International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

IoT-Based Camouflage Military Robot for Surveillance Using Raspberry Pi: A Review

Nitish Singh
Student
Department of Electronic and communication engineering
ITM Gida Gorakhpur

Khushi alia
Student
Department of Electronic and communication engineering
ITM Gida Gorakhpur

Anjali Kumari
Student
Department of Electronic and communication engineering ITM Gida Gorakhpur

Abhishek sharma
Student
Department of Electronic and communication engineering
ITM Gida Gorakhpur

Dr. R.K. Singh
Department of Electronic and communication engineering
ITM Gida Gorakhpur

Abstract -The increasing demand for remote reconnaissance in hazardous and strategically sensitive environments has encouraged the development of compact unmanned ground robots capable of performing surveillance with reduced human exposure to operational risks. Advances in low-cost embedded computing platforms, particularly the Raspberry Pi, have enabled the development of economical robotic systems integrating sensing, wireless communication, image acquisition, and edge-based data processing. This review presents a comprehensive analysis of Internet of Things (IoT)-enabled surveillance robots based on Raspberry Pi and related embedded platforms, with particular emphasis on robotic camouflage and concealment. Existing approaches are examined according to their ability to reduce or manage observable signatures in visual, thermal, acoustic, and electromagnetic domains. The review further investigates commonly employed system architectures, sensors, mobility mechanisms, wireless communication technologies, video-streaming frameworks, computer-vision algorithms, object-detection methods, and edge-computing techniques. Particular attention is given to communication reliability, cybersecurity, latency, energy consumption, processing capability, and remote-operability, as these factors strongly influence the effectiveness of IoT-enabled robotic surveillance systems. A comparative assessment of reported design approaches and performance parameters is presented to identify technological trends and research gaps. The analysis indicates that limited energy availability, communication range, network security, environmental adaptability, computational constraints, and inadequate real-world validation remain significant challenges. The review concludes by identifying potential research directions involving energy-efficient architectures, secure communication, intelligent perception, adaptive concealment, edge artificial intelligence, and comprehensive field-based evaluation. Ethical and operational considerations associated with the deployment of remotely operated surveillance robots are also discussed.

Keywords-Internet of Things (IoT), Raspberry Pi, unmanned ground vehicle (UGV), robotic surveillance, military robotics, camouflage, concealment, edge computing, computer vision, wireless communication, cybersecurity..

I. INTRODUCTION

An IoT-based surveillance robot can be defined as a small unmanned ground vehicle equipped with sensors, cameras, communication modules, and an embedded computing platform for remote monitoring and control. The integration of the Internet of Things (IoT) enables different components of the robotic system to exchange information and communicate with a remote operator through wired or wireless networks. Such systems can support several functions, including real-time video monitoring, environmental sensing, remote navigation, data transmission, and supervisory control [1], [2].

The development of affordable and compact single-board computers has contributed significantly to the growth of small-scale robotic systems. The Raspberry Pi is one of the widely used platforms for robotic research and prototyping because of its relatively low cost, compact size, processing capability, camera interface, general-purpose input/output (GPIO) pins, and wireless connectivity [3]. A Raspberry Pi-based robotic system can integrate cameras and sensors, process collected data, transmit video to a remote station, and perform selected computer-vision and machine-learning tasks. These characteristics make it a suitable computing platform for the development of low-cost IoT-enabled surveillance robots.

However, surveillance capability alone does not determine the effectiveness of a robotic platform. A robot operating in a sensitive or hazardous environment may itself become detectable because of its physical appearance, heat generation, mechanical noise, or electromagnetic emissions. Therefore, camouflage and concealment are important considerations when designing robotic surveillance systems intended to operate without attracting unnecessary attention. Incorporating

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

concealment features during the initial design stage can be more effective than treating camouflage as an additional feature after the robot has already been developed.

Camouflage in robotic systems can be considered across several domains. Visual camouflage aims to reduce the robot's visibility by considering its shape, surface appearance, color, texture, and similarity to the surrounding environment. Thermal camouflage focuses on managing infrared signatures produced by heat-generating components such as motors, batteries, processors, and electronic circuits. Acoustic camouflage concerns the reduction or management of sound generated by motors, gears, wheels, tracks, cooling fans, and other mechanical components. In addition, electromagnetic camouflage or emission management considers the signals and electromagnetic emissions associated with communication systems and electronic components. These different forms of concealment present distinct technical challenges and require consideration of mechanical, electronic, thermal, and communication aspects of the robotic platform.

