

# A Computational Harmonic Detection Algorithm to Detect Data Leakage through EM Emanation

Md Faizul Bari, *Student Member, IEEE*, Meghna Roy Chowdhury, *Student Member, IEEE*, Shreyas Sen, *Senior Member, IEEE*

**Abstract**—Unintended electromagnetic emissions, called EM emanations, can be exploited to recover sensitive information, posing security risks. Metal shielding, used by defense organizations to prevent data leakage, is costly and impractical for widespread use. This issue is particularly significant for IoT devices due to their sheer volume and varied deployment environments. Therefore, there is a research need for an automated detection method to monitor facilities and address data leakage promptly. To resolve this challenge, in the preliminary version of this work [1], a CNN-based detection method was proposed using HDMI cable emanations that provided  $\sim 95\%$  accuracy up to 22.5 m but had limitations due to training data. In this extended version, we augment the initial study by collecting and characterizing emanation data from IoT devices, everyday electronics, and cables. We propose a harmonic-based emanation detection method by developing a computational harmonic detection algorithm. The proposed method addresses the limitations of the CNN-based method and provides  $\sim 100\%$  accuracy not only for HDMI emanation (compared to  $\sim 95\%$  in the earlier CNN method) but also for all other tested devices and cables. Finally, it has also been tested in different environments to prove its efficacy in practical scenarios.

**Index Terms**—emanation, unintended radiated emission, side channel, electromagnetic compatibility, CNN, harmonic detection, Arduino, Zigbee, EMSEC, URE

## I. INTRODUCTION

### A. Background

**D**IGITAL signal switching between logic states causes unintended electromagnetic (EM) emissions from electronic devices and connecting wires. This unintentional switching emission is called ‘*electromagnetic emanation*’. It creates electromagnetic interference (EMI) to the nearby desired signals and may lead to the violation of electromagnetic compatibility (EMC) regulations. In addition to that, the emanation signal contains a significant correlation with the source signal, leading to the recovery of the bit pattern of the source data from it. Essentially emanation provides a ‘*side-channel for information leakage*’ that the attackers can exploit to exfiltrate data, posing a crucial threat to data security.

Fig. 1(a) explains the concept and characteristics of EM emanations. Such EM side-channel leakage has been exploited

Manuscript received October 9, 2024; revised April 11, 2025; accepted June 4, 2025. This work was supported by the Office of the Director of National Intelligence (ODNI), Intelligence Advanced Research Projects Activity (IARPA), via contract: 2021-21062400006. (Corresponding author: Md Faizul Bari)

The authors are with the Elmore Family School of Electrical and Computer Engineering, Purdue University, West Lafayette, Indiana 47907, USA (e-mail: mbari@purdue.edu; mroycho@purdue.edu; shreyas@purdue.edu)

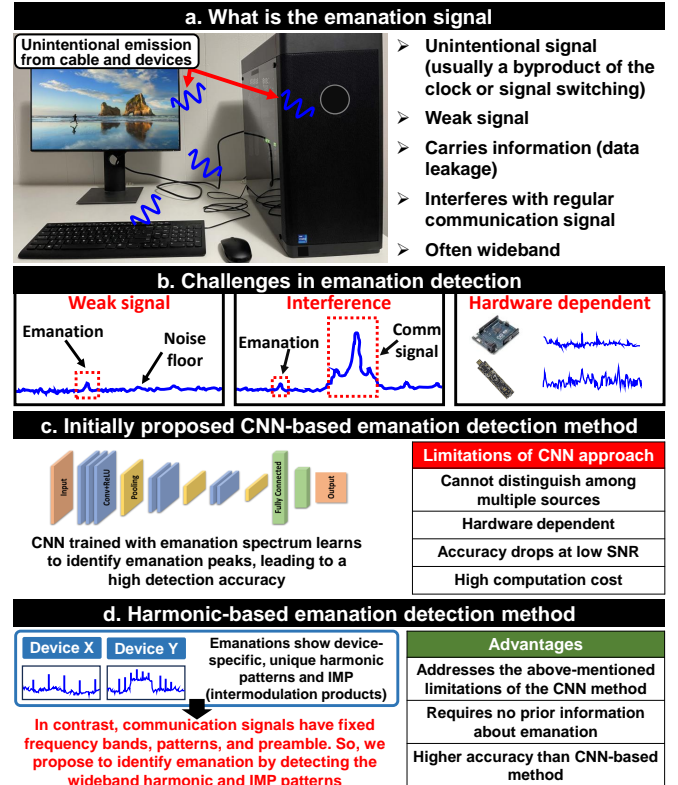


Fig. 1. (a) Emanation is unintentional emission from electronic devices and cables. It is a byproduct of signal switching. (b) The challenges in emanation detection stem from the fact that these are weak signals as they weren't designed to be transmitted. They are often overcast by strong interference from communication signals. (c) A CNN, trained with the processed power spectrum, can distinguish the emanation peaks from other signals. However, it's hardware-dependent, cannot distinguish multiple sources if present, struggles at low SNR, and has a high computation cost. (d) Proposed harmonic-based emanation detection method. A peak detector finds the energy peaks in the spectrum and our computational harmonic detector finds the harmonic patterns. This method addresses all the limitations of the CNN-based method.

for cryptographic key recovery [2]–[4], keystroke inference [5], [6], monitoring USB device activity [7], detecting DNN architecture [8], monitoring smartphone camera activity [9], cryptographic algorithm and key length detection [10], program activity monitoring [11], covert communication [12], [13], reconstructing screen images [14]–[17], etc. To secure sensitive facilities, a metal shielding (Faraday Cage) is deployed to contain the emission within it. However, this is not always feasible for government facilities in the wild (e.g., a

