See No Evil: Discovering Covert Surveillance Devices using Thermal Imaging

Agustin Zuniga‡, Naser Hossein Motlagh‡, Mohammad A. Hoque‡,
Sasu Tarkoma‡, Huber Flores∗, Petteri Nurmi‡
‡ Department of Computer Science, University of Helsinki, Helsinki, Finland
∗ Institute of Computer Science, University of Tartu, Estonia

***Abstract*—Covert surveillance devices ranging from miniature cameras to voice recorders are increasingly affordable and accessible on the market, raising concerns about surreptitious and unauthorized observation of people. The present paper contributes an innovative method for discovering covert surveillance devices using thermal imaging integrated with off-the-shelf consumer devices, such as smartphones. We develop a simple yet efficient processing pipeline for identifying covert devices and demonstrate its effectiveness through extensive and systematic evaluations that consider different types of covert cameras. Our results show robustness against a wide range of factors, including distance to other electrical objects, the environment and luminosity of the space where measurements are taken, the type of camera, and partial occlusion of the hidden devices.**

***Index Terms*—thermal sensing, thermal imaging, privacy, pervasive surveillance, mobile computing, sensing, IoT, pervasive computing**

I. Introduction

Covert surveillance is an unfortunate yet an increasingly ubiquitous and global threat to privacy. Indeed, incidents of people being recorded without their consent in apartments (e.g., in Airbnb apartments) are frequently featured in media [1] and unwarranted recording with malicious intent is also a regular feature in public spaces [2]. This negative trend is driven by the miniaturization of cameras and recording devices as smaller and better concealed devices have become increasingly affordable and accessible. For example, surveillance devices that are integrated into USB sticks, pens, smoke detectors, set-top-boxes, photo frames and other common household objects can be purchased cheaply online. Besides violating the privacy of individual, being subjected to surreptitious surveillance can be highly damaging, degrade trust, and lead to anxiety [3]. Users have also indicated a strong desire to be aware of covert surveillance devices, e.g., a survey of Airbnb users showed that over 80% of users wanted to know the locations of any devices that can potentially monitoring them [4]. To reduce the risks and negative consequences of unwarranted surveillance, easy-to-use solutions that can detect covert surveillance devices are needed.

The simplest and most common way to identify covert surveillance devices is to manually inspect the environment and try to detect anything that is suspicious (e.g., a fire alarm placed on top of a bed). Manual inspection can be difficult as devices may be inactive, programmed to work only at certain hours, or placed in a location where the user does not suspect to look for one, calling for methods that can assist the user. The most common ways to support manual inspection are based on using lens reflectance detection, magnetic field analysis, or network traffic analysis. In the case of lens reflectance, an illumination source, such as a flash or an infrared light, is used to illuminate the environment and cameras are detected from reflections captured on a camera [5], [6]. Magnetic field analysis relies on detecting electromagnetic signatures using the magnetometer of the device [7]. Finally, network analysis relies on identifying abnormal traffic in the network and correlating that with activity taking place in the space [8]–[10]. The main issue with these techniques is that they require relatively heavy interaction from the user and the cameras can actively take countermeasures to avoid the recognition. For example, illumination-based detection is sensitive to the angle at which the light is pointed toward the hidden camera [6] whereas magnetic field detection is sensitive to the the strength of the magnetic field that the surveillance device induces and can be mitigated by putting the devices to sleep when the environment is being scanned. Network-based detection, on the other hand, only works for devices that are connected to the network and can be prevented by piggybacking the camera traffic with other traffic in the network, masquerading as another device [11], delaying the transmissions to periods that do not correlate with any activity, or only using internal storage without transmitting the recordings; see Table II for a summary of the different approaches.

We contribute an innovative approach for supporting the detection of covert surveillance devices using *thermal imaging* integrated with commercial-off-the-shelf devices, such as smartphones. The idea is to use a thermal camera to scan the environment and to use simple processing techniques to identify areas that correspond to potential covert surveillance devices. Thermal imaging is increasingly available on consumer devices, e.g., there are external thermal cameras that can be attached to the charging port of smartphones, and it can offer robust detection even against active countermeasures. As temperature decays slowly, thermal cameras are also capable of recognizing devices that have recently been

monitoring. We build on this increasing availability to develop a pipeline for identifying covert surveillance devices under a variety of conditions and demonstrate the effectiveness of our technique against common countermeasures. The basic idea of using thermal cameras to measure thermal emissions in the environment itself has been explored previously [12]–[15] but thus far no work has demonstrated how this capability can be harnessed to detect covert surveillance devices or how this capability works in different conditions. Indeed, the cost and limited resolution of thermal cameras combined with performance issues in detecting devices that have a low thermal signature or that are close to another device have resulted in limited adoption of the technique. We take a step forward by developing an efficient processing pipeline for identifying surveillance devices from thermal images and demonstrating that it works robustly in a wide range of conditions and against common countermeasures. We also provide insights into how the thermal emissions of devices partially or almost completely shielded by the surroundings can be detected.

We systematically assess factors that affect detection performance, demonstrating that ambient light, distance to target, partial or near to complete occlusion (e.g., by covering the device), and proximity to other heat sources decrease the intensity of thermal signatures but do not prevent the detection of devices that are monitoring the user or the environment. We also compare thermal imaging against magnetic field and network traffic analysis, demonstrating the thermal imaging can detect covert devices more easily and efficiently than these techniques. Our results pave the way toward adopting thermal imaging as a modality for supporting the detection of covert surveillance devices in everyday contexts.

