Evolving Landscape of Spy Hardware: Insights from Literature

Dr. Shobha K. Bawiskar*
Assistant Professor
Department Of Digital & Cyber Forensics, Government Institute of Forensic Science
Chhatrapati Sambhajinagar, Maharashtra ,India 431001

Abstract:

This paper presents the analysis of the literature review on the spyware devices which are invading privacy concerns and challenging the forensic investigation procedures. These devices are increasingly used in the illegal activities and due to the lack of standardized methodology it leads to the loss of data, violation of data privacy, inappropriate results and challenging courtroom procedures. This research focuses on the study of spyware devices including hardware, software and applications that are used for the surveillance. This paper provides the comprehensive review of the existing techniques summarizing their positive and negative outcomes. The literature review studied that there is lot of development in the detection, manufacturing and technical analysis of the spyware devices. It provides the future point of research by the detailed analysis of the existing techniques and methodology. This purpose of this research is to provide the broader view of development in this domain and highlighting the legal and ethical considerations

Keywords: Forensic Framework, Spyware e-devices, Legal ethics, E-surveillance, cybercrimes.

Introduction:

A spyware device is any type of device, whether a physical gadget or a software program used to secretly monitor, track, or record a person's activities and data without their knowledge or consent. These devices have become a dangerous tool for stalkers, abusive partners, and corporate spies. When this type of evidence is found on the crime scene it is difficult to extract the evidence from it as it tries to destroy or try to vanish the evidence.

Spyware devices are categorized into three main parts-A) Audio B) Video C) GPS Trackers. This research provides the study about existing techniques for analyzing these types of evidences and providing scope to develop the framework to forensically analyse these evidences and can be called as admissible in the court of law. And also provides path to analyse these types of evidences to investigators to follow.

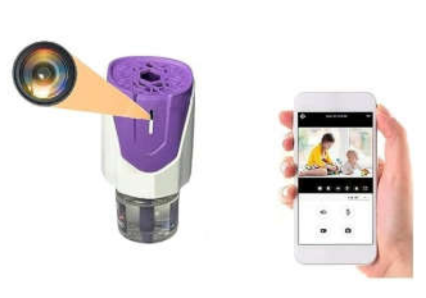
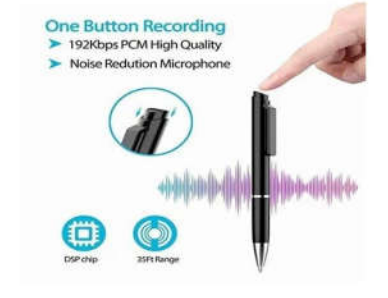
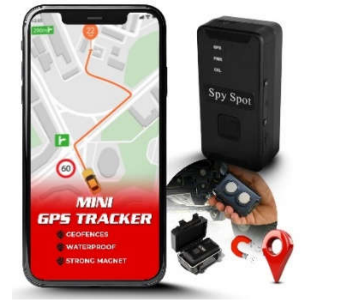
	 One Button Recording 192Kbps PCM High Quality Noise Redution Microphone DSP chip 35Ft Range	 Spy Spot MINI GPS TRACKER GEOFENCES WATERPROOF STRONG MAGNET
Fig 1(a) Wi-Fi Spy Camera Mosquito Repellent [1]	Fig 1(b) Spy Pen Digital Voice Activated Recorder [2]	Fig 1(c) Spy GPS tracker [3]

Fig 1. Spy Hardware Device

Purpose of topic:

1.Privacy Concerns: The spy devices record the sensitive information with the help of camera, audio recorder and GPs tracker and this leads to the privacy violation of individual.

2.Legal forensic methodology: Providing a forensic methodology leads to the ease in the criminal investigation and provides proper SOP to the investigation to follow for investigating these devices

3.Admissibility of spy evidences in court: Proper SOP leads to the accurate and true results of the investigation which helps to extract the data from devices which is admissible in the court of law

4.Easy surveillance: Accessibility of spyware devices to the normal people leads to the increase in the number of crimes

5.Prevention of spy evidences: Proper forensic SOP is essential because the experts may lose data from the devices by examining it without the proper methodology.

Aim:

Examining the existing techniques related to hardware, software and application type of spy devices.

Objective:

1. To do literature survey on spy hardware applications and identify research gap.
2. To study impact of the legal and ethical considerations by use of spy devices.

