CamRadar: Hidden Camera Detection Leveraging Amplitude-modulated Sensor Images Embedded in Electromagnetic Emanations

ZIWEI LIU, Zhejiang University, ZJU-Hangzhou Global Scientific and Tech Innovation Center, China
FENG LIN*, Zhejiang University, ZJU-Hangzhou Global Scientific and Tech Innovation Center, China
CHAO WANG, Zhejiang University, China
YIJIE SHEN, Zhejiang University, China
ZHONGJIE BA, Zhejiang University, China
LI LU, Zhejiang University, China
WENYAO XU, State University of New York at Buffalo, United States
KUI REN, Zhejiang University, China

Hidden cameras in sensitive locations have become an increasing threat to personal privacy all over the world. Because the camera is small and camouflaged, it is difficult to detect the presence of the camera with naked eyes. Existing works on this subject have either only covered using wireless transmission to detect cameras, or using other methods which are cumbersome in practical use. In this paper, we introduce a new direction that leverages the unintentional electromagnetic (EM) emanations of the camera to detect it. We first find that the digital output of the camera's image sensor will be amplitude-modulated to the EM emanations of the camera's clock. Thus, changes in the scope of the camera will directly cause changes in the camera's EM emanations, which constitutes a unique characteristic for a hidden camera. Based on this, we propose a novel camera detection system named CamRadar, which can filter out potential camera EM emanations from numerous EM signals quickly and achieve accurate hidden camera detection. Benefitting from the camera's EM emanations, CamRadar will not be limited by the camera transmission types or the detection angle. Our extensive real-world experiments using CamRadar and 19 hidden cameras show that CamRadar achieves a fast detection (in 16.75s) with a detection rate of 93.23% as well as a low false positive rate of 3.95%.

CCS Concepts: • **Security and privacy** → *Privacy protections.*

Additional Key Words and Phrases: Hidden Camera Detection, Electromagnetic Emanation, Electromagnetic Side-channels

ACM Reference Format:
Ziwei Liu, Feng Lin, Chao Wang, Yijie Shen, Zhongjie Ba, Li Lu, Wenyao Xu, and Kui Ren. 2022. CamRadar: Hidden Camera Detection Leveraging Amplitude-modulated Sensor Images Embedded in Electromagnetic Emanations. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 6, 4, Article 173 (December 2022), 25 pages. https://doi.org/10.1145/3569505

*Feng Lin is the corresponding author.

Authors' addresses: Ziwei Liu, Zhejiang University, ZJU-Hangzhou Global Scientific and Tech Innovation Center, Hangzhou, China, zivliu@zju.edu.cn; Feng Lin, Zhejiang University, ZJU-Hangzhou Global Scientific and Tech Innovation Center, Hangzhou, China, flin@zju.edu.cn; Chao Wang, Zhejiang University, Hangzhou, China; Yijie Shen, Zhejiang University, Hangzhou, China; Zhongjie Ba, Zhejiang University, Hangzhou, China; Li Lu, Zhejiang University, Hangzhou, China; Wenyao Xu, State University of New York at Buffalo, Buffalo, United States; Kui Ren, Zhejiang University, Hangzhou, China.

2474-9567/2022/12-ART173 $15.00
https://doi.org/10.1145/3569505

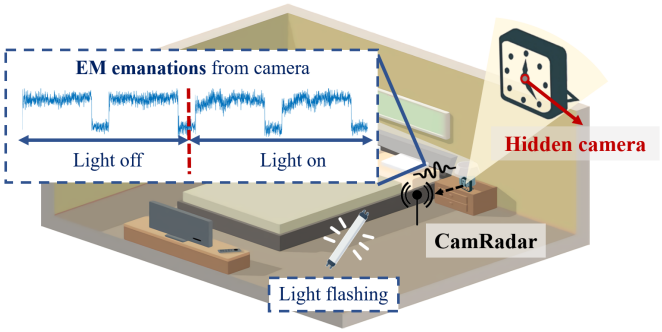


Fig. 1. When the camera's capturing scene changes, CamRadar can detect the hidden camera leveraging the camera's EM emanations.

1 INTRODUCTION

Hidden cameras in sensitive locations have become a growing threat to individual privacy all over the world. There have been reports of hidden cameras in motels [43], bathrooms [46], and offices [8]. Criminals have been found to use hidden cameras to record victims in varying state of undress [34], to capture personal activities [57], and to steal the victim's PIN on debit cards [31]. In South Korea alone, more than 30,000 cases of illegal hidden cameras use were reported to the police between 2013 and 2018 [7]. The threat posed by hidden cameras has attracted great attention from individuals and the government. For example, Chinese authorities have refreshed its crackdown on spy cameras in 2021 [5]. The great threat of hidden cameras has caused a great desire for camera detection approaches. However, due to the small size and the camouflaging capabilities of hidden cameras, which can be disguised as smoke detectors, clocks, or even notebooks [54], even if people think some objects or areas are suspicious, it is difficult to find cameras with naked eyes.

To deal with the threat of hidden cameras, various academic works have been proposed. Most of them detect cameras by analyzing the WiFi traffic of the camera [12, 26, 35, 41, 53, 64]. However, these techniques are limited to WiFi cameras that are streaming videos wirelessly. In practice, a hidden camera can store videos locally into a secure digital (SD) card or use wired connections. These cameras are common and can be easily purchased online [3]. Another category of work has conducted in-depth research on lens reflection [28, 36, 37]. These reflection-based methods typically use high-precision laser arrays to recognize the unique reflection pattern of the camera lens. However, those methods require expensive laboratory equipment which is unavailable to the general public. A state-of-the-art work [48] utilizes a commodity smartphone's time-of-flight sensor to detect the reflection. However, it is still constrained by the detection angle with a cumbersome use process and a high false positive rate (16.7%).

In this paper, we introduce a new direction to address the problem of hidden camera detection. Specifically, we leverage the unintentional electromagnetic (EM) emanations of the camera to detect it and propose a novel camera detection system named CamRadar (shown in Fig. 1). EM emanations have been found to carry information about the device activities. Typical devices that contain well-analyzed EM emanations include displays, keyboards, and computer memories. Plenty of work uses these devices' EM emanations to restore display images, to infer keystrokes, or to detect malwares [29, 30, 33]. Following this line of thought, for the first time, we explore the EM emanations of the hidden cameras. *Our key insight is that the digital output of a camera image sensor will be amplitude-modulated (AM-modulated) to the EM emanations of the camera's clock.* As the image sensor's output directly shows what the camera has captured, the camera's EM emanation will also contain information about the scene the camera is facing. Therefore, based on the insight, we could determine if a hidden camera

exists by checking if there are EM emanations that meet the camera leakage characteristics. As the camera EM emanations have nothing to do with how the camera transmits videos, CamRadar could detect cameras regardless of their transmission types. Thus, cameras that store video locally are also detectable. Besides, CamRadar has few limitations on the detection angle, its detection pipeline is automatic and has well-designed algorithms that ensure fast detection. Thus, the user could put CamRadar near suspicious locations and easily check if a hidden camera exists. All of these make CamRadar a practical solution to hidden camera detection.

Identifying hidden cameras via camera EM emanation characteristics is promising yet challenging as we are targeting an unknown camera, whose EM emanations may come up anywhere in the EM spectrum. Overall, CamRadar mainly tackles three specific challenges: (1) In the actual scene without EM shielding, the EM spectrum will be very noisy as various wireless communication signals exist. Therefore, it is critical for CamRadar to first identify the possible EM emanations from the electronic devices and eliminate other noises. (2) An EM leakage source (e.g., clock) will typically produce multiple harmonics. Besides, an electronic device may have multiple EM leakage sources, let alone there may exist multiple electronic devices in the environment. This means that CamRadar will have to filter out a significant amount of EM emanations from other electronic devices and detect the malicious camera's EM emanations. Therefore, CamRadar requires a fast screening mechanism to eliminate most of the non-camera EM emanations. (3) There could be some electronic devices (e.g., display) that have quite similar EM emanations as the camera. How to quickly and accurately distinguish the screened EM emanations of cameras from other similar devices is also a big challenge.

To overcome the challenges, CamRadar takes advantage of the characteristics of camera leakage. It first uses the frequency domain characteristics to eliminate noises from environmental wireless transmissions and identify EM emanations from electronic devices. Then CamRadar employs a fast adaptive spectrum analysis to identify the best camera-like AM-modulated frequency spikes. Finally, CamRadar leverages a scheme that uses light to stimulate the camera while analyzing the changes in the camera leakage signal to accurately determine whether there is a camera. We implement the prototype of CamRadar with a USRP B210 [42] and conduct extensive experiments to evaluate it. CamRadar can complete the detection of a suspicious object in 16.75s and achieves an overall detection rate of 93.23%, 87.21%, 78.95%, and 70.68% at the distance of 10cm, 20cm, 30cm, and 40cm respectively. Furthermore, CamRadar achieves a low false positive rate of 3.95% on average across all distances in extreme test conditions. Our contributions can be summarized as below:

- We discover that the digital output of the camera's image sensor will be AM-modulated to the camera's clock leakages. The characteristics of this EM emanation can be used to detect hidden cameras.
- We propose a novel system (CamRadar) that could screen potential EM emanations from the camera's clock and accurately examine whether a hidden camera exists.
- We implement the prototype of CamRadar using a portable software-defined radio device and conduct extensive real-world experiments on 19 commercial small cameras.

2 BACKGROUND

2.1 EM Emanations

As derived from Maxwell's equations, EM waves can be created by varying electric currents over time. Based on the principle, modern wireless communication systems use oscillating currents to generate well-designed EM waves over the air for communication. Meanwhile, it is a well-documented fact that electronic devices generate EM radiation on unintended frequencies as a side effect of their internal operations [49]. The unintentionally generated EM emanations may theoretically be anywhere in the EM spectrum. Because of the high integration and complexity of the circuitry, the sources of EM emanations are hard to find. Nevertheless, a few of them are typical and well-known due to their periodic activities like clocking, DRAM refreshing, and display refreshing.

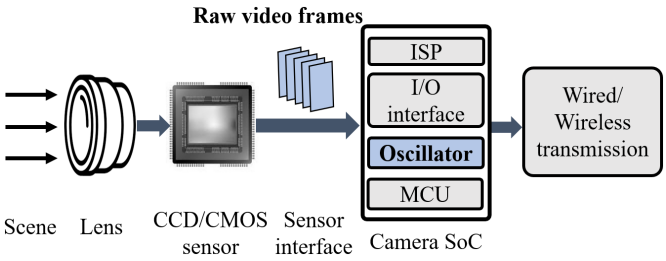


Fig. 2. Typical layout of a camera.

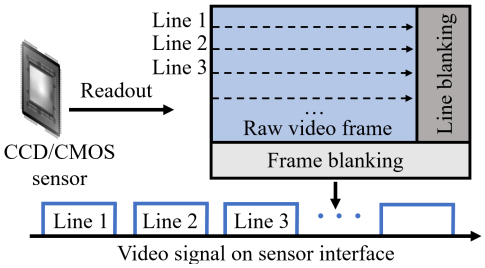


Fig. 3. Progressive scanning of generating a raw video frame and the corresponding video signal.

