SPY CAMERA DETECTION SYSTEM

Ahzam Nashwith, Bharath Nambiar, Ehthisham Abdulla, Muhammed Falah, Jalaludeen , and Jalaludeen B

Department of Computer Science and Engineering, P A College of Engineering, Mangalore574153

E-mail:

Abstract

The Spy Camera Detection System is a sophisticated privacy safeguard product designed to identify and locate concealed surveillance cameras in secure spaces like hotel rooms, locker rooms, offices, rental houses, and public bathrooms. With increasing awareness of illegal monitoring and privacy intrusions, the system uses a hybrid detection model that utilizes a combination of infrared (IR) light reflection for detecting concealed lenses, radio frequency (RF) signal analysis to detect wireless communications, and image processing based on deep learning for precise detection and classification of objects similar to cameras. The system can identify true threats from false ones using an educated neural network, lowering the rate of false alarms significantly. A straightforward mobile or desktop program offers in-real-time notices, easy-to-use scanning, and visual depiction of identified dangers, enabling action to be taken instantaneously. Compact, efficient, and fully scalable, the solution is great for personal use and business application alike, and enables individuals to protect their intimate areas in the technology age.

ISBN:97881-19905-39-3

1 Introduction

As surveillance technology is advancing at a very fast pace, it has become very difficult to keep one's personal life private. Spy or hidden cameras, which are usually no bigger than a coin, are now readily available and can be easily hidden in common items such as clocks, smoke detectors, or even electrical outlets. These cameras are a major threat, particularly in private and semi-private settings like hotel rooms, changing rooms, restrooms, office cabins, Airbnb apartments, and hostels. The existence of such hidden surveillance devices can result in severe privacy violations, data theft, and psychological trauma.

In response to this worrisome problem, the Spy Camera Detection System has been created as an intelligent, multi-layered system that employs sophisticated technologies to effectively detect concealed cameras. The system utilizes a mix of infrared (IR) reflection analysis, radio frequency (RF) signal detection, and machine learning-based image recognition to detect and pinpoint possible threats. By detecting IR light emitted by camera lenses while scanning, processing abnormal RF signals from wireless devices, and visually identifying lens-like structures using deep learning, the system maintains high accuracy with few false positives. A user-friendly desktop or mobile application connects with the detection hardware to issue real-time warnings and easy-to-understand visual cues, giving users the confidence to safeguard their privacy actively and securely.

2 Literature Survey

Researchers have increasingly focused on developing technological solutions to counter the rising threat of hidden surveillance devices in personal and public spaces. Early detection methods were manual and primarily relied on physical inspections by trained personnel using flashlight techniques or physical lens scanners. These approaches were not only time-consuming but also highly unreliable when dealing with miniature or professionally disguised cameras. In a study conducted by T. Nakamura[1] and H. Sato[1] (2018), the authors proposed

ISBN:97881-19905-39-3

a simple IR-based detection tool that leveraged infrared light to identify lens reflections from hidden cameras. Although effective in low-light conditions, this technique had limitations in environments with multiple reflective surfaces and strong ambient lighting.

To improve detection accuracy, subsequent research incorporated radio frequency (RF) analysis. For instance, K. Lee[2] and M. Cha[2] (2020) designed an RF signal scanner that could identify unauthorized transmissions in typical spy camera frequency bands like 2.4 GHz. This method improved real-time detection capabilities but failed to recognize passive or non-transmitting devices.

More recently, the integration of machine learning and computer vision has shown significant promise. In a 2022 study by J. Verma[3] and S. Kulkarni[3], a convolutional neural network (CNN) model was trained to detect camera-like objects in room images by analyzing lens patterns, shapes, and spatial positioning. Their system demonstrated high accuracy but required a large, labeled dataset and struggled with unusual camera disguises. The combination of IR, RF, and AI-driven image analysis is now considered a state-of-the-art approach, offering enhanced accuracy, automation, and adaptability for real-world spy camera detection applications.