Selected samples for literature review criteria (inclusive and exclusive) are

Inclusive: selection-based criteria's
1.hardware spy devices: Focused only on the COTS
2. Included last 5 years research articles are considered for study purpose.

Exclusive: unselected based criteria's
1.Use of AI and machine learning
2. excluded last 5 years research articles are considered for study purpose.

Literature Review:

Spy hardware Devices:

Sr.no	Device used	Technique used	Result	Positive Outcomes	Negative Outcomes
1	Keychain spy camera [4]	Functionality comparison between UFED and Encase	Both software recovered 7 video clips but images recovered by UFED is 7529 images and by Encase less images was recovered	1.Successful Evidence Recovery 2.Validated Methodology 3.Highlights best Forensic Tool.	1.Use of single tool may lead to incomplete data recovery. 2.The findings is incomplete it requires metadata analysis.
2	Listening bugs and spy camera in devices like batteries, monitor watches, pens, identifications tags and tie pin (Wireless devices works on radio signals) [5]	1.RF Detector 2.Spectrum analysis 3.Non-Linear Junction Detector	RF detectors and spectrum analysis are effective methods for detection of active WSDs, NLJDs are more appropriate for detection of both active and passive WSDs.	1.RF Detector and Spectrum Analysis can detect live wireless spy devices 2.NLJDs are effective for the passive WSDs	1.Advancement of Spy devices 2.RF detector prone to false alarms and does not detect passive WSDs. 3.Passive WSDs are major threat
3	Wireless spy camera with Wi-Fi connection [6]	ESPIA: an application to detect spy camera uses machine learning	ESPIA is very effective to detect Wireless Spy camera and provides very fast process.	1.Does not require RF detector for detection. 2.Application is accessible by the general public. 3.Most effective, fast(1second) with high accuracy (96%) 3.Detect every camera regardless of their size	1.Only works with Wi-Fi camera. 2.Required trained model. 3. 4% risk
4	Spy camera (Both active and passive) [7]	Designed LAPD app for detection using smartphones Tofs sensors and give analyze in terms of 1.Shape & Distance Filters	LAPD achieves an 88.9% hidden camera detection rate, while the naked eye experiment yields only a 46.0% hidden camera detection rate	1.Makes smartphone as a detector without any external gadgets 2.Can find both active and passive cameras. 3.Accuracy with88.9%. 4.Pinpoints the location	1. Availability of ToF Sensors in smartphones. 2. Inaccurate 3D Localization. 3.Lengthy scanning process and scan 1 object at a time. 4. Hidden Camera Placement

		2.Deep Learning (AI) Filter 3.Field-of-View (FoV) Filter			
5	Wireless Spy Camera [8]	Uses galaxy S20+ smartphone for detection using ToF sensors	The smartphone's ToF sensor was more effective than commercial K18 detector	1.Smartphone is more effective than commercial detector 2.Easy to use 3.Works in Darkness 4.Proposed Clear Methodology for normal people	1.Availability of ToF Sensors in smartphones. 2.Optimal distance required too short and long can cause confusions 3. SCamF can only detect live streaming spy cameras on Wi-Fi networks. Other types of cameras that store the recorded video in the local storage or transmit the stored video later are not in the scope. 4. It does not consider highly-skilled attackers who figure out the underlying detection algorithms and actively modify traffic 5.Only works on WiFi enabled cameras
6	Wireless spy camera [9]	Stimulating and Probing technique used for detection (Using two app Blink and Flicker)	1.Blink (Simple App): Achieved over 90% detection with a very low false alarm rate (<0.8%) by having the user manually turn room lights on and off. 2.Flicker (Automated System): Proved more robust, using encoded, invisible light to achieve over 80% detection even in difficult conditions. It had a near-zero false alarm rate and worked on both live and offline video.	1.It is suitable with all the camera. 2.It is available to any smartphone user. 3.The "Flicker" system uses encoded, invisible light. 4.The technique works on encrypted traffic patterns, never viewing the actual video content	1.It only sees Wi-Fi cameras 2.You have to flip the light switch 3.The best version needs a special gadget Bright light or busy Wi-Fi can fool it
7	Wireless spy camera [10]	Created a system called DeepDespy which is an AI based tool	Gives 96% accuracy in detecting camera and it is fast and gives result in 1 sec	1.Effortless 2.AI driven with high accuracy (96%) 3.Automatic	1.only detect wi-Fi enabled Camera 2.The phone needs to be "rooted" and have special software installed, which is a major technical issue for the average person. 3. It Can Get Confused in Small Spaces
8.	Wireless spy camera [11]	The system uses a regular laptop or a small hobbyist computer (like a Raspberry Pi) that's been set up to listen to all the Wi-Fi traffic in a room	1.Reliably identify the "heartbeat" of a streaming spy camera. 2.Pinpoint the camera's location to within 30 cm (about one foot) in real-time	1.Does not need expensive gadgets instead work with laptop. 2.Based on the listening signals 3.Not AI driven 4. It works by looking at the "shape" of the data packets, not the content inside, so it doesn't matter	1.Only detect Wi-Fi camera 2.Somes does not give perfect location as there is large no of walls.