Interestingly, it has been found that unintentional EM emanations could carry information about the device's activities. The EM emanations may be AM-modulated or frequency-modulated by the activities [44], which could provide insights for attackers to obtain valuable information. Typical research targets of existing work include leaks of displays, memory, USB, wireless modules, etc. For example, the AM-modulated signals from displays have been used to recover the screen pictures [33, 38]. In this work, we target cameras and study the information carried on their EM emanations.

2.2 Camera Basics

Hidden cameras. There are increasing reports about hidden cameras [8, 43, 46] in recent years. The inconspicuous tiny cameras hidden in hotels, rental houses, and other public spaces have raised people's concern about security and privacy. Hidden cameras are typically quite small. They can capture scenes through a pinhole and can be disguised as common items in daily life like a smoke detector, a clock, a power socket, and a notebook [54]. These disguises make it hard to find hidden cameras with naked eyes. Even if one suspects there may be hidden cameras in some items, it is hard to check as the items typically look normal from the outside, and taking them apart for inspection could be laborious and even inappropriate in most cases, especially in public rooms. A hidden camera can be wired or wireless, depending on how it transmits the images. A wired camera may be connected by a cable to a monitor or a recording device like an SD card. Whereas a wireless camera can transmit real-time scenes remotely with the aid of wireless communication (e.g., WiFi and 4G/5G).

Working pipeline of cameras. Fig. 2 shows the typical hardware components inside a camera. The CCD/CMOS image sensor receives light that is focused through a lens or other optics and performs the function of converting light to digital signals. Depending on the type of the image sensor, the photons are first converted to electrons, then to a voltage (CCD sensor) or a digital value (CMOS sensor) with the help of the analog to digital converter (ADC). CCD sensor's output voltage will also be immediately converted to a digital signal through an ADC. The generated digital values after the image sensor constitute raw video frames. The raw video frames are transmitted through the sensor interface to a camera system on chip (SoC). The SoC typically has an MCU, an oscillator that provides clock signals, and an image signal processor (ISP) that performs necessary steps like demosaicing and denoising to get clear images. Finally, the raw video frames after processing become the images we usually see and are transmitted through the I/O interface. The user may store the images into an SD card or watch online streaming via wireless transmission.

Raw video frames. As mentioned before, the camera image sensor will produce a raw video frame. The frame is generated by scanning each pixel of the image sensor. As shown in Fig. 3, current digital cameras typically use progressive scanning to generate pictures. In the progressive scanning mode, each line is scanned in a linear manner, i.e., line 1, then line 2, line 3, and so forth. As is typical in video applications, blanking or synchronization

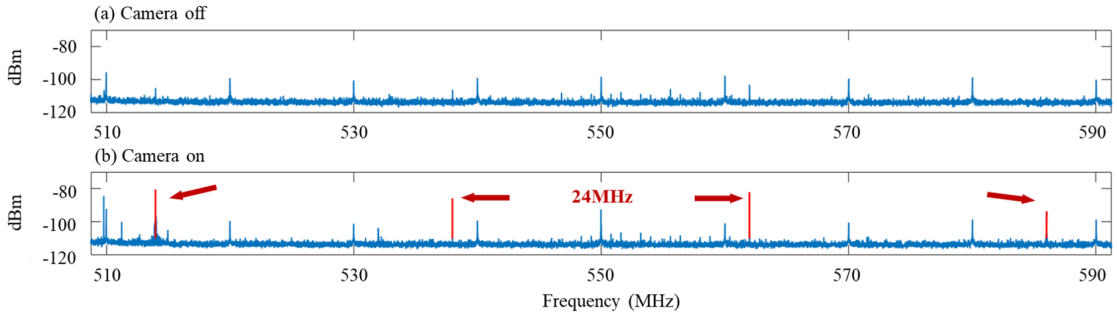


Fig. 4. The power spectra before and after a camera is turned on.

intervals are inserted between successive lines and frames during the readout process [15, 39]. The intervals are line blanking period and frame blanking period in Fig. 3. Thus, when each raw video frame is transmitted via the camera sensor interface, blanking intervals could be seen between the line signals and frame signals.

3 THREAT MODEL

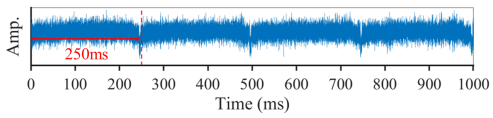
We consider a scenario where an adversary has already put a small hidden camera inside a room. The camera could record the victim's activities secretly, which is a complete violation of privacy. To keep secret and avoid being found, the hidden camera is placed somewhere that the victim usually is hard to notice. For example, the camera may be hidden in a power socket or a smoke detector [54]. What is worse, even if the victim is aware of some suspicious objects that may hide cameras, it is hard for he/she to make sure if there truly is a hidden camera because the hidden camera typically has a small lens that is hard to detect with untrained eyes.

Different from those wireless camera detection works [26, 53], we do not make any restriction on how the hidden camera transmits the recorded video to the adversary. The hidden camera can transmit the video wirelessly or store the video locally (e.g., use an SD card) and the adversary may manually take the video away after the victim leaves. One assumption made in this research is that the camera will continuously record and cannot be turned off intentionally to avoid being detected. The assumption is based on the fact that for wired cameras, the adversary cannot control wired cameras wirelessly, and for wireless cameras, it is unlikely that the adversary will always maintain real-time surveillance of the victim.

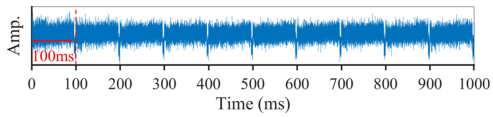
4 CHARACTERIZING CAMERA'S EM EMANATIONS

To detect hidden cameras regardless of their transmission types, we consider the issue from a new perspective, i.e., the camera's EM emanations. Our insight is that the output of the image sensors will be leaked with the aid of the camera's EM emanations. Specifically, the generated raw video frames from the sensor will be AM-modulated on the EM emanations of the camera's clock. Therefore, we can detect the camera leveraging the AM-modulated emanations from the camera. We conduct a series of preliminary experiments to verify our insight into the camera's EM emanations.

Setup. We use three commercial small cameras and a FLIR USB camera (Grasshopper3 GS3-U3-41S4C) as the testing targets. These commercial small cameras are capable of transmitting recorded videos via WiFi and storing them into the local SD cards. In addition, a USRP connected to an amplifier and an antenna is used to collect EM emanations for analysis.

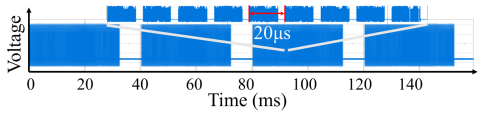


(a) 4fps

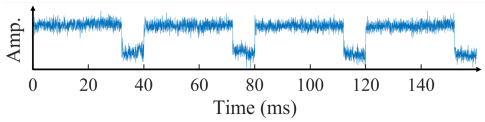


(b) 10fps

Fig. 5. AM-demodulated signal when the FLIR camera's frame rate is set to 4fps and 10fps.



(a) Voltage on the camera's sensor interface



(b) AM-demodulated EM signal of a camera

Fig. 6. Comparison between the voltage and EM emanation of a camera.

4.1 Spectrum Pattern

We first inspect the frequency domain to explore the EM emanations from the working cameras. We turn those cameras on and off with the antenna 15cm from them and inspect the EM spectrum manually. As a result, some new frequency spikes will show up when the camera is turned on, which are the harmonics of the camera's clock frequency. The variation of the power spectrum after a camera starts working is shown in Fig. 4 as an example. We can see there are some new frequency spikes when the camera is turned on (marked with red lines), these frequency spikes are distributed at an equal distance (about 24MHz) over the spectrum, which are the harmonics of the clock frequency.

However, the mere discovery of these EM emanations from a camera's clock is insufficient for determining the existence of a camera. In fact, clocks are typical sources of EM emanations and have been well studied in various works [24, 51]. Plenty of electronic devices could have similar EM emanations. Thus, we will conduct further analysis from the time domain in the next section.

4.2 AM Modulation of Sensor Images

We conduct a series of experiments on the time domain to explore the relevance between the camera sensor images and the EM emanation and to verify that the images are AM-modulated to the EM emanations of the clock. We use the USRP to collect data at one frequency spike of the EM emanation (e.g., the red frequency spikes shown in Fig. 4) with a sampling rate of 500KHz and analyze the amplitude of the signal, i.e., we AM-demodulate the signal so that we can see what information has been carried on the camera's EM emanation. A typical time-domain signal of the EM emanation can be found in Fig. 5, which has a rectangular wave envelope. In fact, all of the tested cameras have similar signals with varying degrees of amplitude, duty cycle, and frequency. We explore the characteristics of the demodulated signal step-by-step from three aspects: the relevance to the camera frame rate, the relevance to the voltage on the camera sensor interface, and the relevance to the capturing scenes. To eliminate the impact of the camera's transmission type and create a baseline, we neither put an SD card into the camera slot nor connect to the camera wirelessly.

Relevance to the camera frame rate. We first test those four cameras and observe that the frequencies of their AM-demodulated EM emanations range from 10 to 25 and are close to their frame rates. *Then we test the FLIR camera in depth as it is capable of adjusting fine parameters, such as the frame rate.* We adjust the camera's frame rate and inspect the variation of the camera's time-domain signal (Fig. 5). We can see the frequency of the time-domain signal's envelope always varies accordingly to the camera's frame rate. Therefore, it is quite probable that the demodulated signal is relevant to the camera sensor image.

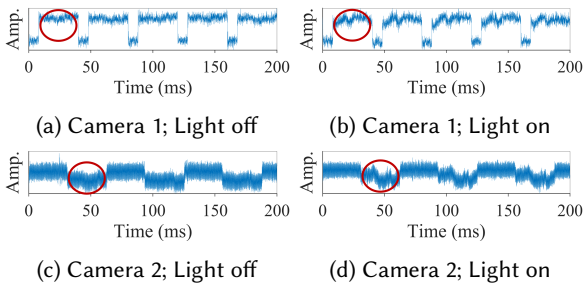


Fig. 7. EM emanation variations to the light.

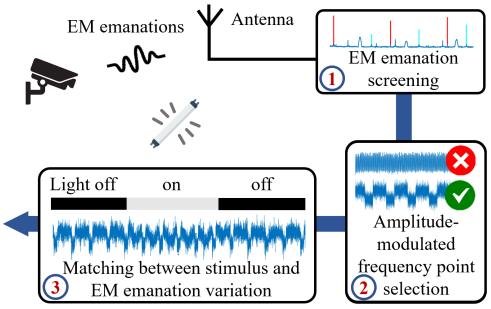


Fig. 8. Workflow of CamRadar.

As the FLIR camera is a USB camera, and USB has been found to have EM emanations [23], one may argue that the measured EM signals here could come from the USB transmission. To disprove this claim, we collect EM signals close to the USB transmission line and far away from the camera. We find the quality of the neat rectangular wave shape time-domain signal drops quickly. Furthermore, the frequencies of the carrier signals are related to the camera's pixel clock frequency and are not the leaky frequencies of the USB transmission. Therefore, we can overturn the possibility of the USB EM emanations and conclude that the time-domain signals of the collected EM emanations have a strong correspondence with the sensor images.