II. Thermal Imaging for Hidden Camera Detection

Any devices that are operating emit thermal radiation [14], [15] with particularly the power source, CPU, and I/O operations resulting in a clearly observable thermal signature. The idea in our approach is to use off-the-shelf thermal cameras, which can be embedded onto smartphones (e.g., the Caterpillar CAT S60 and S61) or attached as a separate sensor (e.g., FLIR ONE cameras connected to the charging port), to monitor the environment and to detect heat signatures resulting from these operations. Any thermal signatures that are observed in unexpected or otherwise suspicious locations (e.g., above a bed) are candidate locations for a covert surveillance device and should be inspected in detail.

Figure 1 illustrates the overall approach and shows the general processing pipeline that is applied on the thermal images. The processing pipeline builds on our earlier work [16] and integrates steps for background removal, image segmentation (using blob detection), and candidate device identification. First, a thermal camera is used to record pictures or video of the area of interest. Using individual images is often better than recording continuous video as the performance of off-the-shelf thermal cameras tends to degrade in continuous use due to the camera heating [17]. If continuous video is used, calibration is recommended to improve the quality of the measurements [17]. The collected images are then cleaned and pre-processed. Thermal noise in the image is removed by applying a Gaussian blur filter. The colour space is then converted to grayscale and an adaptive mean thresholding algorithm with binary threshold is used to detect regions with a high thermal radiation. The average temperature of these regions is compared to the ambient environment and regions that differ significantly from the ambient environment are considered as candidates of surveillance devices. The final decision on whether they are surveillance devices or not is the responsibility of the user and our solution merely highlights all devices that are available in the environment. This decision can be supported through suitable visualizations, e.g., using augmented reality interfaces [18].

The intensity of the thermal fingerprint generally depends on the level of processing the device performs. The power source, CPU and I/O operations tend to result in the clearest thermal signatures, but also other components result in thermal radiation, e.g., network usage requires processing which can also be identified from the thermal signature [14]. Similarly, camera aperture and lens tend to be clearly observable as they provide an outlet for internal heat to dissipate [17]. Note that processing does not need to be currently ongoing as thermal emissions take time to decay. Thus, the only requirement is that the device has been on sufficiently recently (e.g., within the previous 5-10 minutes, depending on the extent of processing). Similarly, objects that have been recently hidden can contain residual thermal signatures resulting from the person that hid the devices [16] and thus any devices that are currently inactive but that have been recently hidden can be discovered with thermal imaging.

Naturally, there are also limitations in the use of thermal imaging. First, the resolution of off-the-shelf thermal cameras tends to be low, which means that the camera needs to be taken sufficiently close to the objects ($\approx$ 6ft/2m). Second, the intensity of the thermal fingerprint depends on the *emissivity* of the material which determines how much of the internal heat is radiated to the environment. Common materials, such as plastics, tend to have high emissivity and thus they can be easily detected. Lowest emissivity values tend to correspond to surfaces that are bright and have high reflectivity (e.g., aluminium, copper, brass) and that are rare as casing materials of electronic devices. Finally, surveillance devices placed in close proximity of other sources of thermal radiation can result in the thermal signature of the surveillance device becoming merged with the signature of the device housing it, especially when the monitoring is carried out from a distance. For example, a digital frame generates thermal radiation along the screen area and thus a surveillance device placed near the edge of the screen can be difficult to spot from the thermal fingerprint. In such cases, the surveillance devices can be detected through more advanced processing techniques that identify variations in the thermal fingerprint within an area or detect areas that appear extensions of another device. We consider these factors as part of our experiments.

III. Experimental Setup

We conduct extensive experiments to demonstrate the robustness of thermal imaging in detecting surveillance devices

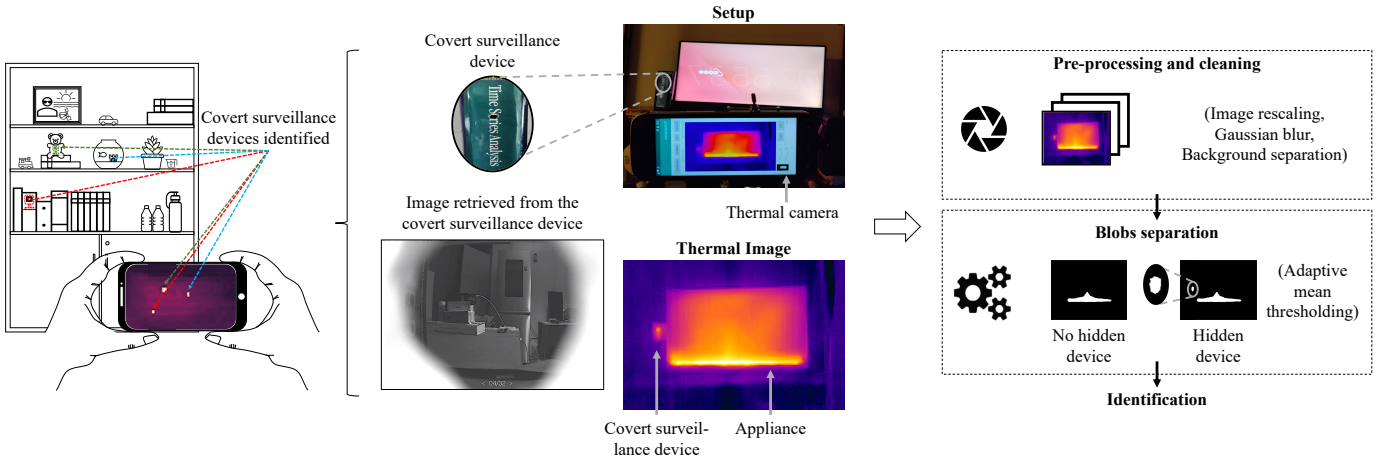

Fig. 1. Thermal imaging targeting a covert surveillance device in a living room and ambient light conditions, and the processing pipeline for recognizing covert surveillance devices from thermal camera input.

in a wide range of conditions and against common countermeasures. We next detail our experimental setups.

