COVERT CAMERA DETECTION

RishikaAnbu[*1], SubikshaDeivasigamani[2], Sri AkshayaSenthilkumar[3], SrijaKasinathan[4], Mr. VenkateshGajendran[5]

[1,2,3,4] UG Scholars, Department of ECE , Panimalar Engineering College, Chennai, India
[5] Assistant Professor , Department of ECE , Panimalar Engineering College, Chennai, India

Abstract
In recent times, our country has blossomed in many ways, but many crimes may still exist. This paper proposes maintaining the security and safety of mankind through the use of secret cameras that can be easily discovered. Due to their low price and tiny size, hidden cameras are now easy to place practically everywhere. It finds use in locations where cameras are actually prohibited. Also, the locality and the offender's pinpointing would be dispatched to the competent authorities. In this review, a practical method for automatically identifying concealed cameras and their recordings is proposed. The main concept is to use a wireless bug detector and RF detector to find and deactivate any electronic spy equipment, such as GPS tracking devices, microphones, and cameras. The technology's capacity for stand-off detection of concealed objects is demonstrated by the detectors' ability to acquire reflection images of a metallic object concealed in a manila envelope. Where the camera is prohibited, these cameras are most frequently utilized. The standard LED light scans the area being monitored. The flashing light will reflect off of it, allowing the spy camera lens to detect it. We draw the conclusion from these findings that similarity of simultaneous observation is a workable technique for finding covert wifi cameras that are streaming a user's footage.

Keywords: Security surveillance system; Complementary metal-oxide semiconductor (CMOS) image sensor; Wireless bug detector; Broadcasting frequencies, Torch detector.

1. Introduction

In recent years, in restricted areas the usage of cameras and mobile phones has drawn more and more criticism. These devices, which provide connectivity between a student sitting in the hall and outsiders, have greatly increased the strain on invigilators to ensure that malpractice is not committed during exams. A student may frequently communicate with other students outside the testing room via email and text messaging. They can connect and exchange information, such as queries and answers, through platforms like what'sApp, email attachments, and others. A student can use a mobile device to take a photo of the test and send it to other students for help. Exam papers can occasionally be leaked, in addition to other ways. Due to the wireless adopter's busy schedule of packet listening on the wireless network. However, after the monitoring application has been stopped, connectivity can be restored. Using a second device, like the ESP32 Wi-Fi microcontroller in the [1]. Uses the Smartphone's magnetometer sensor to track the camera based on electromagnetic waves it emits. Similarly, the electromagnetic radiation from the camera is really weak and needs to be detected at a great distance. In conclusion, it is impracticable to use a hidden camera for any application that necessitates close contact. On the other hand [2]. Employed a web camera /spy camera to generate visual traffic and a smart phone with an extra Wi-Fi to detect traffic from the environment. Flashing lights stimulated the camera. By comparing parallel observations, Wu et al. addressed camera detection [3]. This study made use of a wireless Wi-Fi camera called DEATTI that operates at 2.4 GHz and has a number of high-end features like support for 1080p resolution, night vision, and pan and tilt. Implementing the open-source Nexmon CSI GitHub repository allowed the monitoring mode to be used with the CSI extraction feature [4]. can recognize and show video being streamed by a wireless camera. This gadget recognizes streaming from analogue video sources including PAL, NTSC, and SECAM, yet operates on a variety of frequencies like 1.2GHz, 2.5GHz, and 5.0GHz. The video footage is compressed and encrypted prior to transmission by the Wi-Fi cameras now in use. As a result, this gadget was unable to identify such streaming. On the other hand, a lot of research has been done on Wi-Fi-based activity of human CARM, a conventional approach of machine learning, was used to present human activity recognition [5].

2. Existing system

There are a number of contemporary systems in use that search for hidden cameras using a variety of technologies. The following list of technologies includes some examples,

A. Security surveillance system

In terms of environmental protection, security refers to a state of being "without fear of danger." With an emphasis on autonomous surveillance, this study offers a survey of the relevant literature on security. It does by assembling into a single document the latest technical developments in surveillance systems, applications, and essential components. Its ability to be taught with synthetic images and a generative artificial neural network (GAN) (generative adversarial network) is the module's

distinguishing feature. Additionally, it has to do with the security aspect [17], where more quickly deployed intelligent surveillance software [18] Among others, Dautov [17].

