;etal.,"OnDetectingHiddenWirelessCameras:ATrafficPatten -Based Approach, IEEE, 2020.
[8] Woojin Park;etal.,"Real-TimeSensingAnd On SiteSpottingSchemaOfMulti-Type WLAN Spycams, IEEE, 2024.
[9] SamuelHerodotou;etal.,"SpyingOnTheSpy:SecurityAnalysisOf HiddenCameras",WarwickUniversity,Conventry,IEEE,2023.
[10] KuchulakantiShruthi;etal.,"SpynetADeepLearningApproach ToWireless Spy Camera Detection", IJERT, IEEE, 2025.