The integration of IoT, embedded computing, sensing, wireless communication, computer vision, and camouflage therefore represents a multidisciplinary area of research. A Raspberry Pi-based surveillance robot can combine these technologies within a relatively compact and economical platform. Nevertheless, the performance of such a system depends on several factors, including processing capability, energy consumption, communication reliability, operating range, sensor performance, environmental conditions, cybersecurity, and the effectiveness of its concealment mechanisms.

II. WORKING PRINCIPLE

• Environmental Sensing:-

The robotic platform can employ cameras, color sensors, or other optical sensing devices to acquire information about the surrounding environment. The collected visual information can be analyzed to identify dominant colors, textures, patterns, or other characteristics of the robot's immediate surroundings. This information may subsequently be used to support environmental adaptation and concealment-related functions.

• Adaptive or Active Camouflage:-

An active camouflage subsystem can modify the visual appearance of the robotic platform in response to information obtained from environmental sensors. Depending on the system design, actuators, electronically controlled surfaces, LED-based displays, or other visual elements can be used to alter the robot's apparent color or pattern. The objective is to reduce visual contrast between the robotic platform and its surrounding environment. The effectiveness of such an approach depends on factors including sensing accuracy, response time, environmental illumination, display characteristics, and the complexity of the background.

• IoT Connectivity:-

The Raspberry Pi can provide connectivity between the robotic platform and a remote monitoring or control system through wireless communication technologies such as Wi-Fi or cellular networks. Communication between the robot and a local server, web interface, or cloud-based platform can be implemented using commonly adopted IoT protocols, including MQTT and HTTP. This connectivity enables the transmission of sensor information, system status, and video data while also supporting remote commands and monitoring.

• Remote Monitoring and Control:-

The robotic system can be operated remotely through a computer, smartphone, tablet, or web-based dashboard. The remote interface may provide functions such as navigation control, live video monitoring, sensor-data visualization, and system-status monitoring. By separating the operator from the physical robotic platform, remote operation can facilitate surveillance and inspection tasks in environments where direct access may be undesirable or potentially hazardous.



Fig.1 Prototype



Fig.2 working of iot based camflouge military robot for surveillance using raspberry pi

III. CORE COMPONENTS

• Processing Unit: Raspberry Pi (such as Model 4B or 5) acts as the main brain for processing sensor feeds and running computer vision tasks.

• Vision & Detection: Pi Camera Module for live video streaming, alongside PIR (Passive Infrared) or IR sensors for intruder and human detection.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

• Environmental & Threat Sensors: Temperature sensors, gas detectors, or metal/landmine detectors.

• Locomotion: DC motors paired with a motor driver board (like L298N) configured on a sturdy chassis (such as a 4WD platform).

• Communication: Wi-Fi module or USB dongle for seamless internet connectivity.

IV. . REVIEW SCOPE AND APPROACH

We looked at conference and journal papers, project reports and technical documentation that describe ground robots for surveillance or reconnaissance using IoT connectivity, with particular attention to designs built around a Raspberry Pi. Work on aerial and underwater vehicles was left out unless it said something useful about camouflage or communication. We read each source with the same questions in mind. What hardware was used? How was video delivered? What detection method ran on the robot? How far could it operate? Was anything done to hide it? Was it tested outside a lab? Answers to these questions form the basis of the tables and comparisons that follow.

A caution is needed. Many of the available papers are small prototypes, and they seldom report numbers in a way that allows direct comparison. We therefore concentrate on patterns across the literature rather than ranking individual works.

V. BACKGROUND AND RELATED WORK

3.1 Military and Security Surveillance Robots

Unmanned ground vehicles (UGVs) have been investigated for military, security, and reconnaissance applications for several decades. Early systems were generally based on remotely operated tracked platforms equipped with cameras and other sensing devices. Although these systems demonstrated the feasibility of performing reconnaissance without directly exposing personnel to hazardous environments, their relatively large size, high cost, complex control requirements, and dependence on trained operators limited their accessibility and deployment.

Recent research has increasingly focused on compact and relatively low-cost robotic platforms that can be developed for surveillance, reconnaissance, inspection, and monitoring applications. Depending on the intended application, typical capabilities include real-time video transmission, obstacle detection or avoidance, motion detection, environmental monitoring, remote navigation, and supervisory control through a computer or mobile device [11].

