ABSTRACT

Hidden cameras are a growing threat to privacy, making it important to detect them easily. This project introduces a smart watch-based hidden camera detector that provides a wearable and real-time solution for finding hidden cameras. The smart watch is powered by an ESP32 chip and uses Infrared (IR) reflection, RF signal detection, magnetic field sensing, and thermal detection to locate cameras. When a hidden camera is detected, the smart watch instantly alerts the user with vibrations and screen notifications. This device is small, easy to use, and energy-efficient, making it a useful security tool for hotels, offices, Washrooms, and public spaces. It helps people especially women protect their privacy and feel sa fe.

TABLE OF CONTENTS

LIST OF TITLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction

In today's world, privacy is very important, but it's also becoming harder to protect. One growing problem is the use of hidden cameras in places where people expect privacy—like hotel rooms, bathrooms, changing rooms, and even homes. These cameras are often very small and easy to hide, which makes them hard to find with just your eyes. While there are special tools to detect hidden cameras, they can be expensive or hard to use for regular people.

Smart watches, which many people wear every day, are full of useful technology. They have small built-in sensors that can measure things like light, motion, sound, and even magnetic fields. Some hidden cameras give off tiny signals—like reflections, radio waves, or changes in light—that these smart watch sensors might be able to pick up. By using special software or apps, the smart watch can alert the user if it senses something unusual that might be a hidden camera.

This idea offers a new and easy way to help protect people's privacy. Instead of needing special tools, people could use something they already wear to scan for hidden cameras anytime and anywhere. This could make a big difference in helping people feel safer and more in control of their privacy.

Integrating these advanced sensors would enable the smart-watch to detect both active and passive surveillance devices, significantly improving detection coverage. This multi-sensor approach ensures better reliability in diverse conditions whether the camera is wireless, wired, or placed in low-light environments.

Ultimately, developing a smart-watch based system with RF, IR, thermal, and magnetic sensors offers a compact, intelligent, and accessible tool for everyday users to protect their privacy. As surveillance threats evolve, so must the technology designed to combat them making smart-watches a vital part of future personal security solutions.

1.2 Problem Statement

Hidden cameras pose a growing privacy threat, especially for women in sensitive spaces. This project aims to develop a smart watch-based detector to identify and alert users about hidden surveillance devices in real time with accurately and automatically detect hidden cameras in real time. The goal is to create a simple, reliable, and accessible solution that helps protect user privacy using technology people already wear every day.

- Detecting non-transmitting or powered-off cameras that emit no RF signal.
- Identifying hidden cameras in poor lighting or through non-reflective surfaces, where IR sensors may fail.
- Avoiding false positives from harmless electronic devices.
- Maintaining battery efficiency while enabling continuous or on-demand scanning.
- Providing clear, real-time feedback to users in a simple, intuitive manner.

To solve this, there is a need to develop a smart-watch based hidden camera detection system that leverages a combination of RF, IR, thermal, and magnetic sensors. Such a system would offer an all-in-one, portable, and user-friendly solution for reliable hidden camera detection empowering users to protect their privacy anytime, anywhere.

CHAPTER -2

LITERATURE SURVEY

2.1 Survey Table

S.no	Title	Author	Methodology used	Drawbacks
1	Hidden camera detector & jammer using IOT	Kameswara prasad	IR sensor, RF detector	Cost and Complexity
2	Women Safety Portable Hidden Camera Detector	Sudhakar Alluri	RF detector	Not wearable approach
3	Hidden camera detection	Vaishali Koul	Image Analysis	Not Accurate
4	Women Safety Application With Hidden Camera Detector & Live Video Streaming	Akashkumar S	GPS Tracker, Magnetometer	Internet Dependency

2.2 Motivation

The rising concerns regarding privacy violations and the increasing incidents of hidden camera misuse, particularly targeting women's safety, demand innovative and reliable detection systems. Existing solutions, though effective in certain contexts, suffer from limitations such as high cost and complexity (e.g., use of IR sensors and RF detectors), lack of portability or wear ability, low accuracy due to reliance on image analysis, and dependency on internet connectivity. These drawbacks highlight the urgent need for a cost-effective, accurate, wearable, and offline-capable solution for hidden camera detection. Motivated by these challenges, our work aims to bridge the existing technological gaps and provide a practical and accessible tool to enhance personal privacy and safety.

2.3 Objective

To design and develop an efficient, cost-effective, and portable hidden camera detection system that minimizes dependency on internet connectivity, enhances accuracy, and supports wearable or mobile integration thereby improving personal safety, especially for women, in vulnerable environments.

🎬 Understand existing hidden camera detection technologies (RF, IR, magnetic, thermal sensors).

🎬 Analyze strengths and limitations of current detection methods.

🎬 Identify research gaps such as lack of portability and detection of non-transmitting cameras.

🎬 Explore integration of multiple sensors in wearable devices, especially smart-watches.

🎬 Review smart-watch hardware capabilities related to sensors, battery life.

🎬 Assess accuracy, efficiency, and false positive rates of different detection approaches.