Devices: We use commercial off-the-shelf IP cameras that are accessible and easy to buy in the market. The cameras were chosen to cover representative features that are relevant for surveillance purposes, including: video resolution (1080p, 720p), audio transmission (enable, disable), motion detection (enable, disable), power source (power cord, battery-powered) and access mode (on-line: wireless, off-line: local storage). While all of these cameras are standalone devices instead of household devices that hide the camera, they offer control over camera features. We emulate housing the camera in another device by manipulating the experimental design and camera configurations. The WiFi IP devices used in our experiments are: (i) TP-Link Tapo C100: Home security power cord camera, (ii) D-Link DCS-8000LH: Mini power cord camera with intelligent motion detection, (iii) Nedis WIFICI11CWT: power cord camera with climate sensors, (iv) Reolink Argus 2: battery powered indoor and outdoor camera with micro-SD card for local storage. Additionally, we consider the rear-view camera of a Samsung Galaxy S6 as a representative example of a consumer device repurposed as a surveillance tool. The camera's proprietary apps were used to access the devices and to configure the cameras. On the Samsung Galaxy S6 we used *BabyMonitor*, a WiFi baby monitoring app for Android.

Materials: We use manufactured goods to cover the cameras during our experiments: a cardboard box (single face board E-Flute), a fabric shopping bag (material: 100% cotton, thickness: ≈ 2.5 Mil) and a thermos bottle (material: transparent borosilicate glass, diameter: $6.5\,\mathrm{cm}$). These were chosen as representative examples of common household materials that can be used to hide a camera. A $0.5\,\mathrm{cm}$ diameter hole was drilled in the cardboard and the shopping bag to expose the lens of the hidden camera. All cameras considered in the experiments have plastic housings and thus our experiments also cover the case where the surveillance device is directly integrated into a household object.

Apparatus: We using a FLIR One Pro camera with a thermal resolution of 160×120 and a horizontal field of view of $50°$ that is attached to the USB-C port of a OnePlus Nord N100 smartphone. Thermal images were collected using a custom app that interacts with the FLIR Mobile API.

Testbeds: We first consider a controlled testbed where the cameras are placed in front of a matte navy blue fabric background. The testbed is used to ensure that thermal fingerprints are always captured under the same conditions as the single-color background reduces the likelihood of introducing heat reflection or thermal dissipation noise from other sources. We supplement this experiment with measurements collected from an office room where furniture and other objects are used to hide the cameras. In both test environments, the sensing unit was set on a tripod at one meter distance from the sampled device to keep the same position and FoV relative to the device. The materials used to cover the devices were located in front of the device. Cardboard and fabric were modified to case and wrap the device. The glass bottle was used to run two tests: having the bottle empty or full. The main experiment was performed in dark (luminosity $0\,\mathrm{lx}$) to reduce the effect of ambient light. Separate experiments were carried out to assess the effect of distance and luminosity. Measurements are taken once every 10 seconds for a total duration of two minutes, which helps to reduce variance in the measurements and is approximately the gap between successive camera calibration cycles [17]. Between measurements, we placed the sensing unit in a fridge with a temperature of $2\,°\mathrm{C}$ to $4\,°\mathrm{C}$ for 2 minutes to reduce possible errors from the thermal camera overheating.

Measurements: In total, we consider three experimental designs. First, we performed an experiment to determine the thermal fingerprint of the devices and the effect of different light conditions and distance. Second, we measure each camera in different configurations (video resolution, audio transmission and motion detection) to determine the changes in thermal fingerprint in different operating configurations. Finally, we evaluate the effectiveness of thermal imaging to detect cameras masked by different materials. All experiments were carried out in a regular office space with an ambient temperature of $19\,°\mathrm{C}$ to $22\,°\mathrm{C}$ and relative humidity of $30\% - 34\%$.

IV. Results

A. Characterizing Surveillance Devices

We first use the measurements from the controlled testbed to analyse the differences in the temperature of the devices operating under different configurations and demonstrate that thermal sensing can be used to characterize different camera configurations. We consider eight sets of measurements covering all possible combinations of video resolution, audio transmission and motion detection configurations.