The sensing subsystem plays an important role in the operation of a surveillance robot. Cameras provide visual information for remote observation and can also serve as inputs for image-processing and object-detection algorithms. In addition, inertial or microelectromechanical systems (MEMS)-based sensors can provide information related to acceleration, orientation, and motion. The collected sensor information is processed by the embedded computing system and can be used to support navigation, monitoring, decision-making, and control functions.

The robotic platform generally consists of interconnected sensing, processing, communication, actuation, and power subsystems. The embedded controller receives information from the sensors and generates appropriate control commands for the actuators. . The overall architecture therefore enables surveillance tasks to be conducted while maintaining physical separation between the operator and the monitored environment.

Military and security applications represent one important area of research in unmanned robotics because robotic systems can assist with reconnaissance, surveillance, hazardous-area inspection, logistics, and disaster-response activities. . However, the operational requirements of military and security applications are generally more demanding than those of laboratory prototypes, particularly with respect to reliability, communication robustness, mobility, power endurance, environmental resistance, cybersecurity, and system concealment.

3.2 Internet of Things in Defence and Surveillance Applications

The Internet of Things provides a communication framework through which sensors, computing devices, actuators, and monitoring systems can exchange information over a network. IoT architectures are commonly described using multiple functional layers, including sensing, communication or networking, processing, and application layers [1], [2]. The integration of these capabilities into robotic systems enables sensor information and system-status data to be transmitted to a remote monitoring station while allowing control commands to be communicated back to the robotic platform.

In an IoT-enabled surveillance robot, parameters such as battery status, temperature, position, motion information, and sensor measurements can be collected and transmitted to a local or remote monitoring interface. Similarly, commands related to navigation, system configuration, and other supervisory functions can be received by the robot through the communication network. This approach provides greater flexibility than a completely isolated robotic control system because monitoring and control functions can be accessed through network-connected devices.

Several communication protocols can be used in IoT-based robotic systems depending on the application requirements. Message Queuing Telemetry Transport (MQTT) is particularly relevant to resource-constrained IoT applications because it uses a lightweight publish-subscribe communication model [4]. Other protocols, including HTTP, may be used when communication with web-based services or application interfaces is required.

Research in wireless sensor networks also provides useful concepts for IoT-enabled robotic systems, particularly regarding energy management, distributed sensing, communication reliability, and multi-hop networking [12].

3.3 Raspberry Pi as an Embedded Computing Platform

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

Single-board computers have become increasingly common in robotic research because they provide considerably greater computational capability than conventional microcontroller platforms while maintaining relatively low cost and compact dimensions. The Raspberry Pi is one of the commonly used single-board computers for educational, research, and prototype robotic applications.

A major advantage of the Raspberry Pi is its ability to run a complete operating system and support high-level programming environments. . OpenCV, for example, can be used to perform image-processing and computer-vision operations [5]. Camera modules can also be connected directly to compatible Raspberry Pi platforms, enabling image acquisition and real-time video-processing applications.

For surveillance robots, the Raspberry Pi can perform several functions within the same system. These may include camera control, video processing, wireless communication, sensor-data processing, web-server operation, remote monitoring, and selected machine-learning tasks.

VI. CAMOUFLAGE IN ROBOTIC SYSTEMS

Camouflage in nature is about more than colour. Studies of animal camouflage point to background matching, disruptive patterns that break up an outline, and reducing shadow and contrast as the main mechanisms [6], [7]. The same principles carry over to machines, and the papers we reviewed use them in several ways.

A. Passive Visual Camouflage

The most common approach is a printed or painted shell in a terrain-matching pattern such as desert, woodland or urban grey. Some designs add a low profile and rounded body to cut down shadow. Others disguise the robot as a natural object, for example a rock or a pile of debris. It costs almost nothing, yet it is fixed, so a robot dressed for forest looks out of place on sand. Matte finishes matter too, since a glossy plastic casing reflects sunlight and gives the robot away from a long distance.

B. Thermal and Acoustic Signature Reduction

A running Pi, motor drivers and batteries all produce heat, and motors produce noise. Reported countermeasures include insulated enclosures, heat sinks that spread heat over a larger surface, quieter geared motors, rubber mounts, and a stop-and-observe driving style in which the robot moves in short bursts and then stays still while it watches. A few papers also mention reducing the time the camera and wireless radio are active. Tracked chassis tend to be noisier than wheeled ones on hard ground, but they cope better with loose soil, so designers have to choose which signature matters more for the mission.

