Project Proposal: Hidden Camera Detection

1st Bryan Tran
Gallogly College of Engineering
University of Oklahoma
Norman, Oklahoma, United States of America
bryan.l.tran-1@ou.edu

2nd Ibtesum Arif
Gallogly College of Engineering
University of Oklahoma
Norman, Oklahoma, United States of America
ibtesum.arif-1@ou.edu

***Abstract*—This document explores ten research papers related to detecting hidden cameras. Based on the literature survey of these ten research papers, a proposal for a project will be formed. This paper presents key ideas, methodology, results and limitations of these studies. This paper suggests a potential solution by identifying which technique would be most efficient, accurate, and practical after analysis.**

I. Introduction

An individual's basic right is to control when and how they are being observed, especially in private places like homes, hotel rooms, changing areas, and bathrooms. Hidden cameras record people without consent, which makes them a serious invasion of privacy. This issue has become more common today because of the availability of small and inexpensive surveillance devices that can be hidden inside everyday objects.

The presence of hidden cameras creates risks not only for individuals but also for businesses and organizations that must ensure trust and safety in the environments they provide. Visual inspections are often unreliable because cameras can be disguised too well. For this reason, many technical solutions have been studied, such as thermal emission analysis, optical reflection, wireless traffic monitoring, and machine learning approaches. Each of these techniques can detect certain types of cameras, but none provide a complete solution in every setting.

The difficulty comes from the fact that cameras can operate in different ways. Some transmit data wirelessly, while others store it locally. Some give off heat or electromagnetic signals, while others blend into the noise of surrounding devices. Because of these differences, existing methods often work well in some scenarios but fail in others. This project explores ten research papers that each present methods for detecting hidden cameras. The goal is to study their ideas, methods, and results in order to determine which approach is most effective overall and to propose a solution that builds on the most promising method for real-world use.

II. Bryan Paper 1 Summary

The paper *CamDetector: Detecting and Positioning Hidden Cameras with Raspberry Pi 4 via EM Radiation* [1] presents a system designed to identify and localize spy cameras based on their electromagnetic (EM) emissions. Hidden cameras are difficult to detect because they can operate offline, store video locally, and be disguised in everyday objects. This makes existing approaches such as traffic-based analysis, lens reflection, or thermal imaging less reliable. The authors discover that CMOS-based cameras generate distinct EM signatures caused by coupling between the system clock and the line-by-line pixel readout on the CSI cable. These signatures, which combine high-frequency harmonics and lower-frequency line readout signals, form the basis for their detection method.

CamDetector uses low-cost hardware, including a Raspberry Pi 4 and a software-defined radio (SDR), to capture and analyze signals in the 100–500 MHz range. Its workflow consists of two main stages: sweeping the spectrum to collect candidate signals and then judging whether these signals match the spectral and temporal features of hidden cameras. By leveraging both frequency-domain harmonics and time-domain patterns tied to frame rates, the system can reliably distinguish cameras from other electronic devices. It also provides localization by observing changes in baseband signal strength as a user moves the device around a room.

The system is evaluated on six small commercial cameras, including battery- and USB-powered models. In controlled tests, CamDetector achieves 90.08% accuracy and 88.21% recall at a detection distance of 0.4 m, with maximum ranges up to 165 cm for USB-powered cameras. Real world experiments in an 18 m^2 hotel room show that the system maintains strong performance under interference, achieving about 85% localization accuracy. A user study with 20 volunteers demonstrates that participants could successfully find hidden cameras in roughly 17 minutes on average by following the detector's guidance.

Overall, CamDetector [1] demonstrates that EM radiation signatures offer a practical and effective new way to detect and localize hidden cameras. Unlike prior systems that rely on wireless traffic or optical reflections, CamDetector works even against offline cameras and requires only affordable, portable hardware. This work contributes to the growing field of privacy protection tools that aim to counter the risks posed by covert surveillance devices.