Figure 2a shows the results of the experiment. We observe a clear difference in the thermal fingerprint of the different cameras. The devices that incorporate extra-functionalities (e.g., climate sensing, telephony, mobile connectivity) have the highest thermal fingerprint as they include more internal components that produce heat. As expected, enabling more features during the operation increases the temperature of the device. Video resolution has the highest impact in temperature: using a Full HD video resolution can result in the temperature of the device increasing by $2\,^{\circ}\mathrm{C}$ to $6\,^{\circ}\mathrm{C}$ compared to using HD resolution. A Kruskal-Wallis test indicates the differences in thermal fingerprint to be significant, ($\chi^2 = 11.636$, p$< .05$) and posthoc (Dunn-Bonferroni) comparisons show the differences to be significant for all the devices. A Friedman Test considering different configurations as experimental conditions shows statistically significant differences in thermal fingerprint: 720p resolution ($\chi^2 = 15$, p< 0.01, W$= 0.05$) and 1080p resolution ($\chi^2 = 15$, p< 0.01, W$= 0.84$). Conover's posthoc comparisons (Holm-Bonferroni) prove the differences to be statistically significant in both resolutions for the pair (Voice: OFF, image recognition: OFF - Voice: ON, Image recognition: ON). In practical terms, these results mean that, besides being able to detect cameras that are recording, thermal imaging can offer some insights into the features of the surveillance device has (e.g., resolution, voice recording, or image recognition).

B. Effect of Light and Distance

We collect four set of measurements corresponding to two luminosity conditions (ambient: $40\,\mathrm{lx}$, darkness: $0\,\mathrm{lx}$) and two distances between the object and the sensing unit (1 meter, 2 meters) to determine how different operating conditions affect the thermal fingerprints of the surveillance cameras. The instantaneous field-of-view (IFOV) of the FLIR One unit indicates that placing the thermal camera at one meter distance provides accurate thermal measurements for an object that is approximately $0.5\,\mathrm{cm}$ in size, whereas a distance of two meters supports objects that are $1\,\mathrm{cm}$ in size. Since hidden cameras can be commonly placed inside small objects (e.g., a smoke detector or a light casing), two meters should provide sufficient accuracy for detecting covert surveillance devices in practice.

Figure 2b shows that both luminosity and distance affect the thermal fingerprints. For luminosity, a Friedman test shows the differences in thermal signatures to be statistically significant ($\chi^2 = 51.48$, p< 0.001, W$= 67.81$). The thermal signatures are more intense in darkness, and hence carrying out an inspection in dark is likely to reveal covert devices better than in ambient light conditions, though the devices remain distinguishable also in ambient light. For distance, a Friedman Test verifies that the differences similarly are statistically significant ($\chi^2 = 45.078$, p< 0.001, W$= -61608.78$). Shorter distance results in the surveillance device being covered by a higher number of pixels and making the device easier to identify. Taken together, the results show that the thermal signatures are observable even at two meter distance and in ambient light, which suggests that thermal imaging is a feasible and a practical solution for detecting covert surveillance devices.

C. Effect of Different Materials to Hide Cameras

We next consider the measurements taken in the office environment. Figure 3 shows how the warmest area of the camera is reduced when the different materials are used to cover the cameras. A small area of the thermal fingerprint remains visible when the camera is covered by cardboard and fabric as they require the lens to be exposed. In contrast, when the device is placed behind the transparent borosilicate glass, it does not require an observation hole. A Friedman test was used to confirm that the changes in thermal signatures caused by the different materials indeed are significant ($\chi^2 = 15$, p< 0.001, W$= 0.533$). Posthoc (Dunn-Bonferroni) comparisons showed differences to be statistically significant for all the pairs except when an empty glass container is in front of the camera. Thus, thermal imaging can identify covert surveillance device that are partially or nearly completely covered by other materials, with the exception of glass – though this leaves the camera visible to the user. Materials that require exposing the camera lens reduce the size of the thermal signature, but the devices can still be observed. Darkness and taking the thermal camera as close as possible help to enhance the signature and make detection easier. For glass, the effects depend on thickness. Thicker glass can absorb most of the thermal radiation, provided that the camera is not in direct contact with the glass. If the camera is in direct contact, some of the thermal radiation is absorbed by the glass and the thermal signature would gradually become observable. Conversely, the user can cause thermal reflections in the glass [19]. These can cause false positives – which would cause the user to investigate the location – or obfuscate the thermal signature. Naturally, when the device is covered by glass, it is easier to observe by the naked eye and in practice the only countermeasure is to hide the camera behind a one-way mirror.

We also (i) vary the distance between the cover material and the surveillance camera (0 cm, 0.5 cm, 1 cm), (ii) increase the thickness of the fabric layers (≈ 2.5 Mil, ≈ 5 Mil) and (iii) compare having the bottle filled with water or being empty (the diameter of the glass bottle is 6.5 cm). Friedman test confirmed that the differences in thermal signatures were significant across all devices and conditions: fabric ($\chi^2 = 5$, p< 0.05, W$= 0.95$) transparent borosilicate glass ($\chi^2 = 5$, p< 0.05, W$= 1$) and cardboard ($\chi^2 = 8.4$, p< 0.05, W$= 0.8$). Thickness of the covering material simply reduces the intensity of the thermal signature and makes it closer to the ambient environment, but the signature remains distinguishable for all cameras that were tested. Specialized spy surveillance