C. Radio Emission Discipline

This is the form of camouflage that student projects most often forget. A robot that streams video continuously over Wi-Fi is easy to locate with simple direction-finding equipment, no matter how good its paint job is. Practical steps include sending data only when something is detected, lowering transmit power to the minimum that works, using low-rate long-range links for status messages, and keeping the main radio switched off during idle periods. These steps cost nothing in hardware and make a surprising difference to detectability. Robots are exceptionally structure for human to make our life simpler. Robots are structure for different purposes like military reason, industry, for locally situated application. At outskirt various kinds of tanks, rockets and weapons are utilized by the adversary. This causes issues and will hurt our power or troopers. Hence in this paper a robot is structured and produced for military reason application to ensure our military. The strategy includes a biped strolling robot utilizing equal leg instrument for example PLM which incorporates various capacities like catching certifiable information utilizing advanced picture handling used to recognize its impediment which is found in its way.

D. Adaptive Camouflage

Adaptive camouflage uses colour-changing surfaces, such as e-ink style panels or LED fabrics, driven by a camera that samples the surroundings. This is the most interesting direction, but nearly all of it remains at laboratory scale. Cost, power consumption and durability under rain and dust are the usual obstacles.

VII. . SYSTEM ARCHITECTURE

Despite differences in detail, the reviewed systems share a common structure, shown in Fig. 1. The perception block holds the camera, an ultrasonic or infrared distance sensor, and often a PIR motion sensor. The processing block is the Raspberry Pi, sometimes with a helper microcontroller. The communication block carries video and commands between the robot and the operator. The actuation block contains the motor driver, motors and, in some designs, a pan–tilt camera mount. A rechargeable battery pack powers everything, and regulators keep the Pi supplied with a stable voltage.

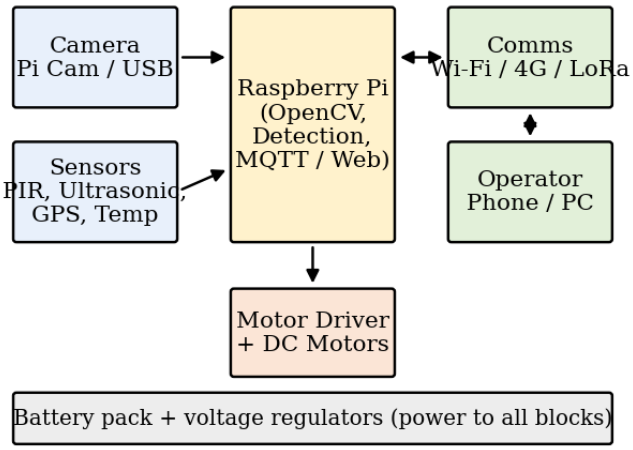


Fig. 3. General block diagram of a Raspberry Pi based surveillance robot.

TABLE I. Typical components in reviewed designs

Block	Typical components
Processing	Raspberry Pi 3/4/Zero 2 W; optional microcontroller
Vision	Pi Camera Module or USB camera; pan–tilt servo
Sensing	Ultrasonic, PIR, IR, gas, temperature, GPS
Actuation	L298N motor driver; DC geared motors; tracked/wheeled chassis
Comms	Wi-Fi, 4G/GSM modem, LoRa module
Power	Li-ion / Li-Po pack with buck converter

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

A. Choosing the Raspberry Pi Model

Table II lists the boards most often seen in the literature. The small Zero 2 W suits a compact, low-power body but struggles with neural network inference. The 3B+ is a balanced choice and appears in many prototypes. The 4B has the strongest processor and more memory, which helps when running detection locally, but it runs hotter and needs a better power supply and cooling, both of which work against camouflage.

TABLE II. Raspberry Pi boards in the reviewed literature

Board	CPU	RAM	Suitability
Zero 2 W	Quad Cortex-A53, 1 GHz	512 MB	Small, low power; light vision only
3B+	Quad Cortex-A53, 1.4 GHz	1 GB	Balanced; common choice
4B	Quad Cortex-A72, 1.5 GHz	1–8 GB	Best for on-board AI; hotter

B. Chassis and Mobility

Two-wheel differential drive with a caster is the simplest and cheapest arrangement. Four-wheel and tracked bases offer better traction on rough ground and are preferred for outdoor trials. Most prototypes are small, under a few kilograms, because small motors and batteries are cheap and quiet, though payload and obstacle-climbing ability suffer. Suspension is rare, which means camera footage on uneven terrain is often shaky. A few designs add a gimbal or software image stabilisation to compensate.