III. Bryan Paper 2 Summary

The paper *On Utilizing Smartphone Time-of-Flight Sensors to Detect Hidden Spy Cameras* [2] introduces a system called LAPD that leverages ToF sensors embedded in modern smartphones to detect and localize hidden cameras. Unlike

traditional detectors that rely on visible light reflections or wireless traffic analysis, LAPD directly exploits lens-sensor retro-reflection: when a laser pulse from the ToF sensor hits a camera lens, nearly all the light energy reflects back toward the source. This produces a unique optical signature that can be distinguished from surrounding objects.

LAPD guides the user through scanning suspicious objects at an optimal distance to ensure reflections are visible but not saturated. Its detection pipeline applies image processing filters to remove reflections too large or irregular to come from a lens, and then uses a CNN trained on 10,000 examples to eliminate remaining false positives. If a hidden camera is confirmed, the system highlights its position on-screen with augmented reality.

The system was implemented on a Samsung S20+ with a Sony IMX516 ToF sensor and evaluated against common baselines, including the K18 hidden camera detector and the naked eye. In tests across 30 objects (nine containing hidden cameras), LAPD correctly identified eight out of nine cameras (88.9%) while maintaining a lower false positive rate of 16.7%. This substantially outperformed the baselines, which struggled with both detection accuracy and false alarms.

Overall, LAPD [2] demonstrates that ToF-based smartphone sensing provides an accessible and accurate way to detect hidden cameras in real-world settings. By combining hardware already available on commodity devices with machine learning filtering, it offers a practical balance between reliability, user effort, and affordability.

IV. Bryan Paper 3 Summary

The paper *LocCams: An Efficient and Robust Approach for Detecting and Localizing Hidden Wireless Cameras via Commodity Devices* [3] shows that smartphones can be adapted to detect spy cameras using ToF sensors and reflections. Building on the same privacy problem, the work presents LocCams, which instead relies on wireless traffic analysis and channel state information (CSI). Unlike ToF-based systems that need specialized smartphone hardware, LocCams works with commodity devices such as regular smartphones. This makes it easier for ordinary users to apply in real-life situations like hotels or rental accommodations.

LocCams operates in two stages: detection and localization. Detection uses the packet transmission rate (PTR) of wireless devices, since cameras transmitting live video show distinctive traffic patterns, especially when the user moves. For localization, LocCams examines CSI distributions to determine if the path between the phone and the suspected device is line-of-sight (LOS) or non-line-of-sight (NLOS). A lightweight CNN model processes these CSI features to help identify the direction of the hidden camera. The user only needs to perform simple stationary-to-turn actions while holding their phone, which is less demanding than earlier methods that required scanning walls or replaying video clips.

The authors evaluate LocCams using nine camera models across eight rooms with different subjects and configurations. Results show that the system can detect and localize hidden cameras with about 95% accuracy and typically within 30 seconds. Importantly, it generalizes well to new rooms and cameras that were not part of the training data. Compared to earlier techniques, LocCams combines high detection accuracy with low cost and minimal user effort, making it both practical and effective.

Overall, the paper demonstrates that wireless traffic analysis can be used not only to detect hidden cameras but also to localize them in three dimensions, including on ceilings. While LAPD [2] relies on optical sensing, LocCams provides a complementary approach based on wireless behavior. Together, these works highlight how smartphones can become accessible tools for protecting personal privacy against hidden surveillance devices.

V. Bryan Paper 4 Summary

The paper titled *AI-aided Hidden Camera Detection and Localization based on Raw IoT Network Traffic* [4] addresses growing privacy concerns caused by the spread of hidden cameras in hotels, motels, and rental accommodations. Hidden cameras are often small IoT devices that connect to Wi-Fi and either store recordings locally or stream video to the cloud. Detecting these devices is critical for protecting privacy, yet traditional methods of scanning or manual inspection are unreliable and time consuming.

To tackle this issue, the authors propose AI-aided Hidden Camera Locator (AHCL), a system that detects and localizes hidden cameras by analyzing raw IoT network traffic. The design of AHCL consists of two components: a monitoring node and an edge server. The monitoring node captures raw packets from the router, while the edge server processes the data. The workflow involves several steps. First, a Support Vector Machine (SVM) filters video-related packets from general network traffic. These packets are then refined through a Denoising Autoencoder (DAE) that removes noise caused by moving objects and other disturbances. Finally, the cleaned packet streams are classified by an ensemble of neural networks, including Multi-Layer Perceptrons (MLP), Convolutional Neural Networks (CNN), and Inception ResNet v2, which collectively identify whether a hidden camera is present and determine its location down to a specific room.