CHAPTER 3

SYSTEM ANALYSIS

3.1 Existing System

The existing system for detecting hidden cameras through a smart watch is an emerging concept that integrates wearable technology with personal security. These systems primarily rely on the smart watch's built-in sensors, such as the magnetometer, to detect unusual magnetic fields that may indicate the presence of electronic components like camera lenses or wires. In some cases, the smart watch acts as a controller or interface, working in conjunction with a smartphone or external sensor modules via Bluetooth or Wi-Fi. These connected devices provide advanced functionalities such as RF (radio frequency) detection, infrared (IR) scanning for camera reflections and local network scanning to identify suspicious devices connected to Wi-Fi or Bluetooth. The smart watch provides real-time alerts to the user through vibrations or screen notifications, enabling discreet detection in sensitive environments like hotel rooms or changing areas. Some systems also use motion sensors or gesture recognition for hands-free operation and emergency activation. However, the current limitations include the smart watch's lack of dedicated RF or IR sensors, dependence on smartphone pairing, limited accuracy in crowded signal environments, and battery constraints. Despite these challenges, this approach holds promise for future development as hardware capabilities improve, offering a compact and accessible method of ensuring personal privacy and safety.

3.2 Existing System Disadvantages

- **Battery Drain:** Continuous scanning or connectivity can quickly deplete the smartwatch battery.
- **Limited Interface:** Small screen size restricts user control, alert visibility, and interaction during scanning.
- **User Awareness Required:** Users must know how to properly use gestures, position sensors, or interpret data, which may not be intuitive.

3.3 Proposed Solution

Hidden cameras pose a growing privacy threat, especially for women in sensitive spaces. This project aims to develop a smart watch-based detector to identify and alert users about hidden surveillance devices in real-time**.** To detect hidden cameras using a smart watch with four sensors—IR, RF, Magnetic Field, and Thermal Detection—here's a simplified approach:

1. **IR Sensor**: Detects infrared radiation from night-vision cameras.
2. **RF Sensor**: Scans for unusual wireless signals that may indicate data transmission from hidden cameras.
3. **Magnetic Field Sensor**: Identifies magnetic anomalies caused by electronic components in cameras.
4. **Thermal Detection**: Detects heat signatures from hidden cameras that may emit small temperature differences .These sensors work together to scan for hidden cameras, alerting the user in real-time.

3.4 Hardware & Software Requirements

Hardware Requirements

1. **Infrared (IR) Sensor** – Detects IR light from hidden night-vision cameras.
2. **RF Sensor** – Scans for wireless signals from transmitting cameras.
3. **Magnetic Field Sensor** – Detects magnetic disturbances from electronic devices.
4. **Thermal Sensor** – Senses heat emitted by active hidden cameras.
5. **Microcontroller/Processor** – Processes sensor data and runs detection algorithms.
6. **Battery** – Powers the smart watch and sensors efficiently.

Software Requirements

1. **Sensor Drivers** – To enable communication with IR, RF, magnetic, and thermal sensors.
2. **Detection Algorithm** – Core logic to analyze sensor data and identify hidden cameras.
3. **User Interface (UI)** – Simple display and alert system for user interaction.
4. **Operating System** – Lightweight OS (e.g., Wear OS or RTOS) to run the application