C. Power Management

Power is the quiet bottleneck. Most designs use a Li-ion pack feeding a buck converter for the Pi and a separate supply for the motors, since motor current spikes can reset the computer. Good designs add a battery monitor so the operator knows when to recall the robot. Duty cycling, in which the Pi sleeps or the camera is switched off between events, extends mission time far more than a larger battery does and also supports the camouflage goals discussed earlier.

D. Sensing Suite

The camera is the main sensor, but it rarely works alone. A passive infrared (PIR) sensor is the cheapest way to notice a warm body and is often used as the trigger that wakes the rest of the system. Ultrasonic sensors give short-range distance readings for obstacle avoidance, although they can be confused by soft surfaces and by wind noise outdoors. Infrared and low-light cameras extend vision into the night, and the better prototypes use an IR-sensitive camera with a small IR illuminator that is switched on only when needed, since a constantly glowing illuminator is visible to night-vision equipment. GPS and an inertial sensor provide position and heading, and a temperature or gas sensor can add environmental awareness for inspection tasks. Each extra sensor adds weight, wiring and power draw, so the reviewed papers that perform best tend to choose a small, well-matched set rather than a long list.

E. Suggested Reference Configuration

Putting the findings together, a practical low-cost configuration for a camouflaged surveillance robot would look like this:

- a Raspberry Pi 3B+ or Zero 2 W as the main computer, with a small microcontroller handling motors and the PIR trigger;
- a low-profile, matte, terrain-matched shell with insulation and a vented heat spreader, mounted on quiet geared motors;
- a compact detector such as MobileNet running only after the PIR sensor fires;
- LoRa for status and alerts, with Wi-Fi or 4G video enabled on demand;
- encrypted, authenticated links and a storage card that can be wiped if the unit is captured.

This is not the only workable choice, but it reflects the points where the literature agrees: do as little as possible while idle, and make every transmission count.

VIII. SOFTWARE AND INTELLIGENCE

A. Software Stack

The typical stack is Raspberry Pi OS, Python, and OpenCV for image handling [5]. Video is usually served over a simple web page so that the operator can watch from a phone browser without installing anything. Driving commands travel the other way through a web interface or an MQTT topic [4].

The choice of video format matters more than it first appears. Motion-JPEG over HTTP is the easiest to set up and is used in most student projects, but it uses a lot of bandwidth. H.264 with RTSP or WebRTC cuts the data rate considerably and gives lower latency, at the cost of a more involved setup. The Pi has hardware H.264 encoding, so using it saves processor time that can be given to detection. Lowering the resolution to what the operator actually needs, often 640 by 480 pixels, is a simple way to save both bandwidth and battery.

B. Detection and Recognition

For detection, early papers rely on classical methods such as the Viola–Jones cascade [8], which is fast enough for a Pi but only good for faces and a few simple objects. Newer work uses compact neural networks such as MobileNet [9], [13] and YOLO-style detectors [10] to spot people or vehicles; a broader survey of the field is given in [14]. On a Pi these run at only a few frames per second unless an accelerator is attached or the input resolution is cut down, and this is a trade-off most papers acknowledge openly. Background subtraction and simple motion detection remain popular as a cheap first filter that wakes the heavier detector only when needed [15].

C. Operating Workflow

A useful pattern we saw repeatedly is to run detection on the robot and send only alerts and short clips over the network, instead of streaming everything all the time. Fig. 2 shows this workflow. It saves bandwidth and battery, and it also keeps the radio quiet, which fits well with the camouflage goal.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

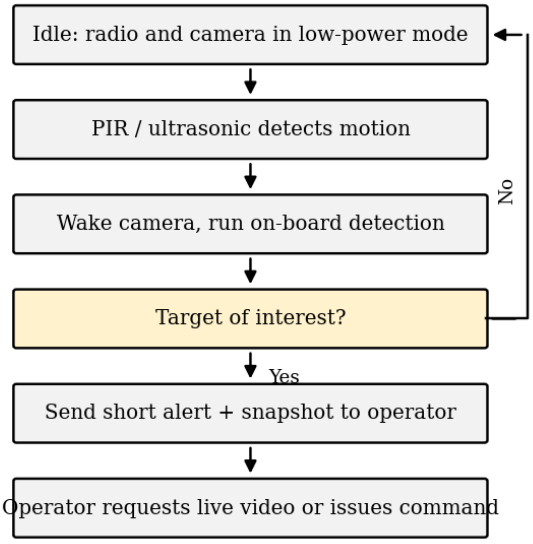


Fig. 4. Event-driven operating workflow that keeps the robot quiet when idle.