				if the video stream is encrypted.	
9	Wireless Iot Devices (camera, speakers, and other electronics) [12]	Detection based on Lumos system	1.Identify hidden device with 95% accuracy. 2. It locate the device's hiding spot with an average accuracy of 1.5 meters (about 5 feet) 3.It takes less than 30 minutes to find and locate all the hidden devices in two bedroom.	1.Provide info which device it is and their location 2.Compatible with phone or laptop 3.AI based system 4.Identify snooping smart devices	1.Detect only wireless devices not memory card devices 2.While an accuracy of 1.5 meters is good enough to tell you which part of the room to search, it won't tell you the exact drawer the device is in
10.	Hidden Wireless devices (camera, microphone, RF sensors) [13]	Designed SNOOPDOG sensor for detection	1.Detect snooping device with 95%accuracy 2. It was able to identify the type of device with 100% accuracy. 3. It was able to identify the type of device with 100% accuracy.	1.Detect any type of wireless sensor 2.It talks about if that camera is actively spying on you 3.Easily accessible with laptop or phone 4.Works by looking at the patterns of encrypted Wi-Fi traffic	1.Detect only wireless devices not memory card devices 2.To confirm a device is spying, you have to actively perform specific movements 3.Require phone manufacturers to allow easier access to Wi-Fi monitoring.
11	Hidden voice recorders [14]	Created **DeHiR-EC**, a system using specialized antennas and a computer to sense the invisible energy these recorders leak	1.Successfully detected every single one. 2.Achieved an overall success rate of over 92% from a short distance (about 8 inches	1.It's the first system that can reliably find offline, non-transmitting voice recorders. 2.The "tickle" method is a brilliant way to confirm a device's presence without ever touching it 3.	1.This is not an app. It requires specialized antennas, amplifiers, and a computer, making it a tool for professionals, not the average person. 2.The system only works from a short distance (less than a foot), so you'd need to know the general area to scan 3.If a recorder is hidden inside a metal case or a special shielding bag, this method won't work

Scope of research:

The scope of this research is to provide a detailed literature review on the spyware devices including hardware. It focuses on all the spyware devices which invading the privacy concerns and used for the covert surveillance. The aim is to study the devices used, techniques used for the analysis of these types of devices and understanding the positive and negative outcomes based on their results which leads to examine the existing the techniques. It also mentioned the ethical and legal challenges rising due to the nature of spyware devices.

Critical analysis:

In the digital age of modern technology, the use of spyware is increasing for the surveillance. These devices are used for the legitimate as well as for illegitimate purpose. It is broadly had role in parental monitoring, stalking partner, illegal activities and in government department. The nature of these types of devices are vulnerable for legal and ethical considerations. This are violating the privacy concerns, abusing partner and may also lead to violence.

This paper presents the literature review based on spyware hardware which is a means for covert surveillance. This research provides a detailed advancement in the field of covert devices for their detection, analysis and extraction.

The literature review on the spy hardware devices shows that these devices are divided into two categories i.e. active and passive devices. The active devices are those which shows the wireless connectivity and give the surveillance on the users smartphones while passive devices are those which stored the data in its local memory and does not have any wireless connectivity. This includes the devices like spy camera, spy audio recorders and spy gps trackers. The research inferred that in case of active spyware devices there is lot of advancement in the detection of these devices based on the ToF sensors in the smartphones and can locate the devices in the limited rang with the average 96% accuracy. The detection is based on the radiations mitigating the spy device and the sensors. In terms of hardware devices, the researchers are focused on the extraction of data from it and the manufacturing of the spy robot with such type of camera but the research lack in the detection of the passive type of devices and use of machine learning and AI. The detection of active devices is difficult in case of hidden arrangement from where the detectors are unable to manifest the radiations.