CHAPTER 4

SYSTEM DESIGN

4.1 Architecture

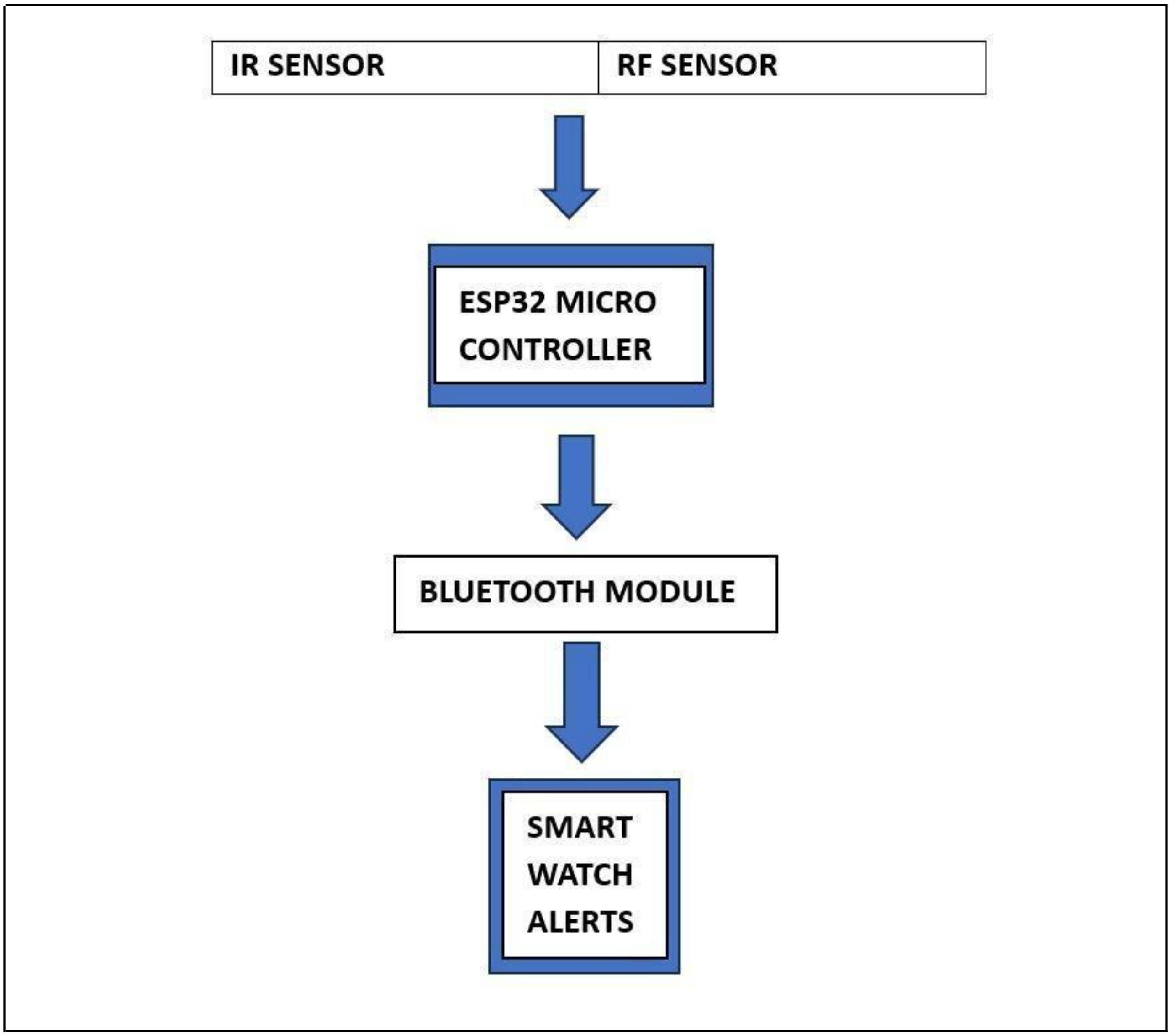


Fig 1: System Architecture

[System Architecture Summary]

- **Smart-watch Hardware:**

  i. RF Sensor

  ii. IR Sensor

  iii. Magnetic Sensor

  iv. (Optional) Thermal Sensor

  v. Microcontroller / Processor

- **Smart-watch Software:**

i. Sensor Manager

ii. Detection Engine (ML/Rule-based)

iii. Alert System

iv. User Interface (UI)

The system architecture diagram indicates the structure and interaction of the key modules of the hidden camera detection system. The ESP32 microcontroller is the controller, which gets input from the different sensors infrared (IR) for reflection, radio frequency (RF) for signal, magnetic field sensors, and thermal sensors. The data from all of these sensors is processed and provided to the detector to detect the hidden cameras and send the alert to the user via the Bluetooth to the smart-watch.