The experimental evaluation involved smartphone cameras acting as hidden devices in classrooms and lab environments, with Zoom video streams used to simulate real-world traffic. AHCL demonstrated strong results, achieving 99.5 percent accuracy in both detecting and localizing hidden cameras. Importantly, this approach avoids reconstructing full video streams, which makes it faster and more efficient than prior methods.

The adversary model assumes that an attacker has planted a hidden camera on the same Wi-Fi network as the monitoring system. Under these conditions, AHCL enables the detection of hidden cameras and their localization in real time.

The study highlights that working with raw packet data, rather than fully processed video, is the key innovation of AHCL, since it allows the system to achieve high accuracy

while remaining computationally efficient. However, the experiments were conducted in limited settings, and the authors note that future work will need to expand testing across diverse environments and a wider variety of camera devices.

In summary, this work provides a practical and effective defense against hidden cameras by combining AI models with network traffic analysis. By filtering, denoising, and classifying raw traffic, AHCL offers a promising solution for real-time protection of user privacy.

VI. Bryan Paper 5 Summary

The paper DeWiCam: Detecting Hidden Wireless Cameras via Smartphones [5] introduces a method for detecting hidden Wi-Fi cameras using only smartphones. Hidden cameras pose serious privacy concerns in public spaces and rental accommodations, but traditional detection methods often require specialized hardware or direct access to video streams. DeWiCam takes advantage of the fact that wireless cameras produce distinctive traffic patterns because of video and audio compression as well as packet fragmentation, even when the traffic itself is encrypted.

The system is designed to run on Android devices. It uses the Wi-Fi card in monitor mode to capture packets and then constructs traffic flows based on MAC addresses. From these flows, DeWiCam extracts features from the PHY and MAC headers, such as packet length distribution, bandwidth stability, and duration values that are tied to camera hardware. These features are then processed by an ensemble learning classifier, ExtraTrees, which determines whether the traffic belongs to a camera.

An additional human-assisted component helps determine whether a detected camera is located in the same room. This works by correlating bitrate fluctuations of the suspected camera traffic with motion data from smartphone sensors. If the bitrate patterns match the user's movements, the system concludes that the camera is in the same physical space.

The authors evaluated DeWiCam with twenty different camera models in a variety of environments. The results showed more than 99 percent accuracy in detecting hidden cameras within an average time of 2.7 seconds. The system was also effective when multiple cameras were present, when the network was congested, and even when encountering camera brands not included in the training phase.

In summary, DeWiCam provides a practical and accessible way to detect hidden cameras by focusing on traffic patterns instead of decrypting video or relying on expensive scanning devices. The work demonstrates that smartphone-based solutions can be powerful tools for protecting privacy in everyday environments.

VII. Arif Paper 1 Summary

The paper titled *CamRadar: Hidden Camera Detection Leveraging Amplitude-modulated Sensor Images Embedded in Electromagnetic Emanations* [6] presents a novel method for detecting hidden cameras by examining the unique electromagnetic signals unintentionally released by their image sensors. Hidden cameras pose a significant privacy risk in locations such as workplaces, public toilets and hotels. Locating hidden cameras visually or through manual inspections is challenging, particularly when they are cleverly hidden. CamRadar provides an intelligent solution by identifying the electromagnetic (EM) signals emitted by cameras during operation. Camera sensors naturally emit electromagnetic signals during operation. CamRadar detects hidden cameras by capturing and analysing these signals. As a result, users can locate hidden cameras without making any contact.

The goal of this study is to develop a system that efficiently and precisely identifies concealed cameras using electromagnetic signals, even in crowded or complicated settings. The system should help users to identify hidden cameras without any specialized equipment.

CamRadar uses devices that can pick up EM signals. The system identifies patterns in the intensity, frequency, and form of these signals to detect active camera sensors. It works in four steps: scanning the environment for EM emissions, picks out features of the signal, eliminating background noise from other electronic devices and applying pattern recognition to find which signals are likely from cameras. The system is designed to minimize confusion from other devices, thereby reducing false alarms.