B. CMOS image sensors

There are currently a wide variety of imaging systems available, each of which can be used for a particular purpose. Imaging systems include well-known devices including digital cameras, cam recorders, webcams, and safety cameras, since they outperform CCDs in terms of performance, CMOS image sensors have drawn a lot of interest over the past ten years. Like camera-on-chip systems or super-low-power technologies, new vistas can be unlocked in light of the circumstances and the most recent advancements in this sector [14]. Despite significant constraints, miniaturization has a rather high level of integration [15]. Imagery at a rapid phase and the ability to capture photos in a very short amount of time [16].

C. Wireless bug detector

Remote government operative devices (WSDs) are surveillance tools, such as listening devices or cameras, hidden inside items or covertly placed inside rooms. Surveillance with WSD is one of the most popular ways to capture conversations for both intelligence gathering and criminal charges. WSDs have however, also been abused for illegal purposes, including industrial espionage and blackmail [19].

D. Broadcasting frequencies

It uses a circuit in the figure.1 with many resistors, a few capacitors, standard ICs, and a piezo-buzzer that emits when a camera is found, make a sound. This device is basically designed using a disc capacitor to detect cell phone signals within a 1.5-metre radius at frequencies between 0.9 and 3 GHz. The radio frequency (RF) signals that some covert cameras broadcast can be detected by a broadcast detector app on your phone. By recognizing the RF signals that the camera emits, these apps can locate hidden cameras. RF Detector and Glint Finder are two common RF detector apps. It detects signal alterations from any nearby transmitting eavesdropping devices using the broad casting detection technique. Any GPS tracker that is magnetically fastened to a vehicle is detected by the magnetic field detection mode [6]. Finding the hidden camera is made easier by the camera's lens finder function. The tool can readily assist you in identifying spy cameras because it is highly sensitive to the electromagnetic emissions that wireless cameras create while recording.

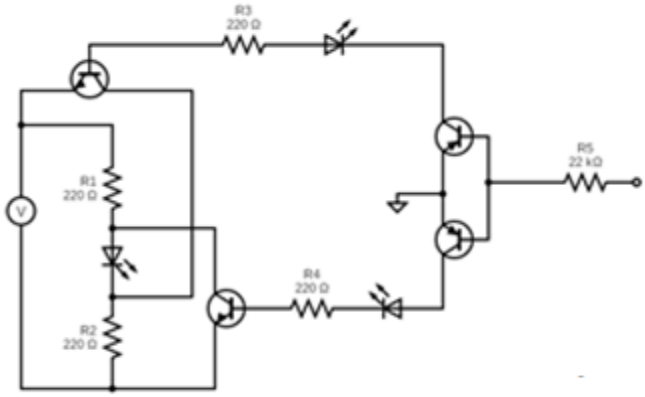

Figure1: Circuit diagram of broadcasting frequencies

E. The torch detector

The time-of-flight detector in the illustration is called TORCH (Timing of internally reflected Cherenkov photons) [7]. 2 was first suggested for the LHCb experiment upgrade [8, 9]. The LHCb particle detection capabilities currently offered by two gaseous ring-imaging Cherenkov detectors would be extended into the low momentum range (2–10 GeV/c) by TORCH [10]. The BaBar DIRC [11], Belle-II iTOP [12], and Panda disc DIRC [13] served as inspiration for the TORCH design.