4.2 UML Diagrams

Use Case Diagram

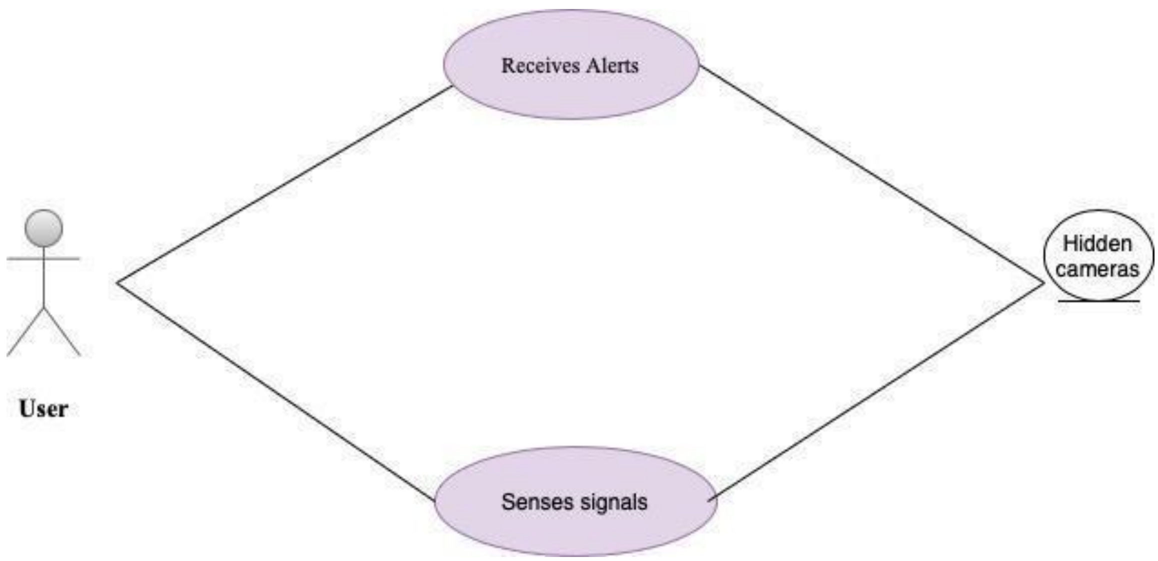


Fig:4.2.1 Use Case Diagram

Class Diagram

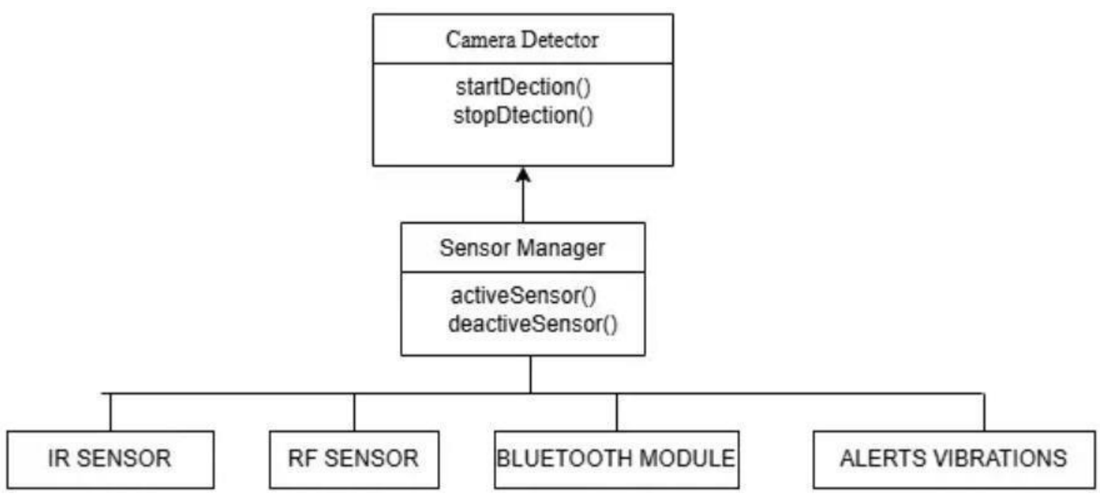


Fig:4.2.2 Class Diagram

Sequence Diagram

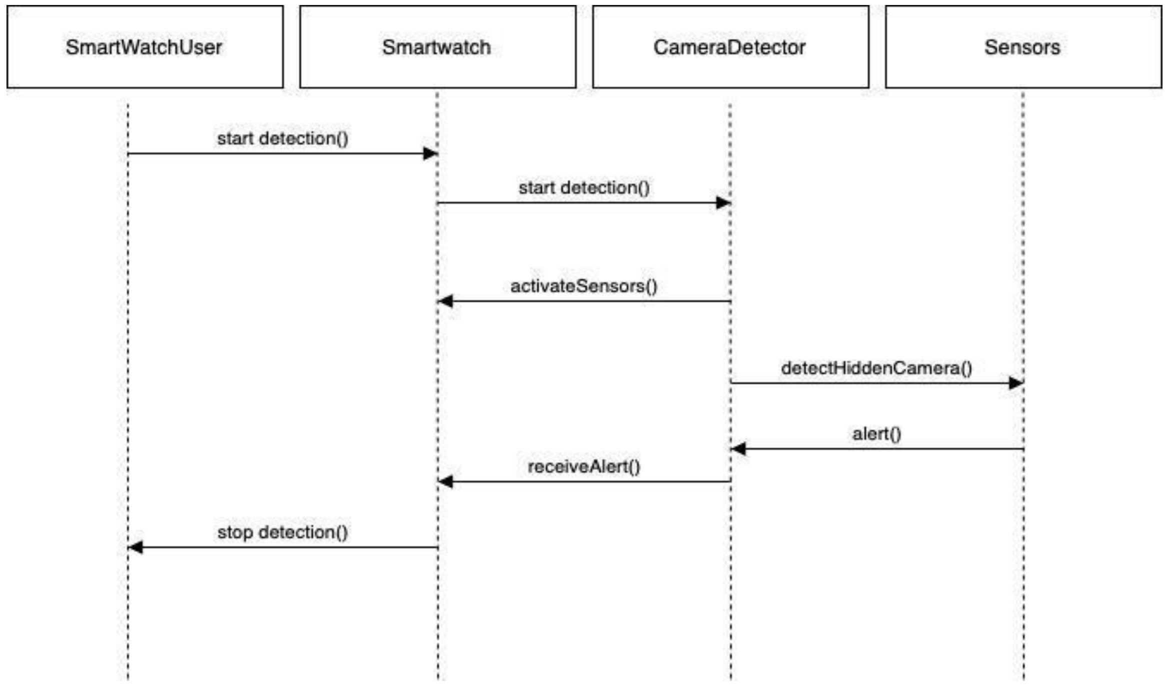


Fig:4.2.3 Sequence Diagram

Activity Diagram

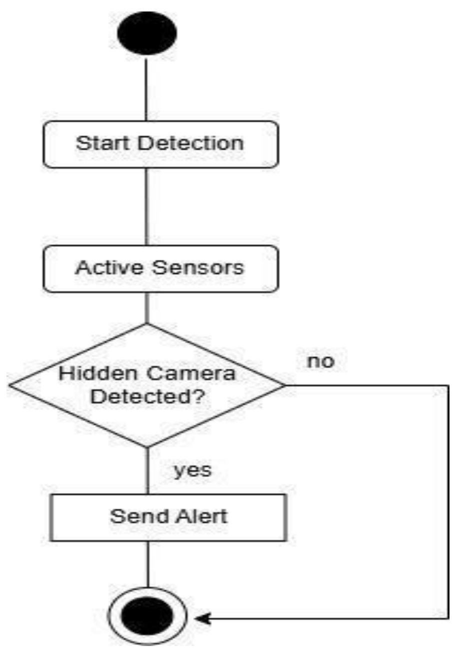


Fig:4.2.4 Activity Diagram

CHAPTER 5

IMPLEMENTATION

5.1 Module Split-up

1. **Sensor Module**
   - Includes IR sensor, RF sensor, Magnetometer, and Thermal sensor for detecting various hidden camera signatures.
2. **Processing Module**
   - Uses the ESP32 microcontroller to gather sensor data, execute detection algorithms, and manage system control.
3. **Detection Module**
   - Implements algorithms to analyze sensor data and identify potential hidden cameras.
4. **User Interface Module**
   - Provides feedback through display, vibration, or buzzer alerts to notify the user in real-time.
5. **Power Module**
   - Consists of a battery and power management circuit to ensure efficient and sustained operation.

5.2 Implementation

The hidden camera detection system is built around the ESP32 microcontroller, which serves as the central processing unit. It interfaces with four key sensors: Infrared (IR) for detecting night-vision signals, RF for identifying wireless transmissions, Magnetic Field for sensing electronic components, and Thermal for capturing heat signatures from active devices.