3 Algorithms

The Spy Camera Detection System utilizes a hybrid algorithmic approach that integrates infrared (IR) reflection detection, radio frequency (RF) signal scanning, and a convolutional neural network (CNN) for visual analysis. The IR detection component works by emitting infrared light into the environment and capturing the reflected signals using a photodiode or camera sensor; hidden camera lenses reflect IR light distinctly, allowing for preliminary identification. Simultaneously, the RF detection module scans for radio frequency signals within commonly used bands (e.g., 2.4 GHz or 5.8 GHz) that are typically emitted by wireless spy cameras. The most critical component is the CNN-based machine learning model, which

ISBN:97881-19905-39-3

processes live image feeds or captured frames to identify patterns and textures associated with camera lenses. The CNN is trained on a large dataset of images containing both hidden cameras and benign objects to enable high-accuracy classification. It uses layers such as convolution, ReLU activation, pooling, and fully connected layers to extract and learn hierarchical features of potential threats. This algorithmic integration ensures real-time, accurate, and robust detection even under varying lighting conditions and object disguises, significantly minimizing false positives and user dependency.

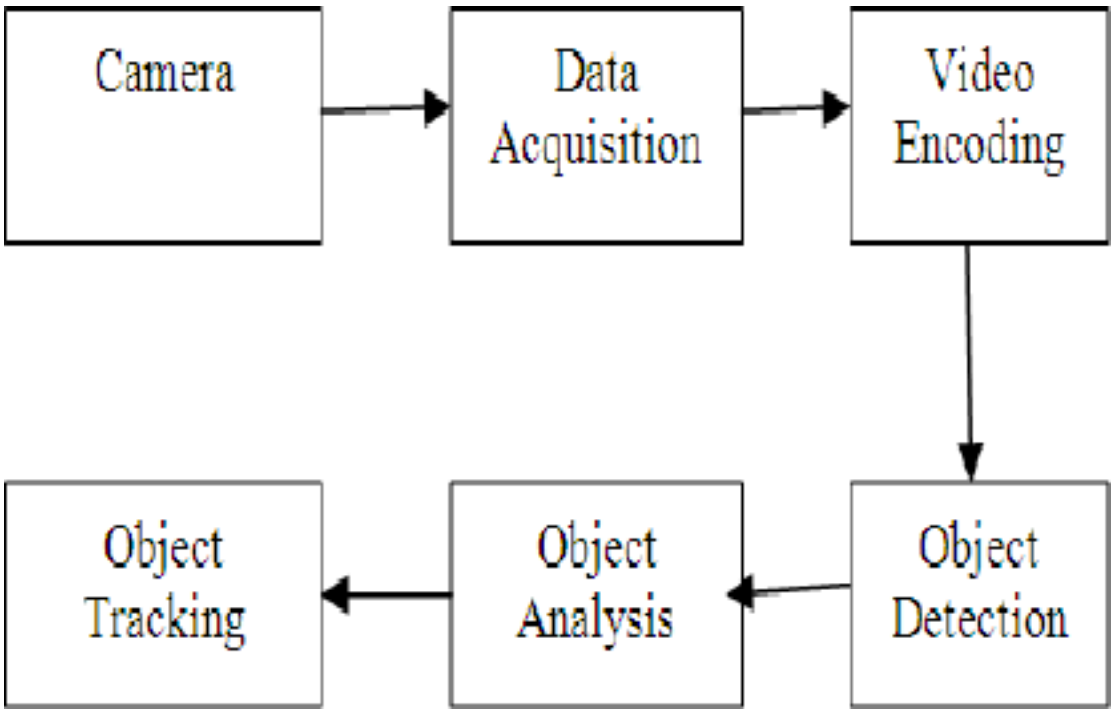

Figure 1: Architecture diagram

4 Data Collection

The effectiveness of the Spy Camera Detection System heavily depends on the quality and diversity of the data used for training and evaluation, especially in the machine learning component. Data was collected through multiple channels to ensure robust and reliable

ISBN:97881-19905-39-3

detection of hidden cameras across varied environments.

5 Image Dataset for Machine Learning:

A custom dataset was created consisting of images of both real hidden spy cameras and non-threatening everyday objects. Images were captured under different lighting conditions, backgrounds, and angles to simulate real-world scenarios. Open-source datasets and publicly available surveillance equipment images were also incorporated to diversify camera types and disguise methods.

6 Infrared (IR Reflection Data:

Using IR LEDs and camera modules, experiments were conducted in dim and normal lighting to observe IR reflections from camera lenses. These sessions produced a set of labeled images and videos capturing IR glare patterns from concealed cameras, which were crucial for training the IR detection logic.