The literature review provides scope that ss this trend is increasing day by day in the crime it is crucial to develop the standard methodology for the forensic analysis of the spyware as it violating the ethical and legal guidelines of an individual and can be admissible as a source of primary evidence.

Ethical Challenges:

1. Privacy violations: The nature of spyware devices leads to the invasion of the person's privacy by controlling their own comfort.
2. Psychological Impact: By monitoring someone may also have affect in their relationships and their mental stability.
3. Misleading of information: The information collected from the spy devices can also vulnerable to the misuse and abuse of an individual.
4. Physical impact: The person being spied with uninformed manner can lead to the suicide and can dehumanize.
5. Consent: The uninformed consent of an individual can create a legal conflict.

Legal Challenges:

The nature of the spyware devices led to the invasion of the various laws in India as follows:

1. **Article 21 of Indian Constitution:**
   Art 21 of Indian Constitution states about the 'Right to life and Personal liberty' an also includes 'Right to Privacy'. The spyware devices which engage in surveillance should follow the procedure of law with regards to privacy is legitimate. If it fails to do so then it violates the fundamental right of an individual.

2. **Section 66(E) of IT Act:**
   It states about the violation of privacy by capturing, publishing, or transmitting of images of private area of a person without their consent. The spyware devices used for capturing the individual movement or actions without their knowledge or consent in a private setting it leads to the breaching of this section. It includes the penalty up to 3 years imprisonment and fine up to 2 lakhs rupees or both.

3. **DPDP Act 2023:**
   Digital Data Personal Protection Act,2023 involves the laws to protect the individual's digital personal data while allowing for lawful data processing. It requires following;
   a) Consent of an individual with exception for lawful purposes such as state functions, medical emergencies and employment.
   b) Data fiduciaries have obligations to ensue data privacy, provide data protection and delete data when its no longer needed. The spyware devices evading the individual's privacy and not satisfying the DPDP Act requirements led to the penalty up to 250 crores but exemptions for national security and public order.

Discussion and Future work:

All findings of the literature review discuss that the spyware devices are not only limited to the intelligence and government department but due to the low cost and easy availability on the online shopping platforms it is accessible to the common people. This stealthy and user-friendly interface of this type of device leads to the violation of privacy concerns, parental monitoring, stalking partner and challenging investigations.

Based on study done it is observed that the **hardware spy devices** focused mainly on the active type of spy devices but there are limitations while dealing with the passive devices. The techniques are developed for the detection of active devices due to its wireless connectivity it is mostly detect by the detectors with the help of Tof sensors in smartphones. The various apps are also developed using machine learning for the detection of active type of spy devices with large percentage of accuracy. While, literature review of passive devices focused on the extraction of data using various forensic tools. By reviewing the literature, it is observed that there is gap in the detection techniques for the passive devices and use of machine learning also for developing standard forensic methodology for the investigation of covert devices.

Study showed lack of standard framework which is the major research gap for developing the Standard Operating Procedures (SOPs) for the analysis of these types of spy devices for purposes of the legal investigation which is admissible in the court of law as evidence with ethical considerations.

Research gap:

1.Detection of passive spyware devices.
2.Analysis of hardware
3.Deep analysis of COTS
4.Only focuses on COTS devices and

Conclusion:

The increasing use of the spyware devices in the crimes leads to the breaching of privacy concerns, legal and ethical considerations. This paper studied that the researchers developed many detection and preventive techniques for the spy devices including hardware to avoid the violation of sensitive information with uninformed consent. Some focused on the manufacturing and technical analysis which shows the high accuracy results. In the technical analysis, they provide a step-by-step guidance to examine the spy devices. Here vulnerabilities, challenges, positive and negative outcomes are also highlighted. And the researchers are trying to solve this problem. This paper presents the detailed analysis of the spyware devices which provides the scope to carry forward the research in this domain.