CamRadar successfully identified hidden cameras with an accuracy rate of 93.23%, typically in less than 17 seconds. Comparative analysis indicated that CamRadar outperformed manual inspection and traditional infrared-based detection methods, particularly in cluttered indoor environments. The system proved to be reliable. It performed effectively even in the presence of other electronic devices.

Although the system is effective, its effectiveness is highly dependent on the relative position and orientation of the camera. The system performs optimally when the hidden camera is oriented in a specific direction. Positioning the camera at an unusual angle may complicate detection. Also, some other devices may produce similar EM signals, causing a 16.7% false positive rate. Factors such as metal walls or elevated RF noise can also diminish accuracy.

CamRadar can be very effective in places where privacy is important. It offers security staff a useful, unobtrusive resource to guarantee adherence to privacy laws and improve overall situational awareness. As it works without touching or moving anything, the system is ideal in situations where direct access is limited.

VIII. Arif Paper 2 Summary

The paper titled *HeatDeCam: Detecting Hidden Spy Cameras via Thermal Emissions* [7] presents a thermal-based method for identifying hidden cameras utilising their unique heat patterns.

The authors propose HeatDeCam, a system that utilizes thermal emissions to spot hidden spy cameras, even in situations where they cannot be seen with the naked eye. As there are growing concerns of unauthorized surveillance through

hidden spy cameras, the system HeatDeCam can be a potential solution.

The primary goal is to Create a dependable technique for detecting hidden spy cameras through thermal imaging. Additionally, Enhance privacy and security in sensitive environments is also a priority. The authors felt the need to provide a tool that can be used by individuals and organizations to protect against unauthorized surveillance.

HeatDeCam employs infrared cameras to capture the thermal emissions generated by objects within a given environment. To detect anomalies that could suggest the existence of hidden cameras, The thermal data collected is analyzed. Moreover, The authors also developed algorithms capable of differentiating between typical heat patterns and those linked to surveillance devices, enabling accurate detection even in intricate environments.

HeatDeCam was effective in recognizing both wired and wireless surveillance devices, demonstrating its versatility in various applications. The system showed a high level of accuracy in spotting hidden spy cameras across various scenarios. Real-world implementations validated its practical utility, suggesting that in order to enhance privacy security, the system can be reliably used in everyday environments.

Although the result shows that the system can be very efficient in real world environments, performance can be affected by environmental factors. For example, variations in ambient temperature may interfere with thermal readings. Moreover, the cost and accessibility of high-quality thermal imaging equipment may limit its widespread adoption. Lastly, detection accuracy can be affected due to differences in camera design and materials.

The paper presents HeatDeCam as an innovative solution to detecting hidden cameras, enhancing security and privacy through thermal imaging technology. The system allows user to check for hidden cameras in private spaces. So anywhere where privacy is needed, this system can be used to detect hidden cameras.

IX. Arif Paper 3 Summary

The paper titled *Hidden Camera Detector Using Magnetometer and Accelerometer Sensor* [8] proposes a mobile application that uses motion and magnetic anomalies to detect hidden cameras.

Smartphones come equipped with built-in sensors that can serve purposes beyond regular tasks. The author proposes a smartphone-based system which helps to detect electronic devices such as cameras and microphones. The built-in sensors in the smartphone can be used to detect hidden electronic devices. As no other special equipment other than the smartphone is needed to detect hidden electronic devices, the approach is attractive. Unlike specialized equipment, smartphones are compact, cost-effective, and commonly utilized.

The goal is to develop an Android app that to detect hidden devices accurately by utilising smartphone sensors. The system should provide real time alerts and operate without any additional hardware.

The app uses two sensors in the phone, which are magnetometer and accelerometer. The magnetometer detects changes in magnetic fields caused by electronic parts. Accelerometer is used for detecting minor movements or vibrations from operational devices. The app constantly monitors the surroundings, searching for irregular patterns, and notifies the user when a potential threat is detected. The workflow involves continuous sensor monitoring, feature extraction, and anomaly detection. Sophisticated algorithms analyze the sensor data to differentiate between typical environmental changes and patterns that suggest the presence of hidden devices.