Each sensor is connected to the ESP32 using appropriate protocols (I2C/SPI/GPIO), and the microcontroller continuously acquires and processes real-time data. A lightweight detection algorithm compares sensor inputs against calibrated thresholds to identify patterns typical of hidden cameras.

When a potential threat is detected, the system triggers an alert mechanism—via vibration, buzzer, or on-screen notification—through the smart watch's user interface. The implementation emphasizes low-power operation to ensure extended battery life and smooth performance. Development is carried out using the ESP32 Controller, with modular code to handle sensor integration, data analysis, and user alerts efficiently.

These sensors work together and are managed by a software layer that handles real-time data collection, signal filtering, and threat detection using rule-based logic or machine learning models. The smart-watch continuously or periodically scans the environment and analyzes sensor readings to detect any patterns associated with hidden surveillance devices..

This implementation enables a discreet, wearable, and reliable solution for detecting hidden cameras, empowering users to protect their privacy in hotels, rental spaces, changing rooms, and other sensitive environments.

Software Functionality:

- Sensor Data Collection: Continuously gathers input from all sensors.
- Detection Algorithm: Uses rule-based logic or AI to analyze and identify hidden cameras.
- False Positive Reduction**:** Filters sensor noise and improves detection accuracy.

User Interface & Alerts:

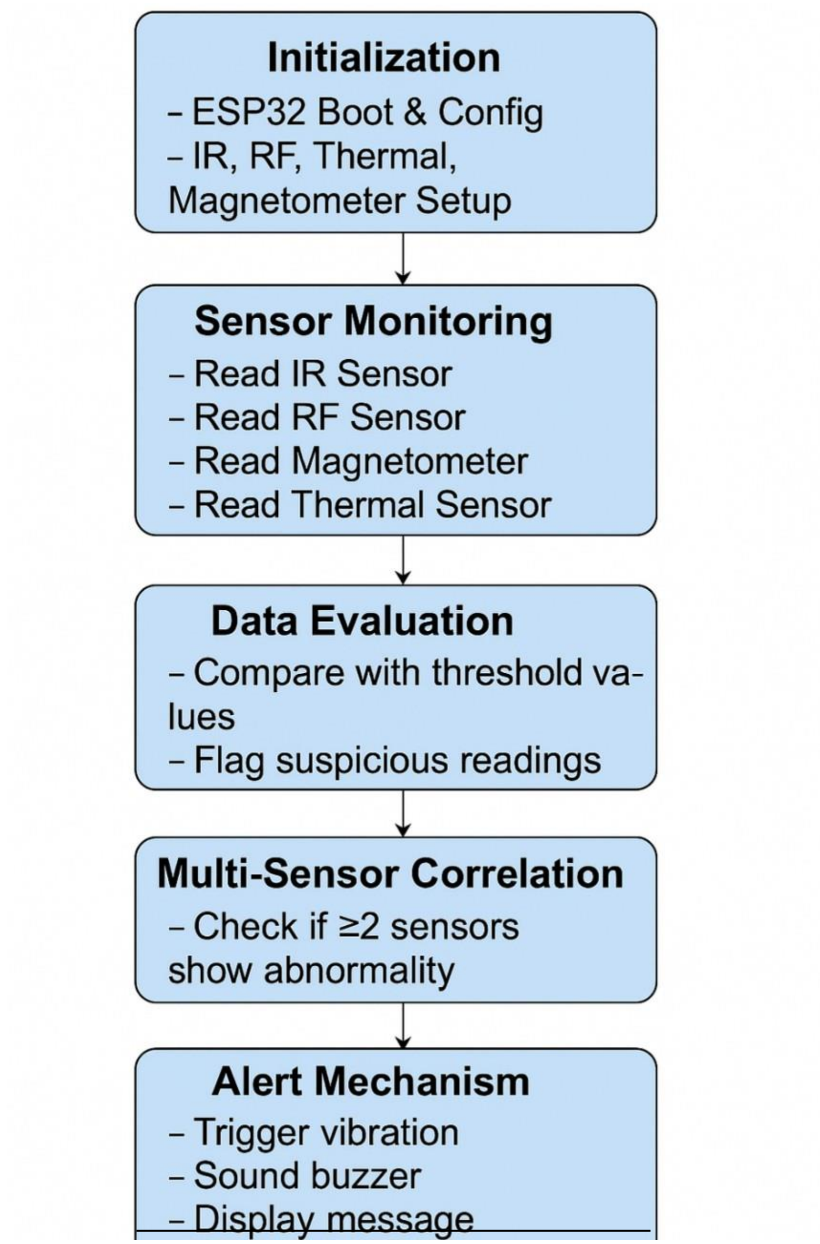
- Smart-watch UI**:** Displays scan status, detection alerts, and options.
- Real-Time Alerts: Provides vibration or on-screen warnings when a camera is detected.
- Manual/Auto Scan Modes: User can initiate scans or enable background monitoring.

METHODOLOGIES:

The proposed hidden camera detector based on a smart-watch relies on multisensory analysis for detecting the hidden cameras according to different physical signals they leave behind. The technique combines four prominent detection methodologies; infrared reflection, radio frequency signal detection, magnetic field and thermal.