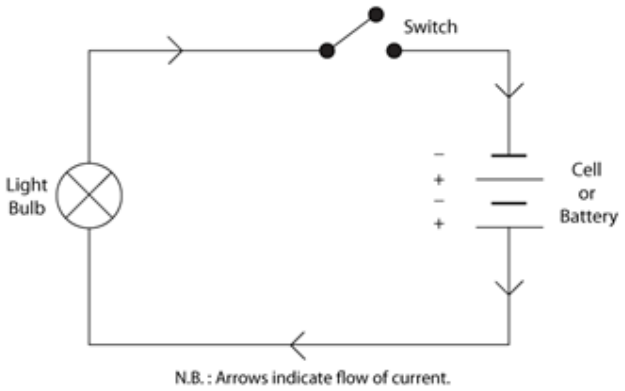

Figure2: Circuit diagram of torch

4. METHODOLOGY

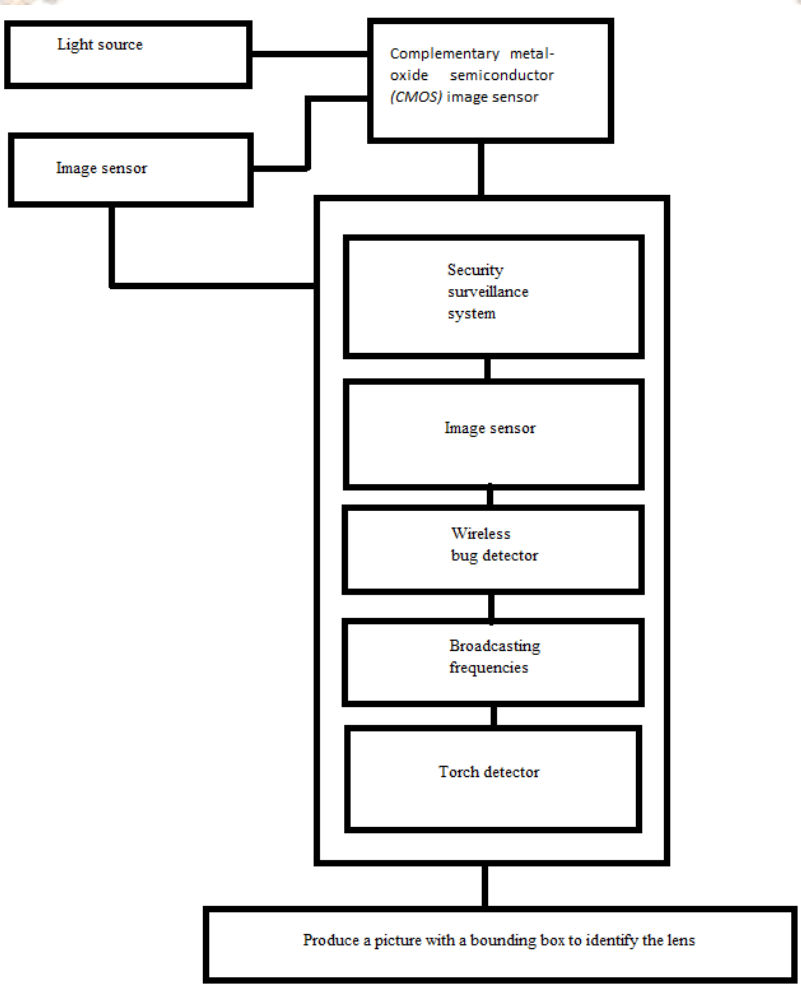

Figure3: Block diagram for covert camera detector

Explanation of block diagram:

The above figure3: explains about,

SECURITY SURVIELENCE: An array of audio, video, or photographic recording devices deployed with the goal of monitoring or capturing activity taking place at the required dwelling makes up a security surveillance system.

IMAGE SENSOR: An image sensor, sometimes known as an imager, is a sensor that collects and transmits data used to form images. It achieves this by translating light waves' fluctuating attenuation (as they pass through or reflect off things) into signals, or brief current bursts that contain information. The waves might be electromagnetic radiation, such as light.

WIRELESS BUG DETECTOR: The term "bug detector" or "RF signal detector" refers to the tool used to identify adjacent wireless or RF espionage devices. A bug detector can find GPS units, microphones, and spy cameras. If there are any nearby bugs or spy gadgets, it warns the user.

BROADCASTING FREQUENCY: In the USA, the FM band runs from between 88.0 and 108.0 MHz The band consists of 100 channels, each 200 kHz (0.2 MHz) wide. The channel's lower end is 100 kHz (0.1 percent by weight) above the central frequency, or half the FM channel's bandwidth.

TORCH DETECTOR: In a modular design, TORCH makes use of quartz radiator plates. Some of the Charged particles travelling through this radiator produce Cherenkov photons, which are subsequently focused onto rapid, position-sensitive single-photon detectors after travelling via total internal reflection and emerging at the edges.

5. Covert camera detector

One of the various tools a technician uses to implement technical surveillance countermeasures is a hidden camera detector in the figure.4. TSCM is the technique of finding electronic surveillance equipment in various places, such as covert cameras. Finding and removing the device is crucial if you believe you are being watched, whether in a personal or business setting.