Relevance to the voltage on the camera sensor interface. To further verify the relationship between the demodulated signal and the sensor image, we dive into the sensor interface circuits of the cameras. We use an oscilloscope to measure the voltage on the data line of the camera's sensor interface. The measurement result of a camera is shown in Fig. 6a as an example. We can see the camera sensor's outputs are grouped into frames and blanking intervals are inserted between frames. If we zoom in on the time axis, we could also see each line of a frame (less than $20\mu s$) and the line blanking intervals. More importantly, comparing the demodulated signal of the EM emanation (Fig. 6b) with the measured voltage, we can see they show great similarity: they have the same period and even similar duty cycles. However, the blanking intervals between each line of a frame cannot be resolved in EM leakage as our sampling rate is not enough. Combining this phenomenon with regards to the camera frame rate, we can conclude that demodulated time-domain signals of the EM emanation come from the transmitted raw video frames, and the transmission of those frames is AM-modulated to the emanations from the camera's clock.

Relevance to the capturing scenes. Considering that the demodulated time-domain signals of the camera's EM emanation come from the image sensor output, if the camera is able to capture different scenes, we should get different time-domain signals. To prove this, the camera is placed facing different scenes and the time domain signal is observed. As the EM emanations of the camera will vary if we move the camera or the antenna, we have to keep both the antenna and camera static. Furthermore, if we put an object or make movements close to the camera, the EM field of the leakage will directly be impacted, which will hinder us from studying the relation of the capturing scenes and EM emanations. Therefore, we first choose to face the camera and make movements (e.g., walk, wave arms.) several meters away. However, we find the variations of the camera EM emanations are weak and hard to tell for some cameras. This is because the scene we have changed only occupies a small part of the whole scene the camera can capture. Therefore, we use light to add in illumination difference instead, which should show a greater impact on the camera's image. Fig. 7 shows the variation of the corresponding time-domain signals of two cameras. We can see the signal in each cycle when the light is on has a different waveform from the signal when the light is off. This happens because the light dramatically changes the scene the camera captures, i.e., the output of the camera sensor changes a lot. All four cameras' signals show variations

when the light changes state, except that the variations of different cameras are not the same. This further proves that the image sensor's output has been AM-modulated to the clock's emanation.

5 SYSTEM OVERVIEW

CamRadar is designed to leverage a working camera's EM leakage characteristics to detect the camera. Fig. 8 shows the workflow of CamRadar, which consists of three key phases: EM emanation screening, AM-modulated frequency point selection, and matching between stimulus and EM emanation variation. CamRadar uses these three phases to gradually screen the possible leak frequency points, and determine whether there is a camera leakage finally.

EM emanation screening. EM emanations could come up at any frequency theoretically. Therefore, CamRadar will first scan across a wide spectrum to grasp a whole view of the frequency distribution of surrounding EM signals. Given that there are multiple noises in the environment, CamRadar first picks out signals with an extremely narrow spectrum and eliminates others as the EM emanations from the clock are typically narrowband. Then CamRadar will further filter and group the selected frequency spikes according to their harmonics because the clock leakage typically has multiple harmonics and different clocks will produce different base frequencies. After this phase, we will have different groups of frequency spikes that come from different EM emanation sources.

AM-modulated frequency point selection. The number of frequency spikes in the different groups after screening is still very large, as an EM leakage source will produce multiple harmonics and there may be many leakage sources around. Furthermore, not all of the camera's frequency points have a good signal quality, which is affected by the camera circuit and the spectrum noises. Therefore, the remaining leakage frequency points need to be further screened. To tackle these, CamRadar will further check if the found frequency spikes have AM modulation similar to a camera's EM emanations in this phase. To achieve rapid screening, CamRadar uses fast spectrum analysis with adaptive resolution and can measure the quality of leaky frequency points with a short sampling time.

Matching between stimulus and EM emanation variation. Finally, the remaining frequency points could still come from some other electronic devices that have similar AM-modulated EM emanations as a camera's. Directly analyzing the signal is difficult to distinguish between a camera and other devices. CamRadar tackles this by exploiting the unique property of the camera's EM emanations, i.e., their relevance to the scenes being captured. Specifically, CamRadar uses a well-designed light stimulation scheme and determines if there exists a camera by checking the synchronization of EM signal variations and light flashes.

6 SYSTEM DESIGN

6.1 EM Emanation Screening

As CamRadar knows nothing about the potential camera's EM leakage frequency, we need to first search across a wide spectrum. Previous work typically uses a long-time window and averages multiple FFTs to obtain an accurate spectrum [25, 50, 69]. However, they either leverage an expensive signal analyzer, or the target frequency has already been known in advance, which is impractical in real life. We target using a portable software-defined radio (SDR) that can facilitate the actual detection. We select a bandwidth of 10MHz, which can be easily supported by popular SDRs like USRP, LimeSDR [40], and HackRF [45]. It is also possible to further decrease the bandwidth, with a sacrifice of longer scanning time or lower FFT resolution, so that a super cheap SDR (RTL-SDR [55]) can also deploy CamRadar. Given such a low bandwidth, we have to make trade-offs between the scanning time and FFT resolution. Specifically, we perform each FFT with 262144 samples, which requires a sampling time of roughly 0.027s. If we perform frequency sweeping from 200MHz to 800MHz, the sampling time would theoretically require a total of 60 * 0.027 = 1.62s. In practice, the time for frequency switching and processing

Algorithm 1: Group peaks according to their sources

Data: All the sharp peaks $P = p_1, p_2, ..., p_n$
Result: Groups of peaks $G = g_1, g_2, ..., g_m$

```
1  G ← ∅;
2  for p_i, p_j ∈ P and p_j − p_i >= 10MHz do
3      g ← p_i ∪ p_j;
4      for p ∈ P and p ≠ p_i, p_j do
5          if p − p_i = k(p_j − p_i) and k ∈ ℤ then
6              g ← g ∪ p;
7          end
8      end
9      if |g| > 5 then
10         G ← G ∪ {g};
11     end
12 end
13 G ← Merge(G);
```

should be considered and we find that scanning with subsequent processing can be accomplished in 5s, which is a tolerable duration. A detailed analysis of these frequency sweeping settings could be found in Section 7.1.

To pick out EM emanations, CamRadar leverages two main insights: (1) the camera's clock will typically produce a sharp signal that serves as the carrier (shown in section 4.1), while wireless communication signals have a wider band; (2) the carrier signal generated by a digital circuit always comes up with multiple harmonics [9]. Thus, CamRadar will find all the sharp spikes and regard the spikes that conform to the harmonic distribution as the emanations from electronic devices. Specifically, CamRadar first calculates the peak envelope of the FFT results obtained before. Therefore, signals with a wide bandwidth will constitute a wide peak in the spectrum and EM emanations will remain a sharp peak. Then CamRadar finds peaks with constraints for the width and height. We use a window of 128 points to calculate the envelope and discard peaks whose width exceeds 512 points and the peaks with a height lower than 5dB.

Next, CamRadar tries to find all the peaks that could constitute harmonics. However, the basic frequency of the carrier is unknown, and not all the harmonics could show up due to the circuit's frequency response and environmental interferences. We devise an algorithm to tackle this and group the peaks according to their leakage sources (shown in Algorithm 1). The algorithm will first take one pair of peaks from all the peaks (p_i and p_j) and temporarily assume the basic frequency as their difference. As the clock used in the camera is typically above 10MHz [62], the algorithm will ignore the pair if the difference is below 10MHz (line 2). Then, the algorithm will check all the peaks again and identify if any peak (p) could be one of the harmonics (lines 3-5). If so, the new peak will be added to the group of p_i and p_j (line 6). After that, if the group is large enough (e.g., have more than 5 members), peaks in the group will be preliminarily determined to be from the same source and the group will be saved (lines 9-10). Finally, the algorithm will conduct a merge among groups considering two situations: one is to merge groups whose basic frequency differences are multiples of another (line 13). This could happen like one group has a minimum difference of $6f$, where f is the true basic frequency. But another group has a minimum difference of $2f$. The other one targets groups that have multiple intersections. For example, group one contains $\{5f, 10f, 20f, 40f, 60f, ...\}$ with a minimum difference of $5f$, group two contains $\{20f, 28f, 32f, 40f, 60f, ...\}$ with a minimum difference of $4f$ and these two groups will be merged up. These merges could compensate for our uncertainty of the true carrier frequency, remove redundant groups and save time for the next phases. Note that

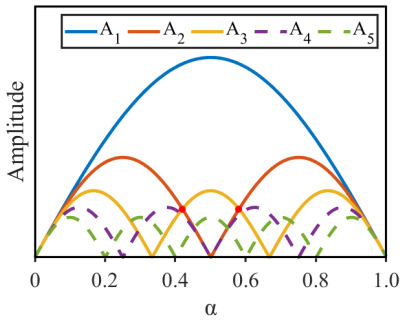
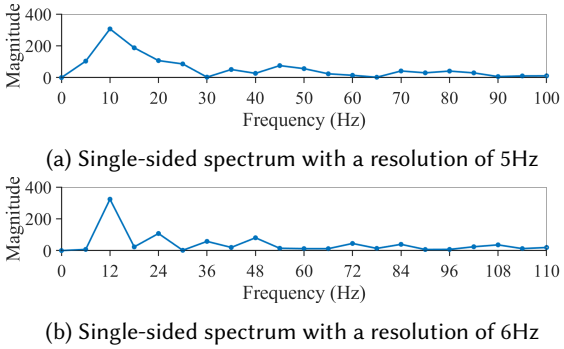


Fig. 9. The amplitude of each sinusoid corresponding to different duty cycle α.



(a) Single-sided spectrum with a resolution of 5Hz

(b) Single-sided spectrum with a resolution of 6Hz

Fig. 10. Single-sided spectrum comparison between the resolution of 5Hz and 6Hz for a camera's signal with a period of 12Hz.

we may not be able to find the true carrier frequency in this phase, but we could still group most of the peaks coming from one leakage source as their frequency differences are accurate multiples.

6.2 AM-modulated Frequency Point Selection

Although we have found EM emanations from potential cameras through the last phase, we still have to narrow down the optional frequencies as there still exist too many peaks. Checking them one by one is time-consuming for practical use. This phase leverages our insight that the camera's EM emanation can be AM-modulated by its sensor images to select the most probable frequency of a camera. Specifically, the amplitude of a camera's AM-modulated signals can be best approximated by rectangular pulses as the data transmission has sharp transitions. Therefore, we can sample at these optional frequencies and if we find a signal whose amplitude envelope looks like a periodic rectangular, this signal has a high possibility to come from a camera. To save time, we do not need to AM-demodulate all the frequencies. Instead, we select 5 frequencies from each group and sample at each frequency for only 0.2s. Then, we AM-demodulate the signals and analyze their amplitudes.

Checking the period of a signal has many methods like calculating its autocorrelation, but we also need to check if the signal is a rectangular wave at the same time. Thus, we select to analyze the spectrum of the demodulated signal. According to Fourier analysis, the spectrum of a rectangular wave is equivalent to a set of sinusoids with various amplitudes at its base frequency and multiples (harmonics). Specifically, the Fourier series expansion for a rectangular wave with a duty cycle of α is:

$$f(t) = \alpha A + \frac{2A}{\pi} \sum_{n=1}^{\infty} \frac{\sin(\alpha n \pi)}{n} \cos(n\omega t) \tag{1}$$

The amplitude of each sinusoid (A_n), which is $\frac{2A}{\pi} \cdot |\frac{\sin(\alpha n \pi)}{n}|$, can be plotted as a function of α (shown in Fig. 9). We only plot up to the 5th harmonic, because the amplitude of the harmonic greater than the 5th will never exceed the intersection of the 2nd harmonic and 3rd harmonics. We can see the greatest two amplitudes always come from the first three harmonics ($n = 1, 2, 3$). Thus, we use a loose judgment condition for a rectangular-shape AM-modulated signal that the highest two peaks of the demodulated signal's spectrum should have a relationship of 2 or 3 times.