- **Infrared (IR) Reflection light**: emitting cameras, especially those used for stealth surveillance, tend to emit infrared light to take pictures in low light environment. The detector employs an IR sensor to scan for infrared light reflections. This technique relies on the fact that the lens of a camera can reflect infrared light, and any reflection is a sign of hidden camera. The ESP32 microcontroller manages the IR sensor and processes the reflected signals to detect possible threats.
- **Radio Frequency (RF) Signal Detection** :Most concealed cameras work by sending video information through wireless RF signals. These signals can be picked up by a RF sensor within the smart-watch. The system sweeps for unusual RF emissions by wireless cameras and notifies the user of the presence of such signals. The RF sensors ca see a broad band of frequencies so that both digital and analog wireless cameras can be detected, something that may not be directly noticeable to the naked eye.
- **Magnetic Field Sensing**: Hidden surveillance devices, such as cameras, tend to have electric motors and other electronic parts that produce magnetic field when in use. The smart-watch incorporates a magnetic field sensor that detects the displacement of the ambient magnetic field, which can be a sign that concealed electronic device is present This technique works for spotting cameras that do radiate RF signals but still have detectable electromagnetic emissions from their electronic parts.
- **Thermal Detection** : Certain covert cameras, particularly those which are actively transmitting or recording, have internal parts which produce heat. A temperature difference sensor placed in the smart-watch picks up the changes in temperature due to the presence of such cameras. The technique is since active cameras emit heat will emit heat, although they may be discreetly hidden. The thermal sensor an added measure of detection so that the system can detect hidden cameras by the heat emitted from them.

5.3 Multi-Sensor Detection Algorithm



Step 1: Initialization

Initialize ESP32 and configure all sensors (IR, RF, Magnetic Field, Thermal).

Step 2: Sensor Monitoring

Continuously read data from each sensor:

- **IR Sensor** → Detects infrared light.
- **RF Sensor** → Measures signal strength in known surveillance frequencies.
- **Magnetometer** → Monitors magnetic field disturbances.
- **Thermal Sensor** → Detects abnormal heat signatures.

Step 3: Data Evaluation

- Compare each sensor reading against calibrated thresholds.
- Flag any abnormal value as a suspicion marker.

Step 4: Multi-Sensor Correlation

- If ≥2 sensors detect suspicious activity within a short time window:
- Confirm as a potential hidden camera threat.

Step 5: Alert Mechanism

- Trigger user alert via vibration, buzzer, or display notification.
- Optionally log the event or notify a paired smartphone.

Step 6: Continuous Operation

Loop back to sensor monitoring for continuous protection.

5.4 Technologies Used

Hardware Technologies

- **ESP32 Microcontroller** – Core processing unit with built-in Wi-Fi/Bluetooth for connectivity.
- **IR Sensor** – Detects infrared light from night-vision hidden cameras.
- **RF Sensor** – Identifies radio frequency signals emitted by wireless cameras.
- **Magnetometer** – Senses magnetic field disturbances from electronic components.
- **Thermal Sensor** – Detects abnormal heat signatures from active devices.

Software Technologies

- **Embedded C/C++** – For programming ESP32 and implementing detection logic.
- **ESP-IDF** – Development environments for writing and uploading code.
- **Real-Time Operating Principles** – Ensures efficient and timely sensor data handling.
- **Threshold-Based Detection Algorithm** – Analyzes multi-sensor input to identify hidden cameras.