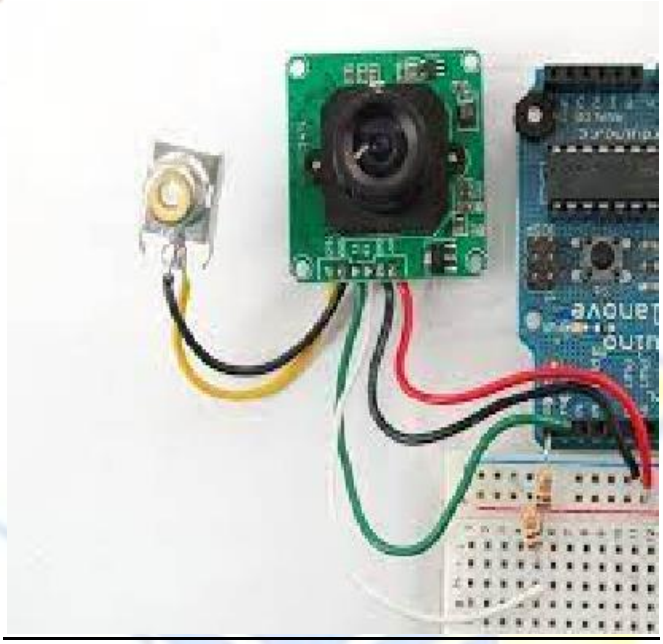

Figure4: Pictorial representation of covert camera detection

6. Conclusion

In this review, trial rooms, theatres, and many other public areas where spy cameras are illegal would all be detected by hidden camera detection, which would then immediately notify the authorities of the discovery. This system is an effective system for detecting camera because, despite how tiny the lenses are, they can be easily recognized, making it nearly impossible to manually check for their presence. Even after rigorous screening, people are still able to sneak cameras into private meeting spaces, conversations of the record, and use the recordings for illicit activities. Therefore, on the application will be quite useful in places that prohibit cameras.

References

[1] S. M. Hernandez and E. Bulut, ‘‘Performing WiFi sensing with off-the shelf smart phones,’’ in Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops), Mar. 2020

[2] Cheng, X. Ji, T. Lu, and W. Xu, ‘‘On detecting hidden wireless cameras: A traffic pattern-based approach,’’ IEEE Trans. Mobile Comput., vol. 19, no. 4, pp. 907–921, Apr. 2020.

[3]W. Kevin and B. Lagesse, ‘‘Do you see what I see? Detecting hidden streaming cameras through similarity of simultaneous observation,’’ in Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom, Mar. 2019,

[4] S. Matthias, W. Daniel, and H. Matthias. (2017). Nexmon: The C-Based Firmware Patching Framework. Nexmon:Project.

[5] W. Wang, A. X. Liu, M. Shahzad, K. Ling, and S. Lu, ‘‘Device-free human activity recognition using commercial WiFi devices,’’ IEEE J. Sel. Areas Commun., vol. 35, no. 5, pp. 1118–1131, May 2017

[6]Gayathri N. and T. Sivasakthi, "Presence of active mobile phones and hidden camera detection", International journal of computers, communication, and information systems, Volume 8, 2016

[7]M. Charles, R. Forty,TORCH: time of flight identification with Cherenkov radiation, Nucl. Instrum. Methds A, 639 (1) (2011), p. 173

[8]The LHCb Collaboration, Letter of Intent for the LHCb Upgrade, CERN/LHCC 2011-001, LHCb LoI (7 March 2011).

[9]The LHCb Collaboration, LHCb PID Upgrade Technical Design Report, CERN/LHCC 2013-022, LHCb TDR 14 (28 November 2013).

[10]A.Papanestis et al., Performance of the LHCb RICH detectors during the LHC Run II, Nucl. Instrum. Methods A, these proceedings.

[11] I. Adam, et al.The DIRC particle identification system for the BaBar experiment,Nucl. Instrum. Methods A, 538 (1-3) (2005), p. 281

[12]J. Fast et al., The Belle II imaging Time-of-Propagation (iTOP) Detector, Nucl. Instrum Methods A, these proceedings.
[13] M. Düren et al., The Endcap Disc DIRC of PANDA, Nucl. Instrum. Methods A, these proceedings.

[14] S.-M. Sohn et al.S. Kim;, “A cmos image sensor (cis) with low power motion detection for security camera applications,” in IEEE International Conference on Consumer Electronics, ICCE. 2003, June 2003, p.(2003)

[15]C.-H. Chen, H.-J. Tsai, K.-S. Huang, and H.-T. Liu, Study for cross contamination between cmos image sensor and ic...

[16] A. Theuwissen, Ccd or cmos image sensors for consumer digital still photography? in International Symposium on VLSI...

[17] Mrs. Prajakta Jadhav1, Mrs. Shweta Suryawanshi2, Mr. Devendra Jadhav3 “Automated Video Surveillance eISSN: 2395 - 0056 | p-ISSN: 2395-0072” International Research Journal of Engineering and Technology (IRJET) Volume: 04 Issue: 05 | May - 2017

[18] Pawan Kumar Mishra “A study on video surveillance system for object detection and tracking” Nalina.P, Muthukannan . K

[19] Muskan Kumari,” Journals of Advancement in Electronics Design: 6 pp. 27-37 (1).”, March 23, 2023