In practice, the resolution of the demodulated signal's spectrum will constitute another great challenge. The FFT resolution of a sampled signal can be calculated as $\frac{f_s}{N}$, where f_s is the sampling rate and N is the number of FFT points. As each of our sampled signals has a length of 0.2s, the FFT resolution of their amplitudes' spectrum

can only reach 5Hz. However, the 1st harmonic of the AM-demodulated signal has a strong correspondence with the camera's frame rate, which typically ranges from 10fps to 30fps [58]. Therefore, an FFT resolution of only 5Hz is too low and our loose judgment condition may not hold. For example, Fig. 10a shows the single-sided FFT results using the resolution of 5Hz for a camera's AM-demodulated signal whose basic frequency is 12Hz. We can see the relationship among the highest FFT bins no longer holds when the resolution is 5Hz because 12Hz does not have an exactly corresponding FFT bin. This would make distinguishing a rectangular-shape AM-modulated signal and other signals quite difficult. Obtaining a higher resolution may solve this but will require a larger N and a longer sampling time. This is impractical as it takes too much time.

To tackle this, we observe that although we cannot use a higher resolution, we could use a more suitable resolution for each signal. Specifically, if the signal's frequency is exactly multiple of FFT resolution, the FFT results are still accurate for the signal. For example, Fig. 10b shows the FFT results with a resolution of 6Hz for the same 12Hz signal. We can see the amplitudes of the signal's harmonics can be well shown and our judgment condition will hold. Therefore, instead of using a fixed resolution of 5Hz, CamRadar will estimate the signal's frequency and adapt the FFT resolution accordingly. The estimation of frequency is implemented by performing autocorrelation and calculating the difference between the two highest peaks. For an estimated frequency f_{est}, CamRadar recalculates FFT resolution R as:

$$R = \frac{f_{est}}{\lfloor \frac{f_{est}}{5} \rfloor} \tag{2}$$

Thus, the new FFT resolution R remains no less than 5Hz and keeps as small as possible. Using the new FFT resolution, each AM-demodulated signal will be checked if our judgment condition is satisfied. Considering that there may exist multiple signals that come from the same source, only one of the five frequencies in each group will be left. Therefore, we need a screening mechanism to find the best frequency with the lowest noise and highest SNR. We use a metric similar to SNR. We sort the FFT bins, sum the amplitude of harmonics in the several highest bins up and calculate the ratio of this sum to the remaining bins. The frequency whose ratio is the highest will finally be left. The idea behind the metric is intuitive: if a signal has less noise and looks more like a rectangular wave, the largest FFT bins will be the harmonics of its basic sinusoid and we will get a high value. Moreover, an empirical threshold is also used to eliminate noisy signals.

We also find that sometimes the frequency of some cameras' leaks do not appear after the final screening in actual tests. This is mainly due to the jittering of frequency points' amplitudes. The AM-modulated frequency points in the spectrum will jitter with the variation of time-domain signals' amplitudes. Recall that in phase one we use a sampling time of only 0.027s for each FFT. Thus, if a camera's frame rate is 10fps, our sampling cannot even cover a complete frame, which will cause the height of the same leakage frequency spike in different trials to change drastically. This will make some frequency spikes with good quality that cannot rank at the top in phase two. A straightforward approach would be to increase the sampling time to obtain a more stable spectrum. However, the time it takes for scanning would be too high. Besides, the missing of high-quality frequency points is dependent on the cameras and we do not want to sacrifice time for all the cameras. Therefore, we use an incremental approach that the whole detection procedure (including phase 3) will be repeated if no camera is detected. The upper limit of trials is set to 3 times.

In total, this phase filters out most of the frequency points without significant AM modulation, reserving for each group one or zero frequency points that may come from the camera. The extremely limited number of frequency points provides the basis for a more refined judgment in the next phase.

6.3 Matching between Stimulus and EM Emanation Variation

In this phase, the final decision on whether the remaining frequency points come from hidden cameras will be made. Although these remaining frequency points are all AM-modulated, AM modulation on EM emanations

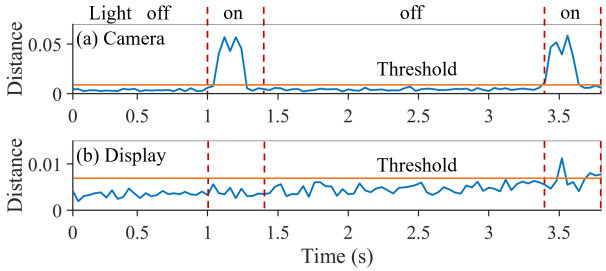


Fig. 11. 3-NN distances of a camera and a display.

with rectangular waveforms is not unique for cameras. Other electronic devices (e.g., display) may have a similar phenomenon. For example, we find the leakages from the display have similar waveforms to that from the camera (see section 7.4).

Therefore, a unique characteristic of the camera's leakage is leveraged in this phase. Specifically, as a camera's AM-modulated emanation contains information of sensor images, we use a light to glow intermittently. The sudden light could stimulate an obvious change to the camera sensor image and thus the camera's leakage signals will vary correspondingly. CamRadar will determine that there exists a camera if the AM-demodulated signal on one frequency point changes as the light starts blinking. Considering the greater impact on the camera when the light is within the camera's field of view, the user could put a light tube in a place where a hidden camera can obviously capture it, such as in the middle of the room. We also find that if we turn the light on for a long time (e.g., 5 seconds), the leakage of cameras will first change drastically and then turn stable. We attribute this phenomenon to some automatic parameter adjustment mechanisms of the camera like auto exposure. Thus, we will turn the light on for a short time instead of keeping it always on.

Nevertheless, determining whether the signal has changed due to lighting is still a challenging task because it is completely unknown how the AM-demodulated signal varies when the light blinks. The variation of signals from different cameras can be quite different, caused by the differences in the cameras' software, hardware, and leakages. What's worse, there could be unexpected noises from the camera circuit that make the AM-demodulated signal fluctuate.

To tackle these, for each suspicious frequency point, we carefully design a lighting scheme and leverage one-class KNN with correlation distance to determine if the signal varies due to lighting. *Our main insight is: although a non-camera signal may occasionally fluctuate just when we flash the light once, it is much less possible that a non-camera signal always varies exactly when we flash the light two or more times.* Specifically, we will first keep the light off for 1 second to get some samples. These samples will be the baseline data of one-class KNN and will also be used to calculate the period (i.e., frame rate). Then we will flash the light twice with a fixed interval, which means the total duration of sampling time is 3.8s (adding up the additional 1s). The collected data will be separated into two parts according to their sampling time: the data while the light is on and the data while the light is off. All the collected AM-demodulated signals including training data will be preprocessed with smoothing and downsampling so that some noises can be removed and the calculation cost can be reduced. Both the on and off parts will be tested in KNN to obtain the nearest distance to those baseline data. The distance is calculated with the length of a frame. Considering that the frame length may not be quite accurately calculated, we will cycle shift one frame and use the minimum correlation distance between two frames. Finally, we recognize the frequency point from the camera if the signals collected while the light is on have a larger distance than those collected while the light is off. This means the signal fluctuates twice exactly as the light flashes twice. Although it is possible to get the light to flash more times, we find that twice is enough for a low false positive rate. Fig. 11

(a) Prototype of CamRadar (b) Tested cameras

Fig. 12. Experimental setup.

Table 1. The list of cameras we test.

ID	Model	ID	Model	ID	Model
1	HDC-DVR camera	6	V380 pro	11	KingFisherPro
2	LaiCam X7	7	HomeEye	12	Botslab
3	LaiCam X9	8	Hopeway	13	HXY-001 usb camera
4	NewFocus X1	9	Netipc S95	14	USB-2MP-camera
5	HIDVCAM A15	10	CamHipro	15-19	RaspberryPi Camera v2

shows the distances to three nearest neighbors of a camera and a display. We can clearly see larger distances in the "on" sections of the camera, which greatly exceed the maximum distance in the "off" sections (threshold). The whole algorithm is fast, does not require training, and can adapt to various cameras as the threshold is adaptive.

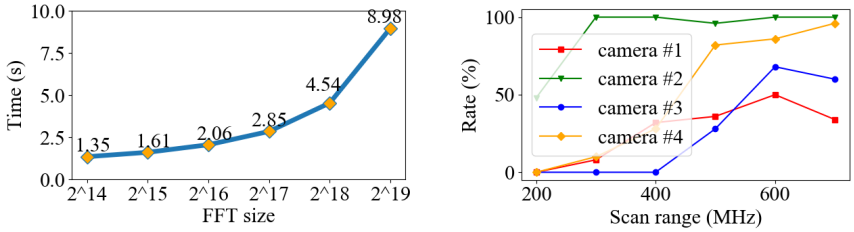
6.4 Camera Localization

Once CamRadar has detected that a hidden camera exists, the camera's location can be narrowed to close proximity (e.g., less than 1 meter) because the EM emanations decay fast in the air and cannot travel too far. Considering that the camera may be disguised so well that it is difficult for people to think of it as a camera, we also propose an approach to accurately pinpoint the camera. Specifically, as we already know the leaky frequency of the camera, the user can directly move the antenna of CamRadar and watch the power spectrum of the camera's leaky frequency. When the antenna is close to the camera, the spectrum will have high power. The localization method is simple and convenient, with high practicability. Besides, one can also use a directional antenna to accurately pinpoint the direction of the signal source. Nevertheless, a simple omnidirectional antenna is enough as the target camera is nearby and the possible positions are limited.

7 EVALUATION

7.1 Experimental Setup

Apparatus. We build the prototype of CamRadar based on a USRP B210, a Foresight low noise amplifier (FST-RFAMP01), and a 3dbi omnidirectional antenna. Note that the USRP can be replaced by other cheaper software-defined radios to reduce cost, as our used sampling rate is low (only 500KHz) except for the frequency sweeping process, which is also possible to use a lower sampling rate by sacrificing more time. To provide the controllable light, we use an infrared-controlled led light tube easily available online and use an Arduino board to control it. The light tube's power is 6W and has a maximum luminous flux of 400lm.



(a) Average time required for different FFT size

(b) Percentage of finding an AM-modulated frequency

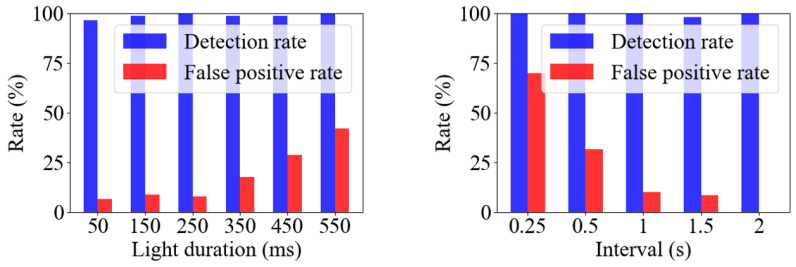
Fig. 13. Trials of setting with different frequency sweeping resolution and range.