D. Navigation and Control

Most robots are driven manually by an operator who watches the video feed. A smaller group adds obstacle avoidance using ultrasonic sensors, and a few follow GPS waypoints for patrol routes. Full autonomy is rare in Pi-based work because mapping and path planning demand more computing than the board can comfortably spare, although established robotics methods [16] show how this can be approached. Latency is the practical problem for manual control. When video lags by more than about half a second, driving becomes difficult, so several designs lower the resolution and frame rate to keep the response quick.

IX. COMMUNICATION AND SECURITY

5. Communication Technologies and Security Considerations
Communication is a fundamental component of IoT-enabled robotic surveillance systems because it enables remote control, telemetry, sensor-data transmission, and video monitoring. The choice of communication technology depends on several factors, including operating range, bandwidth, latency, power consumption, network availability, environmental conditions, and system cost.

5.1 Wireless Communication Technologies

Wi-Fi is commonly used in Raspberry Pi-based robotic platforms because wireless networking is integrated into many Raspberry Pi models and provides relatively high data-transfer rates. This makes Wi-Fi particularly suitable for applications involving real-time video streaming, remote monitoring, and web-based control interfaces. However, its practical communication range is affected by factors such as transmission power, antenna configuration, obstacles, interference, and environmental conditions. Consequently, Wi-Fi-based systems may be more appropriate for relatively short-range operation or environments with suitable network infrastructure.

Cellular communication provides an alternative when operation over larger geographical areas is required and cellular network coverage is available. Technologies such as 4G and other broadband cellular networks can provide substantially greater geographical coverage than conventional local wireless networks and can support video transmission and remote access. However, cellular systems depend on network availability and may introduce additional power consumption, hardware requirements, operating costs, and communication latency.

Long-range low-power technologies such as LoRa are also relevant to robotic applications where only small quantities of data need to be transmitted over relatively long distances. LoRa-based communication can be suitable for telemetry, sensor measurements, status information, and low-bandwidth control data. However, its relatively low data rate makes it unsuitable for high-bandwidth applications such as continuous high-resolution video streaming. Therefore, communication technologies should be selected according to the specific data requirements of the robotic platform.

A hybrid communication architecture can combine multiple technologies to exploit their respective advantages. For example, a low-bandwidth long-range communication link can be used for telemetry and essential status information, while Wi-Fi or cellular connectivity can be employed when higher bandwidth is required for video or other data-intensive applications. Such architectures can also provide communication redundancy, although they increase system complexity and may require additional hardware and power-management mechanisms [17].

5.2 Communication Security

Security is an important consideration in IoT-enabled robotic systems because unauthorized access to communication channels may compromise sensor data, control functions, or the overall operation of the robotic platform. Many prototype systems prioritize functional demonstration and therefore provide limited information regarding cybersecurity. This represents an important research gap, particularly for applications involving remote operation and sensitive information.

Common security practices include the use of encrypted communication channels, strong authentication mechanisms, secure credential management, and the restriction of unnecessary network services. Transport Layer Security (TLS), for example, can be employed to protect data exchanged between networked devices and servers. TLS can also be incorporated into MQTT-based communication and web-based interfaces when supported by the system architecture [18], [19].

Authentication is another important component of secure robotic communication. Default usernames and passwords should be avoided, while stronger authentication mechanisms and appropriately managed cryptographic credentials can reduce the likelihood of unauthorized access. For command-based systems, additional mechanisms can be considered to verify the authenticity and integrity of received commands and to reduce the risk of unauthorized or repeated commands.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

The security of the embedded computing platform itself must also be considered. Unnecessary network services should be disabled, software and operating-system components should be maintained appropriately, and access to administrative interfaces should be restricted. Since robotic systems may operate in environments where physical access to the hardware is possible, protection of locally stored information is also relevant. Encryption of stored data and appropriate credential-management mechanisms can reduce the consequences of physical loss or unauthorized access to the computing platform.