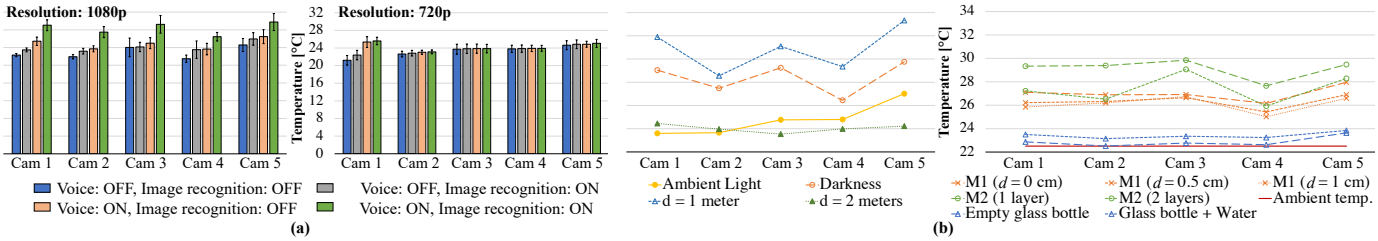

Fig. 2. (a) Mean temperature of the cameras (Cam) for different configurations (resolution, voice, recognition). Mean ambient temperature: $19.57 \pm 0.65°C$. (b) Right: Effect of light and distance in the thermal fingerprints. Mean ambient temperature during the tests: $20.46 \pm 0.16°C$ (light), $22.32 \pm 0.19°C$ (distance). Left: Thermal fingerprint of the surveillance devices for different cover materials (M1: cardboard, M2: Fabric). In cardboard, d indicates the distance between the cardboard cover and the camera).

equipment has been designed for low-power operation and could potentially result in signatures that are insufficiently distinguishable, particularly when the devices are covered, but in our experiments, this was not the case. For the glass container, filling it with water results in the thermal fingerprint becoming again observable due to reflection characteristics of the container changing. Finally, for the cardboard, posthoc tests (Dunn-Bonferroni) indicate that differences in thermal signatures are statistically significant for the pair of distances (0 cm, 1 cm), i.e., the signature is only affected once the surveillance device is sufficiently far from the edge of the material covering it. In practice, these results mean that even active countermeasures, such as occluding the camera or covering it with other material, are unable to prevent the thermal signature being visible. Indeed, the main effect is that the intensity of the thermal signatures decreases which does not prevent detection but makes detecting surveillance devices more difficult and requires bringing the thermal camera closer. The applicability and robustness of the imaging can further be improved by using more advanced processing techniques and higher resolution thermal cameras, which are expected to become a reality in the near future.

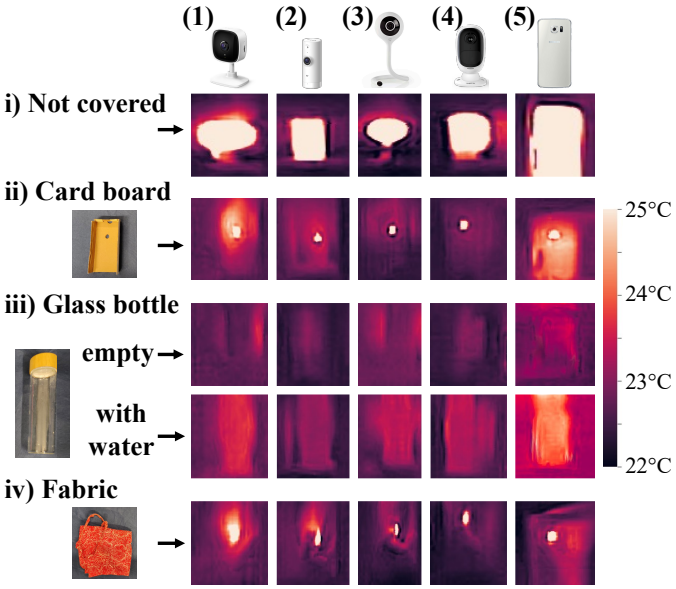

Fig. 3. Thermal fingerprint of hidden cameras with different materials. Cameras: (1) TP-Link Tapo C100, (2) D-Link DCS-8000LH, (3) Nedis WIFICI11CWT, (4) Reolink Argus 2, (5) Samsung Galaxy S6.

D. Proximity to Source of Thermal Emissions

Another way to make detection difficult is to camouflage the device by placing it close to a source of thermal emissions. For example, the screen components of a digital frame emit thermal radiation and placing a camera close to the edge of the screen could mask the thermal signature of the surveillance device (see the thermal image in Figure 1). We next evaluate this effect considering representative examples of common sources of thermal emissions at apartments: smart LED TV (Samsung UE32T4302 32”), microwave (Samsung MS23K3515AW/EE), wall mount radiator, and a fluorescent T8 warm tube light (80 cm, 3000 K, 20 W). We consider the Reolink camera due to its portability and we evaluate different positions relative to the source of additional emissions: camera (i) in front of the object and (ii) next to the object. When the surveillance device is placed directly in front of an object that emits thermal radiation, the background radiation can mask the device and make detection infeasible. In this case, detection requires manipulating the thermal environment [4]. For example, switching the power off would result in thermal radiation dissipating. As materials have varying dissipation characteristics [16], the surveillance device could be detected by analysing differences in dissipation within the region covered by the device serving as the source of background thermal emissions. In contrast, when the surveillance device is placed next to the object emitting thermal radiation, the thermal signature is detected as an extension of the heat source. Discovery in such cases is possible but requires more advanced processing, e.g., segmenting the area into smaller regions and examining areas where the geometric consistency of the fingerprint is compromised.