Testing conducted in residential areas, public spaces, and workplaces demonstrated that the app works well. The app proved to detect electronic devices only using the smartphone sensors and without needing any extra equipment or additional equipment. The smartphone-based approach offered faster detection times and greater convenience in comparison to manual inspection.

The detection may fail if the quality of the built-in sensors in the smartphones are up to the mark. Strong magnetic interference from other electronic devices can lead to false positives, while extremely low-power devices may go undetected. Moreover, the app can not detect very quiet or passive devices that do not emit signals.

This solution is ideal for inspecting hotel rooms, workspaces, or personal areas for hidden devices. Additionally, it can be useful for security teams before private meetings.

X. Arif Paper 4 Summary

The paper titled *Are There Wireless Hidden Cameras Spying on Me?* [9] proposes a smartphone app that uses encrypted Wi-Fi traffic analysis in order to detect and locate wireless spy cameras. The use of wireless hidden cameras is becoming very common due to their easy setup and mobility. Conventional detection methods often struggle because these devices do not depend on visible light or tangible indicators. This paper explores a method that detects hidden cameras by analyzing Wi-Fi traffic. This technique is particularly relevant in environments abundant with Wi-Fi connectivity.

The goal of this project is to develop a smartphone-based system that can reliably detect wireless spy cameras by analyzing network traffic patterns from networks without the need to decrypt any information, thereby safeguarding user privacy.

The system gathers packet level information to detect unusual patterns linked to camera behavior by monitoring Wi-Fi traffic. Without the modification of network hardware or breaching encryption, it is possible to detect and localize hidden cameras through this approach. The system analyzes packet frequency, device functionality, and usage patterns. To differentiate spy cameras from standard devices, machine learning is employed.

The system accurately detected and located hidden cameras in real-world environments. In standard setup, detection accuracy was high and it demonstrated robustness to varying Wi-Fi configurations. It performed really well in spotting cameras us-

ing advanced network protocols, functioned effectively across diverse Wi-Fi environments.

The accuracy of detection may degrade in densely populated networks or in the presence of strong encryption. localization can be complicated because of certain network topologies. Devices that infrequently transmit data or remain silent on the network can go unnoticed. So the system has some limitations.

This approach helps users to keep an eye on networks in offices, hotels and public areas in order to spot unauthorized wireless cameras. This system can be used to enhance privacy. It enables users or security personnel to examine networks for hidden cameras, providing enhanced privacy against unauthorized surveillance.

XI. Arif Paper 5 Summary

The paper titled *Presence of Active Mobile Phones and Hidden Camera Detection* [10] proposes an RF-based system that uses a microcontroller in order to detect hidden cameras and active mobile phones in restricted areas. This authors introduces an affordable embedded system designed to identify RF emissions from functioning devices. The authors felt that as unauthorized mobile phones and cameras pose a significant risk by enabling information leakage in high-security environments, this system can be used to enhance security as the system can deliver immediate alerts to enhance security measures.

The primary goal is to detect active mobile phones and hidden cameras in restricted areas in order to protect sensitive information.

The system uses an ATmega 8 microcontroller to constantly scan the radio frequency spectrum for signals emitted by cameras and mobile phones. Signals are analyzed for frequency, strength and modulation patterns associated with unauthorized devices. The system generates visual or auditory alerts to notify security personnel when a suspicious signal is detected. The system enables real-time monitoring with minimal user involvement.

Testing demonstrated the systems ability to distinguish between mobile phones, cameras, and other electronic devices, reducing false positives. The system proved to be cost effective and suitable for deployment in multiple secure environments. The system produced reliable alerts after successfully detecting active devices within the operational range.

Although the system is efficient, the detection is limited to devices that actively transmits RF signals. There are no observable signals from devices that are passive, in airplane mode, or turned off. Performance can also be impacted by environmental factors like RF interference or dense metallic structures.

The system is useful where preventing unauthorized recording or communication is critical. The system provides real time monitoring and helps to enforce privacy and confidentiality policies.