Wireless communication is additionally subject to threats such as interference, spoofing, and deliberate disruption. Although these issues are recognized in the broader IoT and wireless-communication literature, they are not consistently evaluated in small-scale robotic prototypes. Future studies should therefore include systematic assessment of communication reliability and security under realistic operating conditions, together with quantitative measurements of latency, packet loss, range, energy consumption, and resilience to network disturbances.

X. COMPARATIVE ANALYSIS

Table III summarises the main design choices seen in the literature and the trade-offs that come with each one.

TABLE III. Comparison of common design approaches

Approach	Strength	Limitation
Pi + Wi-Fi video	Simple, cheap, low latency	Short range; easy to detect
Pi + 4G/GSM	Long range with coverage	Needs network; latency; power
Pi + LoRa telemetry	Very long range, low power	No live video
Pi + edge AI detection	Less data sent; auto alerts	Low frame rate; heat
Passive camouflage shell	Low cost, no power	Fixed to one terrain
Event-driven radio	Low emission, long battery life	Delayed first view

No single option wins on every count. A realistic design mixes them, for example a camouflaged shell, local detection on the Pi, LoRa for always-on status and a short-range video link that is only switched on when something has been detected.

XI. EVALUATION METRICS

One of the clearest gaps in the literature is the absence of shared metrics. We suggest that future work report at least the following so that results from different groups can be compared:

- detection accuracy (precision and recall) on realistic outdoor footage, and frames per second on the board;
- end-to-end video and command latency at stated distances;
- communication range in open and obstructed terrain;
- mission duration on a full charge, with and without duty cycling;
- surface and enclosure temperature after continuous operation;
- noise level at a fixed distance while moving and while idle; and
- visual detectability, for example the distance at which human observers first notice the robot against a given background.

The last item is the hardest to measure, but it is the one that tests the camouflage itself and is almost never reported.

Test conditions deserve the same care as the metrics. Results from a lit indoor corridor say very little about a dusty slope at noon or a damp field at night. We recommend that studies describe the terrain, weather, time of day and background used, and repeat each test several times so that variation is visible. Where possible, the same robot should be tested with and without its camouflage shell and with and without event-driven radio control, which would show how much each measure actually contributes. Such controlled comparisons are almost absent from the current literature, yet they would be the quickest way to find out which ideas are worth pursuing.

XII. CHALLENGES AND LIMITATIONS

- Power: a Pi with a camera and a radio drains small batteries within a few hours, which limits mission time.
- Terrain: many prototypes were tested on flat indoor floors, and only a few on grass, sand or slopes.
- Environment: dust, rain, heat and vibration are rarely tested, although they decide whether the robot survives.
- Detectability: radio emissions, motor noise and thermal output can give the robot away even when it looks like a rock.
- Computation: running detection at a useful frame rate on a Pi pushes the board to its thermal limits.
- Security: weak default credentials and unencrypted links are still common in student-level work.
- Evaluation: papers seldom report standard metrics, which makes comparison difficult.

XIII. ETHICAL AND LEGAL CONSIDERATIONS

A surveillance robot can protect soldiers, but it also collects images of people who have not agreed to be filmed, and the data it gathers can be misused. Engineering papers mostly leave these questions aside, yet they deserve attention. Designers should decide in advance what is recorded, how long it is stored and who can access it. Where a robot uses detection to flag people, errors can have serious consequences, so a human should remain responsible for every decision that follows an alert. International discussions about autonomy in military systems stress this point of meaningful human control, and researchers building such platforms should keep it in mind. We also note that this review covers observation and reconnaissance only.

XIV. FUTURE SCOPE

Several directions look worthwhile. Adaptive skins that follow the surroundings would remove the single-terrain limitation of passive shells. Pairing the Pi with a small AI accelerator would raise detection speed without adding much heat. Mesh networking between several small robots would allow area coverage and make the group more resilient if one unit is lost. Energy harvesting with a thin solar layer could extend mission time during long observation tasks. Better thermal management, such as passive heat spreaders built into the shell, would help both reliability and stealth. Finally, field

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

trials with proper test protocols would do more for the field than another prototype demonstrated in a lab.