E. Comparison to Existing Techniques

As the final step of our evaluation, we empirically compare thermal imaging against magnetic field-based detection and network traffic analysis. In the first case, we consider four popular Android Hidden Camera Detector apps (Ahmadyar, FutureApps, A.K.N Soft.inc, i6Apps) that use magnetic field to discover hidden cameras. The apps use a threshold on the magnetic field to detect devices. We take measurements at 1 cm and 10 cm distances from the devices. Notice that in the case of the glass bottle, distances should consider

TABLE I
PERFORMANCE OF HIDDEN DEVICE DETECTION APPS ON MOBILE DEVICES USING MAGNETIC B-FIELD, NETWORK TRAFFIC ANALYSIS AND THERMAL IMAGING FOR DIFFERENT CONFIGURATIONS AND COVERING MATERIALS. FOR THE GLASS BOTTLE, DISTANCES ARE 6.5 CM LONGER DUE TO THE BOTTLE DIAMETER. *POTENTIAL CAMERA DETECTED.

		B-Field [μT]								Network Traffic Analysis [bytes]		Thermal Imaging
		Ahmadyar		FutureApps		A.K.N		i6Apps		Wireshark		Flir ONE
Setup	**Device**	**1 cm**	**10 cm**	**1 cm**	**10 cm**	**1 cm**	**10 cm**	**1 cm**	**10 cm**	**Source**	**Destination**	**Temperature [$^\circ C$]**
Only WiFi	Reolink	138*	30	92*	30	130*	30	88*	36	266.8±336.1*	152.4±235.9*	26.44*
	Galaxy S6	28	26	25	25	26	25	27	25	317.6±489.1*	206.8±399.2*	29.76*
No WiFi	Reolink	124*	20	134*	15	122*	25	124*	26	0	0	29.62*
	Galaxy S6	28	28	28	28	27	26	29	28	0	0	31.27*
Cardboard	Reolink	124*	30	90*	26	128*	31	86*	35	-	-	26.16*
	Galaxy S6	23	22	24	24	22	21	24	24	-	-	27.96*
Fabric	Reolink	122*	24	81*	20	121*	34	81*	30	-	-	27.66*
	Galaxy S6	26	25	24	23	26	25	26	25	-	-	29.48*
Glass Bottle	Reolink	35	30	26	21	28	24	33	28	-	-	22.63
	Galaxy S6	27	26	25	25	26	25	26	26	-	-	23.64*
Glass Bottle +	Reolink	32	28	27	24	27	23	26	22	-	-	23.24*
Water	Galaxy S6	23	23	24	24	26	26	26	26	-	-	23.84*
Baseline (magnetic field threshold / No camera in Network / Ambient temperature)		**120**		**80**		**120**		**80**		**255.0±346.8**	**127.1±178.2**	**22.51**

also the diameter of the bottle (6.5 cm). Network traffic analysis is implemented using Wireshark to capture 3-minute packet transmission in the local WiFi network. The baseline corresponds to the network traffic without cameras in the network. For the experiments, we consider the devices that have presented the highest and the lowest thermal fingerprint in Section IV-C: Reolink and Samsung Galaxy S6.

Table I shows the results for the different experimental conditions. The use of magnetic field has difficulties in discovering (i) the Samsung Galaxy S6, (ii) distant devices and (iii) devices placed behind glass. Network analysis allows to identify abnormal traffic conditions and their source, but requires accessing the local network, does not give the location of the source, requires longer monitoring to quantify surveillance patterns, and fails to detect devices that are not connected to the network. An advantage of network traffic analysis is that it allows to identify the camera type.

Table II summarizes the key advantages and disadvantages of different techniques. As we have shown, thermal imaging can detect the broadest range of surveillance devices, and it operates robustly against various countermeasures, except when the devices are covered by glass. Thus, thermal imaging provides an effective solution that works well as standalone solution or that can complement other approaches. In practice, the best solution is to combine multiple techniques as this would allow finding all possible surveillance devices. Lens reflection can be used to detect devices that have not been active, e.g., those that have a timed delay before starting the monitoring, whereas network-based monitoring can identify objects that are transmitting but are covered by other objects or too small for camera-based methods to recognize.

V. DISCUSSION

Stakeholders: End-users that occupy a space are the primary beneficiaries for thermal imaging. This is particularly relevant on markets that connect users providing services with those that consume them, e.g., Airbnb, Uber, where there often is a lack of trust and a high risk to use those services. Likewise, vendors manufacturing thermal cameras and other infrared devices can be interested on implementing methods in their products to reduce and prevent malicious uses of thermal imaging to carry out privacy attacks.

Thermal imaging attacks: Unfortunately thermal imaging can also be beneficial for attackers as it can be used to identify locations where the surveillance devices are unlikely to be observed. For example, while our method can be used to discover surveillance devices, it can also be used to find a spot where the cover device can blend with the background to avoid detection, e.g., a camera placed next to a heating source. Another issue with thermal imaging is that it can disclose other privacy information from the individuals. For instance, residual thermal radiation that is transferred from users to objects can disclose gender characteristics of individuals [16]. Likewise, thermal attacks have been successfully used to steal passwords and PIN codes (ATMs) by examining the residual thermal radiation in keypads [20] and hence there is also a need for obfuscation methods that support the thermal imaging.