XII. Project Proposal

A. Problem Statement

Hidden cameras significantly jeopardize personal privacy by secretly recording people's activities without their permission and denying them of their privacy. It is very difficult to use current detection methods successfully in real-time because they are frequently too complicated. Moreover they can be limited in scope as they can only identify particular types of devices.

B. Proposed Solution

We propose researching a wireless hidden camera detection system similar to the methods detailed in DeWiCam [5]. After carefully analyzing ten research papers on hidden camera detection methods. DeWiCam [5] demonstrates an optimal balance of detection precision, feasibility of implementation, practicality, and speed.

C. Justification

After reviewing the ten research papers, we found DeWiCam's [5] method to be the most effective solution overall. In terms of both speed and detection accuracy, as well as practicality, DeWiCam [5] consistently outperforms other techniques. While many competing methods require specialized hardware, DeWiCam [5] is practical for everyday use. Its limitation is that it can only detect wireless cameras, though these are also the most common type of hidden cameras. Given the scope and time frame of our project, exploring approaches similar to DeWiCam [5] would provide the most reasonable results.

D. Implementation Plan

The intention is to research a solution using a means that anyone can access. For example, everybody can use this tool via a personal computer (PC).

Our project will focus on implementing and studying the DeWiCam [5] methodology for detecting hidden wireless cameras, with a modification and focus on PC-based environments. Rather than releasing a standalone application, our intention is to carry out a controlled study that demonstrates the feasibility of this approach and evaluates its effectiveness in realistic scenarios. By adapting the ideas presented in the DeWiCam paper [5], our work will replicate the core components of the detection pipeline while simplifying the scope to fit the course project setting.

The first step is to select an appropriate platform. Although DeWiCam [5] was originally developed on smartphones, we will experiment with the method on a PC. This choice makes it better to work with packet capture tools and avoids the complexity of modifying smartphone Wi-Fi drivers. To collect wireless traffic, the PC will be equipped with a USB Wi-Fi adapter that supports monitor mode. Monitor mode allows the system to passively capture all packets in the surrounding area without needing to connect to the network, which is essential for identifying hidden devices. Tools such as `tcpdump` will be used to gather packet traces for further analysis.

Once data has been collected, the next stage involves grouping packets into flows based on their source and destination addresses. The idea is to distinguish between ordinary devices such as laptops or phones and suspicious devices that generate continuous video streams. Flows that clearly do not resemble cameras, for example those dominated by downloads or large file transfers, will be filtered out. The remaining candidate flows will then be studied in more detail.

From each candidate flow, we will extract features that highlight the unique patterns of wireless cameras. The DeWiCam study [5] identified several traffic characteristics that are particularly useful, such as the mixture of large and small packets caused by video compression, the relatively steady bandwidth usage of cameras, and small variations tied to the underlying hardware. By capturing these features at a high level, our system can build a profile of each flow and compare it against known patterns of camera behavior.

To determine whether a flow truly corresponds to a hidden camera, we will employ a supervised learning model trained on labeled examples During testing, the classifier will analyze the extracted features from new flows and output whether a camera is likely present. While DeWiCam [5] uses smartphone sensors for this, our study will instead simulate the effect by logging motion manually and observing how traffic reacts when someone moves in front of the camera. If bit rate fluctuations consistently match periods of movement, we can infer that the camera is likely in the same room. An overview illustration of the concept can be show in Figure 1 below:

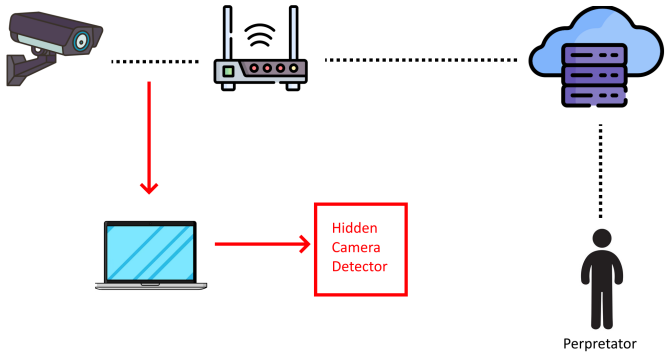

Fig. 1. *Overview of the Concept of the Project*

Finally, the system will be evaluated in controlled environments such as lab rooms or apartments. We will test with different types of devices, including commercial wireless cameras and ordinary networked equipment, to measure detection accuracy and false alarm rates. Scenarios with multiple devices and varying levels of network congestion will also be considered. The goal is not to create a deployable application, but to provide an informative study of how well the DeWiCam method performs when adapted to a PC-based setting, and to highlight its strengths and limitations in practice.