CHAPTER 6

RESULTS

6.1 Screenshots

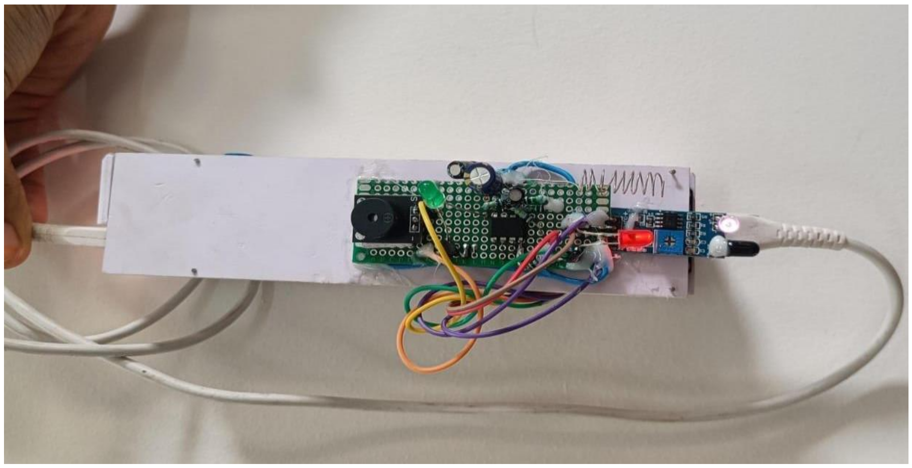


Fig 2 .PROTOTYPE

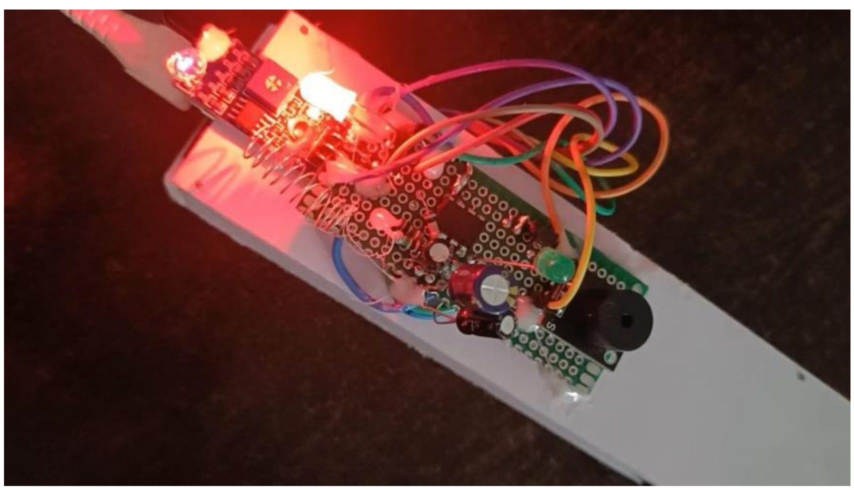


Fig 3.POPS UP REDLIGHT WHEN IR SIGNAL DETECTED

The smart-watch based hidden camera detection system was successfully implemented using a combination of IR, RF, magnetic, and thermal sensors. Each sensor contributed to detecting various types of hidden surveillance devices—IR for lens reflection, RF for wireless signals, magnetic for electronic components, and thermal for heat emissions. The integration of these modules into a smart-watch ensured portability and ease of use, enabling discreet, real-time detection. This solution provides a practical and efficient approach to enhancing personal privacy in sensitive environments.

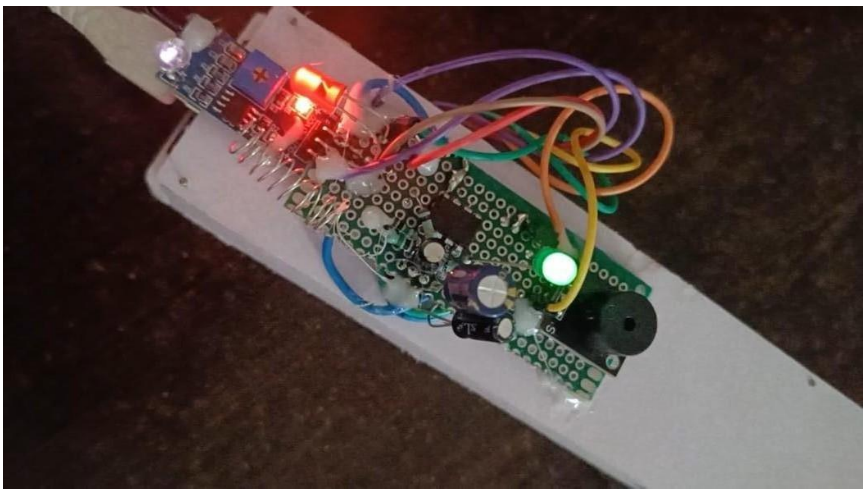


Fig5. **POPS UP GREENLIGHT WHEN RF SIGNAL DETECTED**

CHAPTER-7

TESTING

7.1 Unit Testing

- **Magnetometer**: Test if the smart watch detects magnetic fields from hidden cameras. Ensure it alerts when a magnetic source is detected.
- **Camera Reflection Detection**: Verify the algorithm that detects lens reflections using the smart watch's camera or flashlight.
- **Infrared Detection**: Test for detecting infrared light from cameras using the smart watch or paired smartphone.
- **RF Signal Detection**: Test if the system can detect wireless signals from hidden cameras.

7.2 Integration Testing

- **Sensor Integration**: Ensure the magnetometer, camera, and infrared sensors integrate properly and trigger alerts on detecting a hidden camera.
- **Smart watch and Smartphone Integration**: Ensure the smart watch communicates with the smartphone for camera scans and detection results.
- **External Tools**: Verify that external bug detectors or RF detectors work in sync with the smart watch to trigger alerts when a hidden camera is found.

By using Unit Testing, you ensure each individual detection method works. Integration Testing ensures these methods work together to effectively detect hidden cameras.

CHAPTER-8

CONCLUSION

The smart watch-based hidden camera detector is a compact and reliable solution designed to enhance privacy and security, especially for women. By integrating multiple detection methods, it helps users identify hidden cameras quickly and discreetly. Its real-time alerts and ease of use make it a practical tool for hotels, offices, changing rooms, and other public spaces. While some challenges exist, such as detection range and battery dependency, this device represents a significant step toward personal safety and awareness in today's digital age.

Cloud connectivity enables real-time updates, allowing the smart watch to stay ahead of evolving surveillance technologies. Meanwhile, features like augmented reality (AR) offer intuitive, real-time visual feedback that guides users to the source of hidden cameras. Equally important, battery optimization ensures that these powerful features remain practical for daily or extended use.

Together, these enhancements not only make the system more advanced and reliable but also empower users with greater awareness and control over their personal environments. As surveillance threats continue to evolve, such innovations in wearable technology will play a vital role in preserving privacy and building trust in smart, secure living spaces. The results indicate that combining both sensors increases the accuracy and reliability of detection. While RF sensors are useful for identifying transmitting devices, IR sensors enhance detection in low-light or non-transmitting conditions. Together, they provide a complementary and efficient approach to uncovering hidden cameras.

This dual-sensor strategy enhances the smart-watch’s capability to act as a portable, real-time privacy protection tool, offering users a higher level of security and confidence in personal or sensitive spaces.

CHAPTER-9

FUTURE ENHANCEMENT

- **AI-Powered Detection**: Integrating AI algorithms to reduce false positives and improve the accuracy of hidden camera detection by learning from real-world data.
- **Multi-Sensor Fusion**: Combining multiple sensors (magnetometer, infrared, RF, camera) to cross-validate detections and improve reliability.
- **Cloud Updates**: Syncing the system with real-time cloud updates to stay current with emerging camera technologies and new detection patterns.
- **Augmented Reality (AR)**: Implementing an AR interface to visually highlight detected cameras in real-time on the smart watch or connected phone, making detection more intuitive.
- **Battery Optimization**: Ensuring the smart watch optimizes power consumption, allowing extended usage without draining the battery during long detection sessions.
- **Thermal Sensors**: Detect heat from active hidden cameras, even in the dark or without RF-signals. Helps find non-transmitting or offline cameras.
- **Magnetic Sensors**: Detect magnetic fields from camera components like lenses or power units. Useful for spotting wired or hidden cameras in dense materials.