Potential Improvements: Naturally, there is room for further improvements. For example, while we have shown promising results in an office-like environments thermal imaging may not necessarily perform well in other environments. Generally, the performance depends on the resolution of the camera, the distance from the covert surveillance device, and the temperature difference between the surveillance device and the ambient environment. Information about the current ambient temperature could be used to predict likely values of thermal fingerprints for different distances and any sources of thermal radiation could be compared to these values. While the experiments demonstrated robust performance in general, the recognition of devices that are placed in proximity of other heat sources needs further improvements. Segmentation techniques that consider both the thermal values and the shapes of the blobs can facilitate discovering devices that are close to heat sources. Alternatively, if the thermal environment can be manipulated, e.g., by switching certain devices or heat sources off, this can help discover covert surveillance devices by examining differences in heat dissipation. Finally, naturally a wider range of devices could be investigated, e.g., dedicated spy devices that hide the camera (or other surveillance sensor) inside a pen, USB stick or other object. We focused on devices

TABLE II
COMPARISON OF DIFFERENT APPROACHES FOR DETECTING COVERT SURVEILLANCE DEVICES.

Method	Advantages	Disadvantages
Manual inspection	Requires no external devices	Requires knowledge of device locations, difficult to find well-hidden devices, e.g., those integrated into other objects
Lens Reflection	Easy to use. Works also when the surveillance device is inactive.	Requires lens to be sufficiently exposed to capture the reflection, sensitive to angle of detection, requires close distance to objects, not applicable to other types of surveillance devices (e.g., microphones)
Network monitoring	Reasonably easy to use, effective at detecting networked surveillance devices, provides information on device type.	Can only detect devices that are transmitting, does not reveal device location, vulnerable to active countermeasures (e.g., piggybacking transmissions with other traffic)
Magnetic field	Simple to use, can identify devices that are not transmitting data, many apps readily available for smartphones	Vulnerable to small changes in the electromagnetic field, threshold for identifying covert devices heuristic and varies across apps
Thermal Cameras	Detects a wide range of devices, robust against many countermeasures	Requires specialized equipment (thermal camera), works best at close distance, vulnerable to devices hidden behind a reflective object

that can be obtained without restrictions but our method is also capable of detecting other types of devices, provided that the thermal camera is taken sufficiently close to the sensor and the sensor is active during the monitoring. In practice, we would expect thermal imaging to be but one of the methods that are used for detecting covert surveillance devices and other techniques, such as network analysis, could be used to complement it. Finally, it should be noted that thermal cameras should not be pointed at humans and discovery of devices placed on the human body requires alternative solutions.

VI. SUMMARY AND CONCLUSIONS

We presented an approach that can be used to discover covert surveillance devices using thermal imaging and conducted extensive experiments to analyse how different environmental factors and potential countermeasures influence the detection performance of thermal imaging. We demonstrated that by looking closely at the characteristics of thermal signatures produced by surveillance devices, it is possible to detect even devices that are blended or almost completely hidden within the environment. Luminosity of the ambient environment, distance from the surveillance device, partial or full occlusion by another object, and proximity to another heat source all affect the intensity of thermal signatures, but devices can be discovered in all experimental conditions except when they are directly behind a glass. Our work offers a new method for detecting covert surveillance devices, and we demonstrated that it works robustly in a wide range of scenarios and against common countermeasures. We also derived insights into the use of thermal cameras to support the detection of covert surveillance devices, paving way to improving user privacy and reducing threats of unwarranted surveillance.

ACKNOWLEDGMENT

This research is supported by the Academy of Finland project 339614, the European Social Fund via the IT Academy Programme and the Nokia Foundation grant 20220138. The publication only reflects the views of the authors.

REFERENCES

[1] S. Meza, "Airbnb hosts are recording their guests with hidden cameras," http://www.newsweek.com/airbnb-hidden-cameras-recordingguests, 2017, accessed: 2022-06-20.

[2] B. D. Teshome, "Spy camera epidemic in Korea: A situational analysis," *Asian Journal of Sociological Research*, pp. 1–13, 2019. [Online]. Available: https://globalpresshub.com/index.php/AJSR/article/view/782

[3] A. Oulasvirta, A. Pihlajamaa, J. Perkiö, D. Ray, T. Vähäkangas, T. Hasu, N. Vainio, and P. Myllymäki, "Long-term effects of ubiquitous surveillance in the home," in *Proceedings of ACM UbiComp*, 2012, pp. 41–50. [Online]. Available: https://doi.org/10.1145/2370216.2370224

[4] Y. Song, Y. Huang, Z. Cai, and J. I. Hong, "I'm all eyes and ears: Exploring effective locators for privacy awareness in IoT scenarios," in *Proceedings of ACM CHI*, 2020, pp. 1–13. [Online]. Available: https://doi.org/10.1145/3313831.3376585

[5] T. Liu, Z. Liu, J. Huang, R. Tan, and Z. Tan, "Detecting wireless spy cameras via stimulating and probing," in *Proceedings of ACM MobiSys*, 2018, pp. 243–255. [Online]. Available: https://doi.org/10.1145/3210240.3210332

[6] D. Ward, "Hidden camera detectors tested," https://ipvm.com/reports/hidden-cameras-finder, 2019, accessed: 2022-06-20.

[7] M. Roessler, "How to find hidden cameras," www.thinklikeacop.org/Military%20Manuals/%28ebook%20-%20survival%29%20-%20How%20To%20Find%20Hidden%20Cameras.pdf, 2002, accessed: 2022-05-16.