E. Conclusion

In conclusion, this project sets out to explore the problem of hidden wireless camera detection by adapting the DeWiCam methodology [5] into a form suitable for a controlled class study. By restricting our experiment to a PC-based environment, we will avoid the hardware and software barriers associated with smartphone-based solutions while retaining the central concepts of flow analysis, feature extraction, and machine learning classification. The project will demonstrate how simple traffic-level features such as packet length patterns and bandwidth stability can be leveraged to distinguish cameras from other wireless devices. Through the use of a supervised model, we will show that reliable detection is possible without large datasets or complex infrastructure.

REFERENCES

[1] H. Chen, R. Zhou, C. Yan, X. Ji, and W. Xu, "Camdetector: Detecting and positioning hidden cameras with raspberry pi 4 via em radiation," in *2023 IEEE 7th Conference on Energy Internet and Energy System Integration (EI2)*, 2023, pp. 3597–3602.

[2] S. Sami, S. R. X. Tan, B. Sun, and J. Han, "On utilizing smartphone time-of-flight sensors to detect hidden spy cameras," in *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems*, ser. SenSys '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 384–385. [Online]. Available: https://doi.org/10.1145/3485730.3493371

[3] Y. Gu, J. Chen, C. Wu, K. He, Z. Zhao, and R. Du, "Loccams: An efficient and robust approach for detecting and localizing hidden wireless cameras via commodity devices," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 7, no. 4, Jan. 2024. [Online]. Available: https://doi.org/10.1145/3631432

[4] J. Lee, S. Seo, T. Yang, and S. Park, "Ai-aided hidden camera detection and localization based on raw iot network traffic," in *2022 IEEE 47th Conference on Local Computer Networks (LCN)*, 2022, pp. 315–318.

[5] Y. Cheng, X. Ji, T. Lu, and W. Xu, "Dewicam: Detecting hidden wireless cameras via smartphones," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, ser. ASIACCS '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 1–13. [Online]. Available: https://doi.org/10.1145/3196494.3196509

[6] Z. Liu, F. Lin, C. Wang, Y. Shen, Z. Ba, L. Lu, W. Xu, and K. Ren, "Camradar: Hidden camera detection leveraging amplitude-modulated sensor images embedded in electromagnetic emanations," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 6, no. 4, Jan. 2023. [Online]. Available: https://doi.org/10.1145/3569505

[7] Z. Yu, Z. Li, Y. Chang, S. Fong, J. Liu, and N. Zhang, "Heatdecam: Detecting hidden spy cameras via thermal emissions," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 3107–3120. [Online]. Available: https://doi.org/10.1145/3548606.3560669

[8] G. Menaka and C. Bharani, "Hidden camera detector using magnetometer and accelerometer sensor," *Journal of Multidimensional Research and Review (JMRR)*, vol. 6, no. 1, pp. 70–79, 2025. [Online]. Available: http://www.jmrr.org

[9] J. Heo, S. Gil, Y. Jung, J. Kim, D. Kim, W. Park, Y. Kim, K. G. Shin, and C.-H. Lee, "Are there wireless hidden cameras spying on me?" in *Proceedings of the 38th Annual Computer Security Applications Conference*, ser. ACSAC '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 714–726. [Online]. Available: https://doi.org/10.1145/3564625.3564632

[10] N. Gayathri and T. Sivasakthi, "Presence of active mobile phones and hidden camera detection," *International Journal of Power Control Signal and Computation (IJPCSC)*, vol. 8, no. 1, pp. 61–66, 2016. [Online]. Available: http://www.ijcns.com