Reference :

1. https://www.spyworld.in/wp-content/uploads/2025/04/Long-Time-Recording-Spy-Camera.jpg.
2. https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.indiamart.com 2Fproddetail%2Fgmad019-spy-pen-digital-voice-activated-recorder-8gb-audio-mini-hidden-recording-device-23658005862.html%3Fsrsltid%3DAfmBOorLqEYeiZ07414-JqOek7k7QzbeB_4Bt9L67G6FoMMSeKYUkc8E&psig=AOvVaw1-YIzHL2jUAzBESdc8H33v&ust=1753458879418000&source=images&cd=vfe&opi=89978449&ved=0CBUQjRxqFwoTCKDc8b7t1Y4DFQAAAAAdAAAAABAE41.
3. https://www.google.com/imgres?q=spy%20gps%20trackers&imgurl=https%3A%2F%2Fm.media amazon.com%2Fimages%2FI%2F715ajKAZiLL.jpg&imgrefurl=https%3A%2F%2Fwww.amazon.in%2FSpy-Spot-Tracker-Magnetic-Waterproof%2Fdp%2FB0CH989P6S&docid=edIz1mFuyvbgnM&tbnid=Nyw0o77lyJ109M&vet=12ahUKEwjHtfjM7NWOAxWP6zgGHT63BNYQM3oECAoQAA.i&w=2000&h=2000&hcb=2&itg=1&ved=2ahUKEwjHtfjM7NWOAxWP6zgGHT63BNYQM3oECAoQAA
4. Prasoon, P., Uplenchwar, G. R., Ramakrishnan, P. N., & Krishna, M. (2024). Forensic data extraction from UVC camera-embedded spy devices: A case study. *International Journal of Engineering Research & Technology*, *13*(1). http://www.ijert.org
5. Sathyamoorthy, D., Jelas, M. J. M., & Shafii, S. (2014). Wireless spy devices: A review of technologies and detection methods. *Editorial Board*, *7*(11), 130.
6. Joy, S. E., Plement, N., Shinu, C. M., Sankar, S. R., & Mathew, A. (2023). Espía: A review of application to detect spy camera implementation. *International Research Journal of Modernization in Engineering Technology and Science*, *5*(6), 3128–3131. https://doi.org/10.56726/IRJMETS42296
7. Heo, J., Gil, S., Jung, Y., Kim, J., Kim, D., Park, W., Kim, Y., Shin, K. G., & Lee, C.-H. (2022). Are there wireless hidden cameras spying on me? In *Proceedings of the 38th Annual Computer Security Applications Conference* (pp. 714–726). Association for Computing Machinery. https://doi.org/10.1145/3564625.3564632
8. Sami, S., Tan, S. R. X., Sun, B., & Han, J. (2021, November). LAPD: Hidden spy camera detection using smartphone time-of-flight sensors. In *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems* (pp. 288-301).
9. Liu, T., Liu, Z., Huang, J., Tan, R., & Tan, Z. (2018, June). Detecting wireless spy cameras via stimulating and probing. In *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services* (pp. 243-255).
10. Dao, D., Salman, M., & Noh, Y. (2021). DeepDeSpy: a deep learning-based wireless spy camera detection system. *IEEE Access*, *9*, 145486-145497.
11. Edozie, E., Wantimba, J., Kalyankolo, Z., Adabara, I., & Ukagwu, K. J. (2020). Design and Analysis of a Lab IP Spy Camera and Alarm System using Raspberry Pi and ATMEGA328P.
12. Sharma, R. A., Soltanaghaei, E., Rowe, A., & Sekar, V. (2022). Lumos: Identifying and localizing diverse hidden {IoT} devices in an unfamiliar environment. In *31st USENIX Security Symposium (USENIX Security 22)* (pp. 1095-1112).
13. Singh, A. D., Garcia, L., Noor, J., & Srivastava, M. (2021). I always feel like somebody's sensing me! A framework to detect, identify, and localize clandestine wireless sensors. In *30th USENIX Security Symposium (USENIX Security 21)* (pp. 1829-1846).
14. Zhou, R., Ji, X., Yan, C., Chen, Y. C., Xu, W., & Li, C. (2023, May). Dehirec: Detecting hidden voice recorders via adc electromagnetic radiation. In *2023 IEEE Symposium on Security and Privacy (SP)* (pp. 3113-3128). IEEE.