We test 19 small cameras, including 14 popular hidden cameras that are available online [3, 56] and 5 Raspberry Pi cameras (v2) that are representative of homemade hidden cameras [27]. The prototype of CamRadar and all the tested cameras are shown in Fig. 12. These cameras' detailed models are shown in Table 1. Among these 14 commercial small cameras, 12 of them (*#1-#12*) are capable of storing videos locally to an SD card, 11 of them (*#1-#11*) can transmit videos wirelessly, and 2 of them (*#13-#14*) can transmit videos through a USB connection. In addition, those 5 Raspberry Pi cameras (*#15-#19*) are driven by two Raspberry Pi boards to ensure the universality of detection. The light tube is placed 50cm in front of the camera. All cameras are initially unplugged and use battery power, except for those without batteries (e.g., USB cameras and Raspberry Pi cameras). In addition, we configure all the cameras (if they can) not to store or transmit videos, so that we can eliminate the possible interference from data transmission.

Metrics. We use the following three metrics:

- Camera detection rate: A hidden camera detection occurs when we put a working camera around and CamRadar concludes there exists a camera. The detection rate is measured as the ratio of detectable cameras to all tested cameras.
- False positive rate: A false positive occurs when there is no camera around but CamRadar misjudges that there is. It is measured as $misjudges/tests\ without\ camera$. **As we find CamRadar hardly misreports when there is no electronic device around, we design an extremely challenging setup to test CamRadar's false positives.** Specifically, we use the EM emanations from cameras to simulate the EM emanations from non-camera devices, except that the non-camera devices will not be stimulated by the light. Therefore, when we test each camera, we will always collect two traces. In one of them, we will trigger the light normally to see if the camera can be detected by CamRadar and calculate the detection rate. In the other, we will use the camera to simulate as a non-camera device and will not trigger the light, which will be used to measure the false positive rate. Note that false positive rate is also important in hidden camera detection, as false alarms not only waste the user's effort, but also impact the credibility of the detection method (imagine a clean room always has some objects or facilities that make the detector alarm).
- Detection time: The detection time is measured as the time required for CamRadar to conduct a complete detection procedure regardless of whether there is a camera detected or not. As CamRadar has at most 3 trials to ensure the accuracy of the frequency point selection (see section 6.2), it may take CamRadar longer to conclude there is no working camera around.

Setup of frequency sweeping. CamRadar performs frequency sweeping to screen EM emanations as the first phase, the sweeping resolution and range are two key factors that could impact the time and detection accuracy. Thus, we test four cameras and perform frequency sweeping as well as the subsequent AM-modulated frequency



(a) Different light durations (b) Different light intervals

Fig. 14. Trials of setting with different lighting setup.

point selection (phase 1 and 2) with different settings. Each camera is tested 50 times and the result is shown in Fig. 13. We first fix the scanning range to 600MHz (from 200MHz to 800MHz) and vary the FFT size with a sampling rate of 10MHz. The time required for each FFT size is shown in Fig. 13a. We find the FFT size of 2^{18} (262144) is the best resolution we could afford as phase 1 and 2 could still be completed in about 4.54s. Although a higher FFT size (e.g., 2^{19}) could provide a better spectrum resolution, the time cost is already too high (8.98s). Thus, we use the FFT size of 262144 for frequency sweeping.

We then vary the scanning range and check if the camera's AM-modulated frequency points could be selected. The percentage of finding each camera's frequency points is shown in Fig. 13b. We find that a scanning range over 300MHz is typically required for camera detection and a scanning range of 600MHz is enough for these cameras. Therefore, we configure CamRadar to scan from 200MHz to 800MHz (spanning 600MHz).

Setup of triggering light. As stated in section 6.3, we use the blinking light to trigger changes in the camera's EM emanation signals. Therefore, the duration of the light and the interval between two flashes will undoubtedly affect the detection of cameras and should be studied and set up in advance. We test three cameras, and for each one of them, we skip the frequency scanning process and directly collect signals at one of its leakage frequency points.

We first fix the interval between two flashes to 1 second and study how long the light should be on. If we use a long lighting duration, the unstable noise of the leakage signal will increase the probability of misjudgment. On the contrary, a too-short lighting duration will raise a concern that the light cannot cause enough changes to the camera's EM leakage. Fig. 14a shows the result. Due to the limitation of infrared control by the Arduino board, the minimum lighting duration can only be set to 50ms. We can see the false positive increases as the duration increases and that 50ms is optimal to trigger cameras.

As for the intervals, we fix the duration to 50ms and vary the interval from 0.25s to 2s, the result is shown in Fig. 14b. When the interval is too small, there will be a high false positive rate. Theoretically, the false positive rate will reach 100 percent if the interval is set to 0. Considering that a longer interval will introduce a greater time overhead, we set the interval to be 2s. Altogether, we use a duration of 50ms and an interval of 2s for the following evaluations. Due to the delay of the control flow and the performance of the light, we find that even if the code on the Arduino is designed to only light up for 50ms, the actual total time consumed by the blinking phase is about 400ms. This means that it takes $light\ is\ off(1s) + blinking(0.4s) * 2 + interval(1s) = 3.8s$ for each frequency point in phase 3.

7.2 Overall Performance

CamRadar's overall detection performance with 19 cameras is illustrated in Table 2. We compare CamRadar with LAPD [48], which is the existing state-of-the-art camera detection system for all kinds of cameras. CamRadar's

Table 2. Overall performance for CamRadar and LAPD.

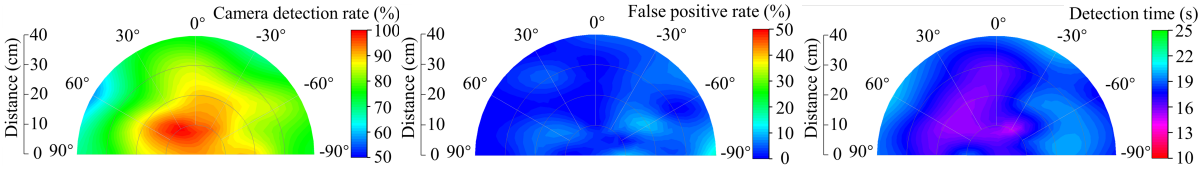
	Detection rate (%)	False positive rate (%)	Detection time (s)	Detectable range (cm)	Detectable angle	Hardware or software	User intervention
LAPD [48]	88.9	16.7	180	30-150	20°	software	yes
CamRadar	**93.23(10cm) 87.21(20cm)**	**3.95**	**16.75**	**0-40**	**180°**	**portable SDR**	**no**

data is collected by putting the antenna 10-40cm to the camera and from multiple angles. The detailed results concerning distance and angle can be found in section 7.3. *We can see CamRadar can achieve a comparable detection rate (93.23% at 10cm and 87.21% at 20cm) with LAPD while maintaining a much lower false positive rate (3.95%).* This should be attributed to our insights about the EM emanations from the camera.

In addition, benefiting from our well-designed detection procedure, *CamRadar can achieve detection for a suspicious object in a short time (16.75s) and has a significant advantage over LAPD (180s).* Note that LAPD may also use a faster version with a 77.8% detection rate, which still requires 60s and is much longer than CamRadar. Although LAPD has a farther detectable range, *CamRadar has a greater advantage in the detectable angle.* This is quite beneficial for practical use. For example, if the user suspects there is a hidden camera in a smoke detector, he/she could simply put CamRadar anywhere close to it and get the result with only one trial. Even if the user hopes to inspect the whole room (e.g., $4 \times 4m^2$) thoroughly, CamRadar would require $4m * 4/(20cm * 2) * 16.75s = 11.2$ minutes with a 20cm detection range. This could be further reduced to 5.6 minutes if a detection range of 40cm is used. In comparison, LAPD would use $4m * 4/(tan(20°/2) * 150cm * 2) * 180s = 90.7$ minutes with a detectable range of 150cm. However, a user does not need to search for the hidden camera inch by inch in practice, as the user could easily rule out most of the places where the camera is impossible to be hidden (e.g., in the wall). **Thus, the user just needs to inspect the limited suspicious objects with CamRadar to make sure the room is clear, which means a significantly-reduced inspection time (e.g., less than 3 minutes for 10 suspicious objects).** One of LAPD's advantages is the software implementation on smartphones, CamRadar uses a portable SDR to compensate for this. In addition, CamRadar's detection procedure requires little user intervention. The user just needs to set the antenna close to the suspicious object and wait for the result. These make CamRadar user-friendly with high usability.

7.3 Distance and Angle

In this section, we evaluate CamRadar's performance at different distances and from different angles. The camera is fixed in the center and we set the antenna in front of the camera from 10cm to 40cm and from -90° to 90°. We only consider the 180-degree view in front of the camera as it is almost impossible that a hidden camera's back is



(a) Camera detection rate (b) False positive rate (c) Detection time

Fig. 15. Camera detection performance with different angles and distances.

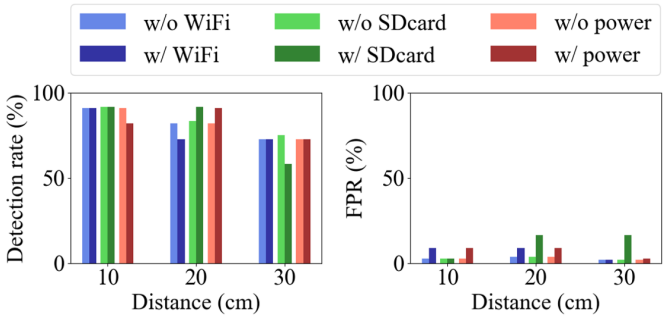


Fig. 16. Detection rate and false positive rate (FPR) with different working statuses.

facing the user. Fig. 15 shows CamRadar's camera detection rate, false positive rate, and detection time with all 19 cameras.

From Fig. 15a we can see CamRadar is capable of detecting cameras from all angles. Note that the distribution of detection rate is not symmetric as the EM field of the camera may not be symmetric, which has a slight effect on the detection rate. Anyway, **CamRadar can achieve an average detection rate of 93.23% at a distance of 10cm and 87.21% at 20cm.** Besides, we can see the camera detection rate is lower when CamRadar is away from the camera. This is because the signal strength of EM emanations decreases quickly over the air. Nevertheless, we can still achieve an average detection rate of 78.95% across all angles at 30cm and 70.68% at 40cm.

Fig. 15b shows CamRadar's false positive rate, which is low at all the positions. The average false positive rate across all the distances is as low as 3.95% and even the worst false positive rate at location (-90°, 40cm) is only 15.78%. Note that the false positive rate has little correlation with distance or angle. A false positive occurs only if an AM-modulated EM emission happens to fluctuate in CamRadar's detection window, which is highly random. Besides, note that our false positives are evaluated with a rigorous setup where there are electronic devices around and these devices are simulated using EM emanations from cameras. If there are no electronic devices around, phase 3 of CamRadar's detection procedure will not be raised and false positives will never occur, meaning that the false positive rate is likely to be much lower in practice. Moreover, the user can also turn off legitimate electronic devices to further reduce false positives.