[8] B. Lagesse, K. Wu, J. Shorb, and Z. Zhu, "Detecting spies in IoT systems using cyber-physical correlation," in *IEEE @PerCom Workshops*, 2018, pp. 185–190. [Online]. Available: https://doi.org/10.1109/PERCOMW.2018.8480257

[9] Y. Cheng, X. Ji, T. Lu, and W. Xu, "On detecting hidden wireless cameras: A traffic pattern-based approach," *IEEE Transactions on Mobile Computing*, vol. 19, no. 4, pp. 907–921, 2019. [Online]. Available: https://doi.org/10.1109/TMC.2019.2900919

[10] A. D. Singh, L. Garcia, J. Noor, and M. Srivastava, "I always feel like somebody's sensing me! A framework to detect, identify, and localize clandestine wireless sensors," in *Proceedings of USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 2021, pp. 1829–1846. [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/singh

[11] L. Yu, B. Luo, J. Ma, Z. Zhou, and Q. Liu, "You are what you broadcast: Identification of mobile and IoT devices from (public) WiFi," in *Proceedings of USENIX Security Symposium (USENIX Security 20)*. USENIX Association, 2020, pp. 55–72. [Online]. Available: https://www.usenix.org/conference/usenixsecurity20/presentation/yu

[12] M. Tung, "How to find hidden cameras," https://www.securitybees.com/blogs/home/48443077-how-to-find-hidden-cameras, 2015, accessed: 2022-06-20.

[13] Murray Associates, "Thermal emissions spectrum analysis," https://counterespionage.com/tscm-technology/thermal-emissions-spectrum-analysis, accessed: 2022-05-16.

[14] H. Flores, J. Hamberg, X. Li, T. Malmivirta, A. Zuniga, E. Lagerspetz, and P. Nurmi, "Evaluating energy-efficiency using thermal imaging," in *Proceedings of ACM HotMobile*, 2019, pp. 147–152. [Online]. Available: https://doi.org/10.1145/3301293.3302364

[15] H. Flores, J. Hamberg, X. Li, T. Malmivirta, A. Zuniga, E. Lagerspetz, and P. Nurmi, "Estimating energy footprint using thermal imaging," *ACM GetMobile*, vol. 23, no. 3, pp. 5–8, 2020. [Online]. Available: https://doi.org/10.1145/3379092.3379094

[16] H. Emenike, F. Dar, M. Liyanage, R. Sharma, A. Zuniga, M. A. Hoque, M. Radeta, P. Nurmi, and H. Flores, "Characterizing everyday objects using human touch: Thermal dissipation as a sensing modality," in *Proceedings of IEEE PerCom*, 2021, pp. 1–8. [Online]. Available: https://doi.org/10.1109/PERCOM50583.2021.9439120

[17] T. Malmivirta, J. Hamberg, E. Lagerspetz, X. Li, E. Peltonen, H. Flores, and P. Nurmi, "Hot or not? Robust and accurate continuous thermal imaging on FLIR cameras," in *Proceedings of IEEE PerCom*, 2019, pp. 1–9. [Online]. Available: https://doi.org/10.1109/PERCOM.2019.8767423

[18] C. Bermejo Fernandez, P. Nurmi, and P. Hui, "Seeing is believing? Effects of visualization on smart device privacy perceptions," in *Proceedings of ACM Multimedia*, 2021, pp. 4183–4192. [Online]. Available: https://doi.org/10.1145/3474085.3475552

[19] Y. Abdelrahman, A. Sahami Shirazi, N. Henze, and A. Schmidt, "Investigation of material properties for thermal imaging-based interaction," in *Proceedings of ACM CHI*, 2015, pp. 15–18. [Online]. Available: https://doi.org/10.1145/2702123.2702290

[20] K. Mowery, S. Meiklejohn, and S. Savage, "Heat of the moment: Characterizing the efficacy of thermal camera-based attacks," in *Proceedings of WOOT@USENIX*, 2011, pp. 6–6. [Online]. Available: https://dl.acm.org/doi/abs/10.5555/2028052.2028058

Agustin Zuniga is a Doctoral Researcher at the Department of Computer Science, University of Helsinki, Finland. His current research focuses on machine learning, internet of things, pervasive computing and data science. He completed his MSc. in Computer Science at the University of Helsinki, Finland in 2018. Contact him at agustin.zuniga@helsinki.fi.

Naser Hossein Motlagh is a Postdoctoral Researcher at the Department of Computer Science, University of Helsinki, Finland. His research interests include IoT, WSN, UAVs and AUVs. He completed his D.Sc. in Networking Technology at Aalto University, Finland in 2018. Contact him at naser.motlagh@helsinki.fi.

Mohammad A. Hoque is a Postdoctoral Researcher at the Department of Computer Science, University of Helsinki, Finland. His research interests include energy efficient mobile computing, data analysis and resource-aware scheduling. He completed his PhD at Aalto University, Finland in 2013. Contact him at mohammad.a.hoque@helsinki.fi.

Sasu Tarkoma is a Full Professor at the Department of Computer Science, University of Helsinki, Finland. His research interests include mobile computing, Internet technologies, and AI. He completed his PhD in Computer Science at the University of Helsinki in 2006. Contact him at sasu.tarkoma@helsinki.fi.

Huber Flores is an Associate Professor at the University of Tartu, Estonia. His research interests include distributed, mobile and pervasive computing systems. He completed his PhD in Computer Science at the University of Tartu, Estonia in 2015. Contact him at huber.flores@ut.ee.

Petteri Nurmi is an Associate Professor at the Department of Computer Science, University of Helsinki, Finland. His research interests include distributed systems, pervasive data science, and sensing systems. He completed his PhD in Computer Science at the University of Helsinki, Finland in 2009. Contact him at petteri.nurmi@helsinki.fi.