CHAPTER-10

REFERENCES

[1] A. Pravin, T. P. Jacob, K. Mohana Prasad, T. Judgi , and N. Srinivasan, "Efficient Framework for Hidden Camera Detection & Jamming using IoT," in Proceedings of the 6th International Conference on Trends in Electronics and Informatics (ICOEI 2022), Chennai, India, 2022, pp. 634–637. doi:10.1109/ICOEI53556.2022.9776943.

[2] T. Shah and M. Sharma, "Spy Cam Detection,"GitHub repository. [Online]. Available: https://github.com/tanishq396/Spy_Cam_Detection

[3] D. Dharva, "Spy Camera Dataset," Roboflow Universe, Dec. 2022. [Online]. Available: https://universe.roboflow.com/dharva/spy-camera

[4] A. Pravin, T. P. Jacob, K. Mohana Prasad, T. Judgi, and N. Srinivasan, "Efficient Framework for Hidden Camera Detection & Jamming using IoT," in Proceedings of the 6th International Conference on Trends in Electronics and Informatics (ICOEI 2022), Chennai, India, 2022, pp. 634–637. doi:10.1109/ICOEI53556.2022.9776943.

[5] A. S. Gaikwad and P. S. Walia, "ESPÍA: A Review of Application to Detect Spy Camera Implementation," Int. Res.J. Mod. Eng. Technol. Sci., vol. 5, no 6, pp. 1–6, Jun. 2023. [Online]. Available:https://www.irjmets.com/uploadedfiles/paper/issue_6_june_2023/42296/final/fin_irjmets1687328741.pdf

[6] D. Dao, M. Salman, and Y. Noh, "DeepDeSpy: A Deep Learning-Based Wireless Spy Camera Detection System," IEEE Access, vol. 9, pp. 145486–145497, 2021, doi: 10.1109/ACCESS.2021.3121254

[7] "Digital Camera Detection and Deactivation Using Image Processing," image, Academia.edu.Accessed:May12,2025.[Online].Available: https://images.app.goo.gl/nEji89wW5ArfWZHX7

[8] T. Liu, Z. Liu, J. Huang, R. Tan, and Z. Tan, "Detecting Wireless Spy Cameras via Stimulating and Probing," in Proceedings of the 16th Annual International Conference on Mobile

Systems, Applications, and Services (MobiSys '18), Munich, Germany, Jun. 2018, pp. 243–255,doi: 10.1145/3210240.3210332. [9]A. K. Singh and R. K. Sharma,"Spynet: A Deep Learning Approach to Wireless Spy Camera Detection," Int. J. Eng. Res. Technol. (IJERT), vol. 14, no. 4, pp. 374–378, Apr. 2025. [Online].Available: https://www.ijert.org/research/spynet-a-deep-learning- approach-to-wireless-spy-camera detection- IJERTV14IS040374.pdf

[10]Q. Zhang, Z. Liu, and Y. Wang, "Eye of Sauron: Long-Range Hidden Spy Camera Detection and Positioning," in Proc. 33rd USENIX Security Symp. (USENIX Security 2024), Philadelphia,PA,USA,Aug.2024,pp.1–16.[Online].Available: https://www.usenix.org/system/files/sec24fall- prepub-357-zhang-qibo.pdf

SAMPLE CODE

```
#include <RCSwitch.h>

#define IR_SENSOR_PIN D1      // GPIO5

#define RF_RECEIVER_PIN D2   // GPIO4

#define LED_PIN D5           // GPIO14

#define BUZZER_PIN D6        // GPIO12

RCSwitch mySwitch = RCSwitch();

void setup() {

  Serial.begin(9600);

  pinMode(IR_SENSOR_PIN, INPUT);

  pinMode(LED_PIN, OUTPUT);

  pinMode(BUZZER_PIN, OUTPUT);

  digitalWrite (LED_PIN, LOW);

  digitalWrite (BUZZER_PIN, LOW);

        mySwitch.enableReceive(digitalPinToInterrupt(RF_RECEIVER_PIN));          //
interrupt-based receiver

  Serial.println("System Ready: IR + RF Monitoring Active");

}

void loop() {

  bool alertTriggered = false;

  // IR Sensor check

  int irValue = digitalRead(IR_SENSOR_PIN);
```

```
if (irValue == LOW) { // Assuming LOW = IR Detected
  Serial.println("IR Detected: Obstacle or IR Light");
  alertTriggered = true;
}
// RF Receiver check
if (mySwitch.available()) {
  long rfCode = mySwitch.getReceivedValue();
  if (rfCode != 0) {
    Serial.print("RF Signal Detected: ");
    Serial.println(rfCode);
    alertTriggered = true;
  } else {
    Serial.println("Unknown RF Signal");
  }
  mySwitch.resetAvailable();
}
// Alert via LED and Buzzer
if (alertTriggered) {
  digitalWrite(LED_PIN, HIGH);
  digitalWrite(BUZZER_PIN, HIGH);
  delay(1000);  // Alert duration
  digitalWrite(LED_PIN, LOW);
  digitalWrite(BUZZER_PIN, LOW);
```

```
  }
  delay(200); // Avoid flooding serial output
}
```