The detection time is plotted in Fig. 15c. The time required for detection at each position ranges from 14.57s to 20.41s and is 16.75s on average. Recall that the time for each detection is mainly impacted by four parts: the frequency sweeping in phase 1, the number of groups that are checked in phase 2, the number of frequency points that are checked in phase 3, and the number of trials. Therefore, if the antenna is put at a position that has a high detection rate, it has a higher probability to detect the camera successfully and terminate the detection quickly. On the contrary, a low detection rate will induce more trials as the camera is harder to be found and results in more detection time. This relationship between detection rate and detection time can be clearly shown by comparing Fig. 15a and Fig. 15c.

7.4 Status of Camera

Camera working status. The EM emanations may vary when the camera is in a different working status. Thus, we evaluate the robustness of CamRadar considering camera transmissions and power supply. Two types of transmission are evaluated here, which are WiFi streaming and writing to SDcard respectively. As for the power supply, we consider whether the camera uses an external power supply (w/ power) or only uses the internal battery (w/o power). We put the antenna in front of the camera at a distance of 10cm, 20cm, and 30cm. The

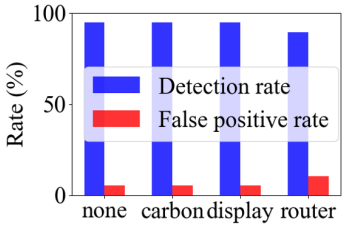


Fig. 17. Performance with various housings.

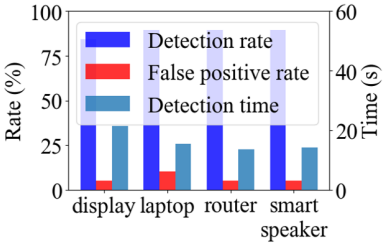


Fig. 18. Performance with electronic devices around.

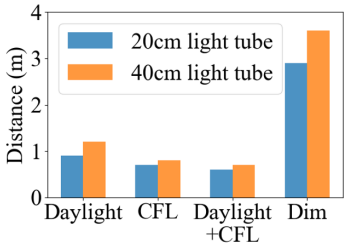


Fig. 19. The light's maximum placement distance under different ambient light.

detection rate and false positive rate are shown in Fig. 16. Note that the capabilities for our tested cameras may be different, which means the tested cameras for each status are not all the same. Specifically, experiments concerning WiFi and power both involve 11 small cameras, and experiments of SDcard uses 12 small cameras. We can see CamRadar could perform well no matter whether the camera is streaming via WiFi or writing to SDcard. Besides, the way of power supply also shows little impact on CamRadar.

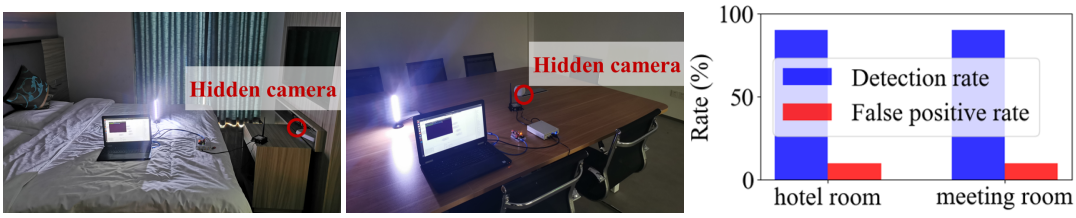
Camera housings. In practice, the camera may be hidden in various objects. Therefore, we deliberately put the cameras in different housings and evaluate CamRadar's performance. All the housing objects are not powered on and the antenna is fixed 15cm to the camera. The detection result is shown in Fig. 17, from which we can see the housings will not affect the detection of CamRadar.

Surrounding devices. Considering that cameras may be incorporated into working electronic devices to achieve stealthiness, these devices will also produce EM emanations that may confuse the detection. Therefore, we select four typical electronic devices and evaluate the performance of CamRadar when these devices are placed next to the camera. Specifically, the two surfaces are close to each other and they are equidistant from CamRadar's antenna. The antenna is fixed 15cm to the camera in this evaluation and the results are shown in Fig. 18. We can see the detection rate and false positive rate do not show great variations when the electronic devices are working around, which proves the effectiveness of CamRadar. It is also worth noting that the detection time used when a display is put next to the camera is a bit longer (at least 5 seconds) than the others. This is because the display will also produce AM-modulated EM emanations, which are intense and very similar to the camera's. Except that EM emanations of the display will not vary with the light. Thus, CamRadar will detect the EM emanations from the display in phase 1 and 2, and phase 3 is always required to reject the display, which results in a relatively longer detection time.

7.5 Lighting Condition

Since we use light as the stimulus, ambient lighting conditions will inevitably affect how well we stimulate the camera. We evaluate how faraway our small light tube can be put under different combinations of natural daylights and compact fluorescent light (CFL), which are the most typical light sources in daily life. Two light tubes that serve as the stimuli are used. One of them is 20cm long with a power of 6W and a luminous flux of 400lm, which has been used in other evaluation sections. The other one is 40cm long with a power of 8W and a luminous flux of 650lm. We ensure each light tube is in the camera's field of view during the experiments.

5 cameras are tested in this section and we fix CamRadar 15cm to the camera. The maximum distance the light tubes can be placed when the cameras can be detected by CamRadar is shown in Fig. 19. We ensure the camera is detected at least 4 out of 5 times during the experiment. We can find the stimulus effect is weaker in strong ambient light, which is about 1m. However, if we decrease the ambient light, CamRadar could stimulate and detect cameras with the light tube placed much further (>3m). **This implies that it is better to dim the**



(a) Hotel room (b) Meeting room (c) Result

Fig. 20. Detection performance in various environments.

indoor ambient light when using CamRadar. Besides, we can see the light tube with a higher luminous flux could be placed further. Note that the brightness of the light tubes used in our experiments is relatively low. In fact, indoor light tubes with more than 1000lm can be seen everywhere, which means that stronger light tubes can be used to further increase the distance. What is more, we also find that the light source does not necessarily need to come up in the scene of the camera, although the stimulus effect could be weaker. For example, the opening of indoor lights could also make the EM emanations of a camera fluctuate a lot. In sum, the intensity of the stimulus and the intensity of the ambient light dominate everything.

7.6 Varying Environments

We also evaluate CamRadar in two practical scenarios: a hotel room and a meeting room (shown in Fig. 20). When the camera is in a new scenario, not only the EM signals in the environment are different, but also the scene the camera is facing becomes different. 10 small commercial cameras are tested in each scenario. We specifically put cameras in a location where they could be hidden. Then we control the indoor lighting to a state that is dim but does not affect daily behavior. For example, we close the curtains. We ask a tester who is unknown of the camera's location to use CamRadar to detect the possible camera in the room. The detection rate and false positive rate are shown in Fig. 20c. We can see CamRadar could perform well in various environments.

7.7 Resilience to Adaptive Attackers

If the presence of CamRadar is known, an adaptive attacker may try to avoid being detected in two directions: suppress the EM emanations via EM shielding or introduce more EM noises.

EM shielding. As the camera's EM emanations are unintentional, it is hard to suppress the signal by modifying the device circuit. Thus, the attacker may use EM shielding (e.g., a metal shell) to suppress the EM emanations. **However, a camera can never be completely shielded as its lens has to be put outside, which could make the detection still feasible.** We experiment to put commercial small cameras in a faraday cage made up of EM shielding material (e.g., aluminum foil) with the lens exposed. *We find that although the EM emanations are kind of suppressed, CamRadar can still detect 10 out of 14 cameras at a distance of 15cm.* Moreover, EM shielding will inevitably result in a larger size of the camera and reduce the concealment of the camera. Especially considering that some hidden cameras have a long wire connecting the sensor and the ISP circuit, they are more covert and more threatening but also harder to cover.

EM noises. The attacker could introduce more noises either from the frequency domain (targes phase 1 and 2 of CamRadar) or the time domain (targes phase 3). However, adding EM noises to cover the frequency domain requires a noise spanning across a wide band to hide the camera's leakage spikes, which is impractical. To introduce noises in the time domain, the attacker has to first introduce noises at most of the camera's frequency spikes. One probably the most convenient solution could be using another camera of the same model, which should

have the most similar EM emanations. Then when we AM-demodulate at a leakage frequency, the amplitude would be the superposition of two or more cameras, which may affect the detection of CamRadar. To evaluate this scenario, we use two models of four cameras and see how CamRadar performs when two cameras of the same model are put together and working at the same time. We find that because the two cameras are of the same model, their time-domain signal periods are the same, and the superposed time-domain signal is still periodic. In addition, even if the two cameras are of the same model, their signal strengths and waveforms at different frequency points are different, and there are still many frequency points whose waveforms meet the detection conditions of CamRadar. We detect 12 times for each camera model and succeed 9 times on average. Although we could not detect two cameras at the same time, the user can detect and eliminate cameras one by one.

8 DISCUSSIONS

Increase of detection range. CamRadar's detection range is possible to further increase. On the one hand, when CamRadar is far from the camera, the intensity of the camera's frequency spikes is weak and the time-domain variations to the light are obscure. However, it is possible to use machine-learning methods [17, 66] to help find those weaker frequency spikes and detect minor changes. Thus, CamRadar could achieve a larger detection range. On the other, the antenna used by CamRadar is simply a 3dBi omnidirectional antenna. Although it can already achieve a good result, we should note that the signals from 180 degrees behind are completely useless noises in practical use. Therefore, CamRadar may use an antenna with stronger directionality and higher gain [4] to increase the detection range.

Light stimulus. CamRadar is equipped with a common infrared-controlled led tube and an Arduino simply for easy control of the light stimulus. The Arduino board uses an infrared transmitter to control the tube's on and off. In practice, if there are smart bulbs indoors that can be controlled remotely [63], CamRadar could directly use the existing bulbs as the stimuli for cameras. Thus, the Arduino and the light tube are no longer needed.

Small form factor. To provide better portability, CamRadar's size could be further reduced. For example, the laptop could be replaced by small-size computers like the LattePanda [14], whose size is close to a smartphone. Or it is possible to discard the standalone computer and directly use the MCU of the SDR for processing like the PortaPack [60] for HackRF. These approaches make it possible for CamRadar to reach the size of a palm. Thus, the portability could be increased.

Automation. We could note that the detection procedure of CamRadar does not require human intervention (except for the setup of light and antenna). This is a great advantage of CamRadar and can be further improved for practical use. For example, CamRadar could be used with increasingly popular robot platforms like the cleaning robot and the room service robot [16, 52]. Thus, the robot could be scheduled to scan the whole room automatically.

Non-sharp frequency spikes. We also find a small number of low-end cameras' EM emanations have a wide band instead of sharp frequency spikes in the spectrum. This could be because they use less stable (cheaper or simpler) oscillators. However, we find these frequencies are still AM-modulated. Therefore, CamRadar could be further improved by covering these cameras.

Manual assistance. CamRadar is designed with an automatic process to release the burden of users. In practice, an experienced user may increase the detection performance with some manual assistance. For example, CamRadar can easily report potential EM emanations with steps 1&2, this information can be particularly useful as there should be no electronic device around (e.g., in the ceiling). The user can manually inspect these emanations and help screen possible frequencies or directly check if the emanations come from nearby locations. In this case, the sign of abnormal signal source is already enough to alarm the user and the detection accuracy can be increased.

EMI reduction. We have shown that simple EM shielding has a limited effect in evading CamRadar's detection in Section 7.7. However, advanced attackers with careful EMI reduction [6, 68] or selection of low-EMI cameras may

reduce the hidden camera's EMI to minimum. CamRadar will fail to detect these cameras if their EM emanations are too weak.