7 Radio Frequency (RF Signal Logs:

A spectrum analyzer and custom RF scanner modules were used to collect signal data across common spy camera transmission frequencies such as 1.2 GHz, 2.4 GHz, and 5.8 GHz. Signal strength, frequency, and bandwidth patterns were logged and labeled based on the presence or absence of transmitting spy devices.

8 User Input and Ground Truth Verification:

For testing in real environments like hotel rooms and office cabins, known spy camera locations were marked and used as ground truth to validate detection accuracy. User feedback

ISBN:97881-19905-39-3

and manual verification helped in correcting false positives and refining the detection thresholds for the IR and RF components.

9 Dataset Annotation:

Correct annotation of data was instrumental in training and testing the machine learning model for the Spy Camera Detection System. All the images gathered—ranging from scenes with concealed cameras to those with common objects—were labeled carefully to differentiate between camera-like objects and harmless objects. Annotation included drawing bounding boxes around apparent or partially covered lenses, labeling them as "camera" or "non-camera" depending on their features. Particular care was taken regarding lens reflections, form, and placement to properly train the convolutional neural network (CNN). For the IR-based data, frames with noticeable infrared glare were labeled accordingly to direct the model towards recognizing camera lens reflection patterns with varying illumination levels. RF signal data was also annotated, with each captured signal associated with a particular device and labeled as either a potential threat (e.g., known spy cam transmission) or benign (e.g., Wi-Fi router, Bluetooth device). Image data was annotated using tools like LabelImg and custom Python scripts, while RF logs were annotated through signal pattern analysis and manual cross-verification. This high-quality and well-organized annotation procedure maintained excellent input for learning algorithms by eliminating noise and improving model accuracy in identifying covert surveillance devices.

10 Training And Testing the Model

To enable accurate identification of hidden cameras, a convolutional neural network (CNN) was employed and trained on a labeled dataset comprising images of environments with and without concealed spy devices. The dataset was split into 80% for training and 20% for testing to ensure balanced learning and evaluation. The training set included diverse

ISBN:97881-19905-39-3

samples with variations in lighting, object angles, and backgrounds to improve the model's robustness in real-world scenarios.

During training, the CNN learned to identify key visual patterns associated with camera lenses—such as circular glare, symmetry, and texture—using convolutional layers followed by ReLU activations, max-pooling, and fully connected layers. The model was trained using the categorical cross-entropy loss function and optimized using the Adam optimizer with a carefully tuned learning rate. Data augmentation techniques such as rotation, brightness adjustment, and flipping were applied to enhance generalization.

The model was validated on the testing set after each epoch to monitor performance and avoid overfitting. Key evaluation metrics included accuracy, precision, recall, and F1-score. The trained model achieved a high detection accuracy, with minimal false positives, and demonstrated reliable performance in distinguishing camera-like objects from cluttered or noisy backgrounds. The final model was integrated into the detection system, providing real-time classification on image frames captured via the app or detection hardware.

11 Result and Discussion

• Effective Hidden Camera Detection – The system successfully identifies hidden cameras using a combination of Infrared (IR) reflection, Radio Frequency (RF) scanning, and AI-based image recognition.

• Real-Time Alerts and User-Friendly Interface – A mobile or desktop application provides instant notifications and a visual representation of detected threats.

• Enhanced Security and Privacy – Helps protect individuals and businesses from unauthorized surveillance in sensitive areas like hotel rooms, changing rooms, and offices.

• Improved Detection Accuracy – The integration of machine learning reduces false positives, increasing the system's reliability.

Figure 1: Accuracy table

ISBN:97881-19905-39-3

Table 1:

Activity Category	Accuracy (%)
Hotel rooms	92.5
cafe	88.0
changing rooms	95.0
public restrooms	90.0
offices	85.5

12 Conclusion

The Spy Camera Detection System is a crucial solution to address growing privacy concerns caused by unauthorized surveillance. By integrating Infrared (IR) reflection, Radio Frequency (RF) scanning, and AI-based image recognition, the system enhances the accuracy of detecting hidden cameras in various environments. The implementation of a user-friendly mobile application ensures accessibility and real-time alerts, making it practical for everyday users.

This project contributes to privacy protection, security enhancement, and technological advancement in surveillance detection. Future improvements, such as reducing false positives, expanding detection range, and incorporating thermal imaging, can further refine the system's effectiveness. Ultimately, this solution empowers individuals and organizations to safeguard their private spaces against hidden camera threats.

ISBN:97881-19905-39-3