Two further areas deserve mention. First, learning methods that adapt a detector to a new environment on the device itself, without sending images to a server, could improve accuracy while protecting data. Second, newer low-power wide-area and 5G technologies may close the gap between range and bandwidth that forces today's designs to juggle several radios. Both depend on hardware that keeps getting cheaper, so we expect them to reach small robots within a few years.

XV. CONCLUSION

IoT and the Raspberry Pi together make small surveillance robots achievable at very low cost, and the literature shows steady progress in video streaming, detection and remote control. Camouflage, on the other hand, is treated as an afterthought in most of the work we reviewed, even though it is what decides whether a surveillance robot can do its job. Bringing together passive, thermal, acoustic and radio measures with an event-driven communication strategy appears to be the most practical path today, with adaptive camouflage as a longer-term goal. Better security, shared evaluation metrics and honest field testing remain the biggest gaps, and closing them would make future work far easier to trust and to build on. The development of an IoT-based military robot with environmental sensing, live webcam broadcasting, and movement based on commands demonstrates significant potential for enhancing military operations. Through the integration of temperature, gas, and MEMS sensors, the robot can effectively monitor its surroundings, providing real-time data on environmental conditions crucial for situational awareness. The inclusion of a webcam enables remote operators to visually assess the operational environment in real time, further enhancing decision-making capabilities. Movement based on commands offers flexibility and adaptability, allowing the robot to navigate diverse terrain and respond dynamically to mission requirements. Overall, this project showcases the value of IoT technologies in improving operational efficiency, reducing risks to personnel, and enhancing mission success rates in military settings.

ACKNOWLEDGMENT

The authors thank their project guide Dr. R.K. Singh and the Department of Electronic and communication engineering
ITM Gida Gorakhpur for their guidance and support during the preparation of this review.

REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.

[2] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, 2010.

[3] E. Upton and G. Halfacree, Raspberry Pi User Guide. Chichester, U.K.: Wiley, 2014.

[4] A. Banks and R. Gupta, Eds., "MQTT Version 3.1.1," OASIS Standard, 2014.

[5] G. Bradski, "The OpenCV Library," Dr. Dobb's J. Softw. Tools, 2000.

[6] S. Merilaita, N. E. Scott-Samuel, and I. C. Cuthill, "How camouflage works," Phil. Trans. R. Soc. B, vol. 372, no. 1724, 2017.

[7] M. Stevens and S. Merilaita, "Animal camouflage: Current issues and new perspectives," Phil. Trans. R. Soc. B, vol. 364, no. 1516, pp. 423–427, 2009.

[8] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," in Proc. IEEE CVPR, 2001, pp. I-511–I-518.

[9] A. G. Howard et al., "MobileNets: Efficient convolutional neural networks for mobile vision applications," arXiv:1704.04861, 2017.

[10] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You only look once: Unified, real-time object detection," in Proc. IEEE CVPR, 2016, pp. 779–788.

[11] B. Siciliano and O. Khatib, Eds., Springer Handbook of Robotics. Berlin, Germany: Springer, 2008.

[12] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Comput. Netw., vol. 52, no. 12, pp. 2292–2330, 2008.

[13] M. Sandler, A. Howard, M. Zhu, A. Zhmoginov, and L.-C. Chen, "MobileNetV2: Inverted residuals and linear bottlenecks," in Proc. IEEE CVPR, 2018, pp. 4510–4520.

[14] Z. Zou, K. Chen, Z. Shi, Y. Guo, and J. Ye, "Object detection in 20 years: A survey," Proc. IEEE, vol. 111, no. 3, pp. 257–276, 2023.

[15] R. Szeliski, Computer Vision: Algorithms and Applications. London, U.K.: Springer, 2010.

[16] R. Siegwart, I. R. Nourbakhsh, and D. Scaramuzza, Introduction to Autonomous Mobile Robots, 2nd ed. Cambridge, MA, USA: MIT Press, 2011.

[17] M. Augustin, J. González, L. Samper, and J. Martínez, "A study of LoRa: Long range & low power networks for the Internet of Things," Sensors, vol. 16, no. 9, art. 1466, 2016.

[18] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," Comput. Netw., vol. 57, no. 10, pp. 2266–2279, 2013.

[19] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," IETF RFC 8446, Aug. 2018.

[20] A. A. Alshdadi, "Evaluation of IoT-Based Smart Home Assistance for Elderly People Using Robot," Electronics, vol. 12, no. 12, p. 2627, Jun. 2023, doi: 10.3390/electronics12122627.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)