Scheduled cameras. As mentioned in section 3, CamRadar works with an assumption that the hidden camera is continuously working during the detection process. However, if the camera is exactly inactive when CamRadar performs detection, the camera will evade the detection. Thus, a scheduled camera [71] that works intermittently (e.g., only work during night) will have a higher probability of being undetectable by CamRadar.

Motion influence. As CamRadar requires a detection time of 16.75s on average, holding it by the user may introduce some motion interference. Although we empirically believe that slight motion may have little effect on detection performance, rigorous motion effect experiments are not explored in this paper. Considering that CamRadar is a prototype system now, we intend to leave motion impacts as future work to test the effects after miniaturization of CamRadar.

9 RELATED WORK

Hidden camera detection. Due to their small form factors, hidden cameras are hard to detect with naked eyes. There are a few Apps and commercial detectors that claim to be able to detect cameras [59, 72]. A great number of them utilize light-reflection-based methods that require users to detect the tell-tale signs of tiny reflections. Other Apps claim to detect magnetic materials with the magnetometer. Unfortunately, those methods are found unable to work reliably [12]. The reflective surfaces could lead to high false positives to the light-reflection-based methods [48]. The magnetometer-based methods also show poor performance due to their vulnerability to small changes in the EM field. Interferences from other electronic devices could greatly impact their effectiveness [12, 71].

Recently, various academic works have been proposed to detect hidden cameras, which can be mainly divided into three categories.

- The first category detects the hidden camera by correlating the wireless traffic pattern with human motions [12, 35, 41, 47, 64]. State-of-the-art works [26, 53] further show it is possible to pinpoint the hidden camera by creating motion stimuli and sniffing wireless traffic. While these approaches are promising, they are quite limited in practice as they only target wireless cameras. In practice, hidden cameras could use SD cards to store the video locally and cameras using the cellular network for wireless transmissions are commonly available.
- The second category uses high-precision laser arrays to obtain high-energy cat-eye reflection from the hidden camera [28, 36, 37]. Specifically, the hidden camera will reflect the laser beam at a higher intensity as the camera's sensor system is often retroreflective [19]. While these works can detect not only wireless cameras and even inactive cameras, they require expensive laboratory equipment or high-precision sensors that are unavailable to the general public. Besides, the reflections are limited by the camera's optical properties and cameras can be detected only at constrained angles, which reduces the practicality. A recent work [48] uses a smartphone to obtain cat-eye reflection from hidden cameras. However, it still has a high false positive rate (16.7%) and requires a long manual scanning time (60 seconds) for simply one suspicious object. Besides, similar to other reflection-based methods, its detection angle is quite limited: the user has to face the hidden camera and detect it in the camera's 20° field of view.
- The third category uses thermal imaging to detect hidden cameras. A recent work [71] uses a thermal camera to identify areas that correspond to potential hidden devices. The heat generated from a hidden camera could make it distinct from the ambient environment in a thermal image. This method is effective to various surveillance devices and could detect currently inactive devices that have worked recently. However, thermal imaging also has a few drawbacks. Hidden cameras behind a reflective object can make the thermal-based detection ineffective. Besides, the heat from other devices could be potential interferences. For example, a camera hidden in a working router may constitute a great challenge to thermal-based detections.

Compared to the approaches above, CamRadar utilizes the unintentional EM leakage from the camera as the distinct characteristic for camera detection and offers the following advantages: (1) not limited to camera communication types, (2) arbitrary detection angles, (3) robust to environmental interferences (effective even if the camera is embedded into other electronic devices), and (4) automatic detection process without human intervention.

On the other hand, CamRadar also has some limitations compared with existing approaches: (1) Additional hardware. CamRadar uses a portable SDR for detection. In contrast, some methods (magnetometer-based methods and LAPD [48]) only require a smartphone. (2) Distance limitation. As EM emanations decay rapidly in the air, CamRadar's performance is limited by the distance to the camera and a closer distance is recommended. Thus, using CamRadar to detect some suspicious objects could be a better option (e.g., checking if there is a camera hidden in a router). Nevertheless, a combination of multiple methods should be the optimal strategy to detect all the hidden cameras.

EM side-channels. EM side-channels have been widely exploited for attacks. For example, EM leakage can be used to restore the display [24, 33, 38], to achieve data exfiltration from air-gapped computers [22, 23, 51], to retrieve cryptographic keys [2, 10, 11], and to infer keystrokes [29]. Apart from attacks, researchers recently have started to study how to leverage EM side-channels to help defense. For instance, EM emanations have been exploited to detect wireless eavesdroppers [50] and discover malware attacks [30, 69]. Yet, to the best of our knowledge, there has been little work leveraging EM leakage to detect cameras. CamRadar is the first work to leverage the camera's AM-modulated EM leakage for hidden camera detection.

EMI-based device identification. Electronic devices inevitably generate EM emanations, which are influenced by their hardware and software. This property enables EM emanations to serve as the signature for device identification [21, 61, 70]. Göksu et al. [18] use features derived from the wavelet packet analysis of measured emissions to detect and identify vehicles. Gulati et al. [20] propose an in-depth study into high-frequency EMI signatures of multiple appliances. Laput et al. [32] propose a proof-of-concept wearable implementation to capture EM emanations and successfully distinguish general classes of objects with a support vector machine (SVM) classifier. Except for device identification of different classes, EM emanations have been further demonstrated to identify objects of the same model. Yang et al. [65] show that devices like electronic toys, cellphones and laptops can all be individually identified. Cheng et al. [13] utilize the featured EMI signals radiated by CPU modules to fingerprint devices. The uniquely distinguishable EM emanation patterns of a known electronic device could also help to identify any potential hardware modification [49]. This feature has been leveraged to detect malicious modifications at the fabrication level [67] and distinguish counterfeit hardwares [1].

Generally, EMI-based device identification samples signals at a specific frequency and attempts to identify different devices by extracting various features from the EM emanation. The identification requires prior registration and training. In contrast, our work targets a slightly different goal. We are trying to identify potential cameras out of various electronic devices. Our target camera has various unknown leakage frequencies and we have no prior knowledge about the camera.

10 CONCLUSION

In this paper, we investigate the EM emanations of the cameras and find the camera sensor images are AM-modulated to the clock leakage. Based on this, we propose a novel system named CamRadar, which can detect hidden cameras by checking the existence of camera EM emanations. CamRadar can automatically detect cameras regardless of their transmission types from any angle. The effectiveness and robustness of CamRadar have been demonstrated under different scenarios with 19 small cameras. CamRadar's fast detection procedure (16.75s on average) ensures a high detection rate (93.23%) as well as a low false positive rate (3.95%).

ACKNOWLEDGEMENTS

The authors would like to thank all anonymous reviewers for their insightful comments on this paper. This research was in part supported by the National Key R&D Program of China (Grant No. 2020AAA0107700), National Natural Science Foundation of China (Grants No. 62032021, 61972348, 61772236, 62172359, and 62102354), Leading Innovative and Entrepreneur Team Introduction Program of Zhejiang (Grant No. 2018R01005), Fundamental Research Funds for the Central Universities (No. 2021FZZX001-27), Research Institute of Cyberspace Governance in Zhejiang University.

REFERENCES

[1] Mosabbah Mushir Ahmed, David Hely, Nicolas Barbot, Romain Siragusa, Etienne Perret, Maxime Bernier, and Fredric Garet. 2017. Radiated electromagnetic emission for integrated circuit authentication. *IEEE Microwave and Wireless Components Letters* 27, 11 (2017), 1028–1030.

[2] Monjur Alam, Haider Adnan Khan, Moumita Dey, Nishith Sinha, Robert Callan, Alenka Zajic, and Milos Prvulovic. 2018. One&Done: A Single-Decryption EM-Based Attack on OpenSSL's Constant-Time Blinded {RSA}. In *27th {USENIX} Security Symposium ({USENIX} Security 18)*. 585–602.

[3] Amazon. 2022. *hidden cameras*. https://tinyurl.com/83h9hkes

[4] Ardalan Amiri Sani, Lin Zhong, and Ashutosh Sabharwal. 2010. Directional antenna diversity for mobile devices: Characterizations and solutions. In *Proceedings of the sixteenth annual international conference on Mobile computing and networking*. 221–232.

[5] ANI. 2021. China launches fresh crackdown on spy cameras in a bid to tighten digital privacy laws. https://tinyurl.com/ya95r4k2.

[6] Bruce Archambeault, Colin Brench, and Sam Connor. 2010. Review of printed-circuit-board level EMI/EMC issues and tools. *IEEE Transactions on Electromagnetic compatibility* 52, 2 (2010), 455–461.

[7] Laura Bicker. 2021. 'I was humiliated': The continuing trauma of South Korea's spy cam victims. https://tinyurl.com/bdcmk4vr.

[8] Gabrielle Burkhart. 2021. New Mexico police chief investigated for hidden camera in office vent. https://tinyurl.com/bdhded3v.

[9] Robert Callan, Alenka Zajić, and Milos Prvulovic. 2015. FASE: Finding amplitude-modulated side-channel emanations. In *2015 ACM/IEEE 42nd Annual International Symposium on Computer Architecture (ISCA)*. IEEE, 592–603.

[10] Giovanni Camurati, Aurélien Francillon, and François-Xavier Standaert. 2020. Understanding screaming channels: From a detailed analysis to improved attacks. *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2020), 358–401.

[11] Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, and Aurélien Francillon. 2018. Screaming channels: When electromagnetic side channels meet radio transceivers. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. 163–177.

[12] Yushi Cheng, Xiaoyu Ji, Tianyang Lu, and Wenyuan Xu. 2018. Dewicam: Detecting hidden wireless cameras via smartphones. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*. 1–13.

[13] Yushi Cheng, Xiaoyu Ji, Juchuan Zhang, Wenyuan Xu, and Yi-Chao Chen. 2019. Demicpu: Device fingerprinting with magnetic signals radiated by cpu. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 1149–1170.

[14] DFROBOT. 2022. LattePanda Alpha 864s. https://www.dfrobot.com/product-1728.html.

[15] Lawrence J Fennelly. 2016. *Effective physical security*. Butterworth-Heinemann.

[16] Julia Fink, Valérie Bauwens, Frédéric Kaplan, and Pierre Dillenbourg. 2013. Living with a vacuum cleaning robot. *International Journal of Social Robotics* 5, 3 (2013), 389–408.

[17] Lorenzo Giambagli, Lorenzo Buffoni, Timoteo Carletti, Walter Nocentini, and Duccio Fanelli. 2021. Machine learning in spectral domain. *Nature communications* 12, 1 (2021), 1–9.

[18] Hüseyin Göksu, Donald C Wunsch, Xiaopeng Dong, Ali Kökce, and Daryl G Beetner. 2018. Detection and identification of vehicles based on their spark-free unintended electromagnetic emissions. *IEEE Transactions on Electromagnetic Compatibility* 60, 5 (2018), 1594–1597.

[19] Mali Gong, Sifeng He, Rui Guo, and Wei Wang. 2016. Cat-eye effect reflected beam profiles of an optical system with sensor array. *Applied Optics* 55, 16 (2016), 4461–4466.

[20] Manoj Gulati, Shobha Sundar Ram, and Amarjeet Singh. 2014. An in depth study into using EMI signatures for appliance identification. In *Proceedings of the 1st ACM Conference on Embedded Systems for Energy-efficient Buildings*. 70–79.

[21] Sidhant Gupta, Matthew S Reynolds, and Shwetak N Patel. 2010. ElectriSense: single-point sensing using EMI for electrical event detection and classification in the home. In *Proceedings of the 12th ACM international conference on Ubiquitous computing*. 139–148.

[22] Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval Elovici. 2015. Gsmem: Data exfiltration from air-gapped computers over {GSM} frequencies. In *24th {USENIX} Security Symposium ({USENIX} Security 15)*. 849–864.

[23] Mordechai Guri, Matan Monitz, and Yuval Elovici. 2016. USBee: Air-gap covert-channel via electromagnetic emission from USB. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 264–268.

[24] Yuichi Hayashi, Naofumi Homma, Mamoru Miura, Takafumi Aoki, and Hideaki Sone. 2014. A threat for tablet pcs in public space: Remote visualization of screen images using em emanation. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. 954–965.
[25] Yu-ichi Hayashi, Naofumi Homma, Yohei Toriumi, Kazuhiro Takaya, and Takafumi Aoki. 2016. Remote visualization of screen images using a pseudo-antenna that blends into the mobile environment. *IEEE Transactions on Electromagnetic Compatibility* 59, 1 (2016), 24–33.
[26] Yan He, Qiuye He, Song Fang, and Yao Liu. 2021. MotionCompass: pinpointing wireless camera via motion-activated traffic. In *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*. 215–227.
[27] HOID. 2017. Create a Wireless Spy Camera Using a Raspberry Pi. https://tinyurl.com/yvv3ukh5.
[28] Jiahao Huang, Haiyang Zhang, Lin Wang, Zilong Zhang, and Changming Zhao. 2021. Improved YOLOv3 Model for miniature camera detection. *Optics & Laser Technology* 142 (2021), 107133.
[29] Wenqiang Jin, Srinivasan Murali, Huadi Zhu, and Ming Li. 2021. Periscope: A Keystroke Inference Attack Using Human Coupled Electromagnetic Emanations. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. 700–714.
[30] Haider Adnan Khan, Nader Sehatbakhsh, Luong N Nguyen, Milos Prvulovic, and Alenka Zajić. 2019. Malware detection in embedded systems using neural network model for electromagnetic side-channel signals. *Journal of Hardware and Systems Security* 3, 4 (2019), 305–318.
[31] Brian Krebs. 2019. Hidden Cam Above Bluetooth Pump Skimmer. https://tinyurl.com/d5sm9p9v.
[32] Gierad Laput, Chouchang Yang, Robert Xiao, Alanson Sample, and Chris Harrison. 2015. Em-sense: Touch recognition of uninstrumented, electrical and electromechanical objects. In *Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology*. 157–166.
[33] Ho Seong Lee, Dong Hoon Choi, Kyuhong Sim, and Jong-Gwan Yook. 2018. Information recovery using electromagnetic emanations from display devices under realistic environment. *IEEE Transactions on Electromagnetic Compatibility* 61, 4 (2018), 1098–1106.
[34] ALTHEA LEGASPI. 2021. Audiotree Cofounder Accused of Using Hidden Cameras to Take Nude Images. https://tinyurl.com/yuvcy6ry.
[35] Zhijing Li, Zhujun Xiao, Yanzi Zhu, Irene Pattarachanyakul, Ben Y Zhao, and Haitao Zheng. 2018. Adversarial localization against wireless cameras. In *Proceedings of the 19th International Workshop on Mobile Computing Systems & Applications*. 87–92.
[36] Chun Liu, Changming Zhao, Haiyang Zhang, Zilong Zhang, Zitao Cai, and Zhipeng Li. 2019. Spectrum classification using convolutional neural networks for a mini-camera detection system. *Applied optics* 58, 33 (2019), 9230–9239.
[37] Chun Liu, Changming Zhao, Haiyang Zhang, Zilong Zhang, Yanwang Zhai, and Yali Zhang. 2019. Design of an Active Laser Mini-Camera Detection System Using CNN. *IEEE Photonics Journal* 11, 6 (2019), 1–12.
[38] Zhuoran Liu, Niels Samwel, Léo Weissbart, Zhengyu Zhao, Dirk Lauret, Lejla Batina, and Martha Larson. 2020. Screen Gleaning: A Screen Reading TEMPEST Attack on Mobile Devices Exploiting an Electromagnetic Side Channel. *arXiv preprint arXiv:2011.09877* (2020).
[39] Marc J Loinaz, Kanwar Jit Singh, Andrew J Blanksby, David A Inglis, Kamran Azadet, and Bryan D Ackland. 1998. A 200-mW, 3.3-V, CMOS color camera IC producing 352/spl times/288 24-b video at 30 frames/s. *IEEE Journal of Solid-State Circuits* 33, 12 (1998), 2092–2103.
[40] Lime Microsystems Ltd. 2020. LimeSDR. https://limemicro.com/products/boards/limesdr/.
[41] Richard Mitev, Anna Pazii, Markus Miettinen, William Enck, and Ahmad-Reza Sadeghi. 2020. Leakypick: Iot audio spy detector. In *Annual Computer Security Applications Conference*. 694–705.
[42] NI. 2022. USRP B210. https://www.ettus.com/all-products/ub210-kit/.
[43] The Associated Press. 2021. Seoul police arrest 4 over cameras hidden in entire motel. https://tinyurl.com/bdfxcrms.
[44] Milos Prvulovic, Alenka Zajić, Robert L Callan, and Christopher J Wang. 2016. A method for finding frequency-modulated and amplitude-modulated electromagnetic emanations in computer systems. *IEEE Transactions on Electromagnetic Compatibility* 59, 1 (2016), 34–42.
[45] reatscottgadgets.com. 2021. HackRF Product Line. https://greatscottgadgets.com/hackrf/.
[46] Rebecca Salinas. 2021. Arrest made after plumber finds camera hidden in women's bathroom. https://tinyurl.com/bzuvudu9.
[47] Muhammad Salman, Nguyen Dao, Uichin Lee, and Youngtae Noh. 2022. CSI: DeSpy: Enabling Effortless Spy Camera Detection via Passive Sensing of User Activities and Bitrate Variations. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 6, 2 (2022), 1–27.
[48] Sriram Sami, Sean Rui Xiang Tan, Bangjie Sun, and Jun Han. 2021. LAPD: Hidden Spy Camera Detection using Smartphone Time-of-Flight Sensors. In *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems*. 288–301.
[49] Asanka Sayakkara, Nhien-An Le-Khac, and Mark Scanlon. 2019. A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics. *Digital Investigation* 29 (2019), 43–54.
[50] Cheng Shen and Jun Huang. 2021. EarFisher: Detecting Wireless Eavesdroppers by Stimulating and Sensing Memory {EMR}. In *18th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 21)*. 873–886.
[51] Cheng Shen, Tian Liu, Jun Huang, and Rui Tan. 2021. When LoRa meets EMR: Electromagnetic covert channels can be super resilient. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1304–1317.

[52] Takeshi Shimmura, Ryosuke Ichikari, Takashi Okuma, Hiroyuki Ito, Kei Okada, and Tomomi Nonaka. 2020. Service robot introduction to a restaurant enhances both labor productivity and service quality. *Procedia CIRP* 88 (2020), 589–594.
[53] Akash Deep Singh, Luis Garcia, Joseph Noor, and Mani Srivastava. 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)*.
[54] SpyGadgets. 2021. Hidden Cameras. https://tinyurl.com/2p9yuaxx.
[55] MB Sruthi, M Abirami, Akhil Manikkoth, R Gandhiraj, and KP Soman. 2013. Low cost digital transceiver design for Software Defined Radio using RTL-SDR. In *2013 international mutli-conference on automation, computing, communication, control and compressed sensing (iMac4s)*. IEEE, 852–855.
[56] TaoBao. 2022. *cameras*. https://tinyurl.com/29y6hvxp
[57] CBSNewYork Team. 2021. Brooklyn Man Thomas Tamborski Accused Of Spying On Female Roommates With Hidden Cameras. https://tinyurl.com/2d4n2bsp.
[58] IPVM Team. 2021. Frame Rate Guide for Video Surveillance. https://tinyurl.com/65v7m2cm.
[59] technlicious. 2019. The Secrets to Finding Hidden Cameras.
[60] ShareBrained Technology. 2022. portapack-hackrf. https://github.com/sharebrained/portapack-hackrf.
[61] Frank T Werner, Baki Berkay Yilmaz, Milos Prvulovic, and Alenka Zajić. 2020. Leveraging em side-channels for recognizing components on a motherboard. *IEEE Transactions on Electromagnetic Compatibility* 63, 2 (2020), 502–515.
[62] Wikipedia. 2021. Crystal oscillator frequencies. https://tinyurl.com/2p8whasc.
[63] WIRED. 2021. The Best Smart Bulbs to Light Up Your Room. https://tinyurl.com/mvrc3dx9.
[64] Kevin Wu and Brent Lagesse. 2019. Do you see what i see? detecting hidden streaming cameras through similarity of simultaneous observation. In *2019 IEEE International Conference on Pervasive Computing and Communications (PerCom*. IEEE, 1–10.
[65] Chouchang Yang and Alanson P Sample. 2016. EM-ID: Tag-less identification of electrical devices via electromagnetic emissions. In *2016 IEEE International Conference on RFID (RFID)*. IEEE, 1–8.
[66] Jie Yang, Jinfan Xu, Xiaolei Zhang, Chiyu Wu, Tao Lin, and Yibin Ying. 2019. Deep learning for vibrational spectral analysis: Recent progress and a practical guide. *Analytica Chimica Acta* 1081 (2019), 6–17.
[67] Kaiyuan Yang, Matthew Hicks, Qing Dong, Todd Austin, and Dennis Sylvester. 2017. Exploiting the analog properties of digital circuits for malicious hardware. *Commun. ACM* 60, 9 (2017), 83–91.
[68] Juntao Yao, Zhedong Ma, Yanwen Lai, and Shuo Wang. 2021. A survey of modeling and reduction techniques of radiated EMI in power electronics. In *2021 IEEE International Joint EMC/SI/PI and EMC Europe Symposium*. IEEE, 1081–1086.
[69] Zhenkai Zhang, Zihao Zhan, Daniel Balasubramanian, Bo Li, Peter Volgyesi, and Xenofon Koutsoukos. 2020. Leveraging em side-channel information to detect rowhammer attacks. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 729–746.
[70] Nan Zhao, Gershon Dublon, Nicholas Gillian, Artem Dementyev, and Joseph A Paradiso. 2015. EMI Spy: Harnessing electromagnetic interference for low-cost, rapid prototyping of proxemic interaction. In *2015 IEEE 12th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*. IEEE, 1–6.
[71] Agustin Zuniga, Naser Hossein Motlagh, Mohammad A Hoque, Sasu Tarkoma, Huber Flores, and Petteri Nurmi. 2022. See No Evil: Discovering Covert Surveillance Devices Using Thermal Imaging. *IEEE Pervasive Computing* (2022).
[72] Hashir Zuniga. 2022. 12 Best Hidden Camera Detector Apps for Android and iOS. https://tinyurl.com/5n8wnne7.