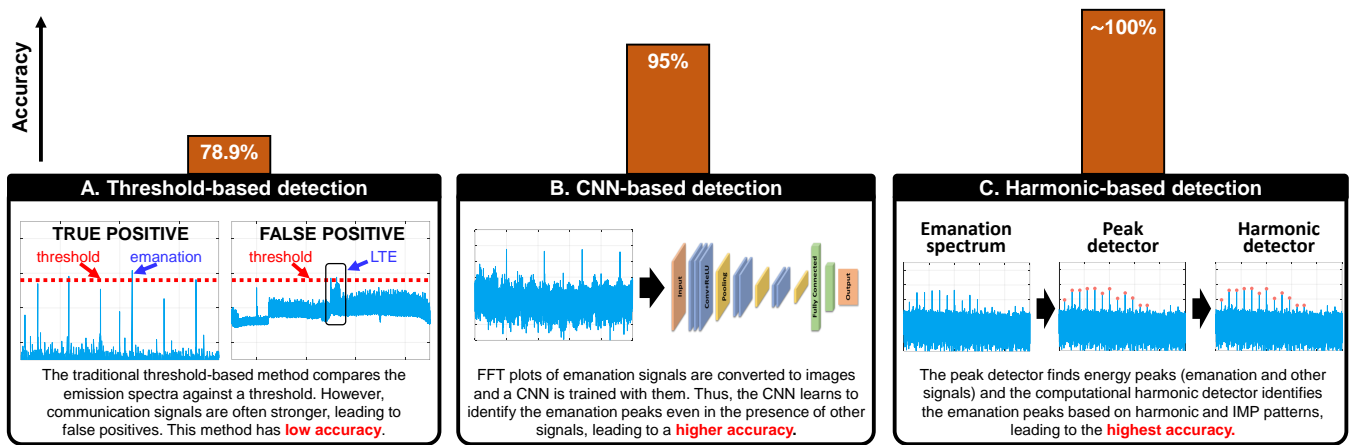


Fig. 2. Our algorithm development journey from traditional threshold-based method to initial CNN-based method to currently proposed harmonic-based method. (a) Traditionally used threshold-based method compares the emission peaks against a threshold value. However, too high or too low threshold results in false negatives and false positives respectively. In general, this method has the worst performance. (b) In the CNN-based method, FFT plots are treated as images and fed to a CNN which learns to distinguish between the emanation and other signals. This approach renders much higher accuracy, though it has some limitations stemming mostly from the training data. (c) The harmonic-based method exploits emanations' distinct harmonic and IMP patterns compared to other signals. This method performs the best of the three with  $\sim 100\%$  accuracy.

temporary base in a foreign country). Also, for non-military facilities, shielding is not the best solution because almost all electronic devices leak EM emanation. Shielding the huge number of electronic devices being used every day leads to a massive cost and inconvenience. This is an even more substantial issue for Internet of Things (IoT) devices which are already deployed in large numbers and growing rapidly. Research company IoT Analytics has predicted that there will be nearly 18.8 billion IoT devices by the end of 2024 [18]. Also, even if the shielding is deployed, it may deteriorate over time or be damaged by a malicious adversary, leading to the failure in leakage containment. The best solution is to dynamically monitor the RF spectrum for EM side channel leakage and take steps if significant emanation is detected. However, the current emanation detection method involves RF spectrum sensing using EM probes or SDRs and analyzing them manually. This calls for a research need to develop a smart and automatic emanation detection method which prompted several agencies to fund such research projects (e.g. SCISRS [19] project by IARPA).

Fig. 1(b) explains the challenges in detecting EM emanation automatically. Emanations are weak as they are just leakage signals. From the perspective of emanation detection, regular communication signals are much stronger and act as interference. Also, EM emanation is hardware-dependent and its emission frequency can be anywhere in the spectrum. Searching such weak signals within the huge RF spectrum is akin to looking for a needle in a haystack. In our initial observation, it was found that HDMI cables had relatively stronger emanations compared to other off-the-shelf electronic components and peripherals. So, in the preliminary version of this work [1], we collected data from HDMI cables of 3 different shielding types (unshielded, single-shielded, and double-shielded) using Ettus B210 SDR as a receiver (RX) in an office environment. Improving SNR through time and frequency-domain processing and applying transfer learning approach (a

pretrained ResNet50 has been retrained using spectrum plots as images), we achieved  $\sim 100\%$  detection accuracy up to 16 m from the target cable and  $\sim 95\%$  accuracy at 22.5 m, even in the presence of strong communication signals. This is the highest reported range for HDMI emanation in the literature. Fig. 1(c) shows the principle of CNN-based detection. Despite having a high accuracy and detection range, the CNN-based detection approach had some limitations. Firstly, it cannot differentiate between emanations from multiple sources. Additionally, the characteristics of emanations are dependent on the hardware, making it impractical to train a CNN on every possible type of hardware. Consequently, the CNN-based algorithm struggles with new or unfamiliar hardware. Furthermore, the accuracy decreases in low SNR conditions (maximum SNR  $< 3$  dB) because the fine details often get lost during the conversion from signal to image domain. Lastly, the CNN-based method is computationally intensive due to the complexity of the ResNet50 network, and converting each spectrum to the image domain requires extra computation for the same information content.

In this extended version, we augment our previous study by collecting and characterizing emanation data from a wide range of IoT devices (Arduino, PSoC, ESP32, and Zigbee), other commonly used electronic devices (PC and monitor), and cables (HDMI and USB). Analyzing the data, we find that: (1) the emanation signal consists of energy peaks in the frequency domain with harmonics and intermodulation products or IMP (also forms a harmonic pattern with much smaller frequency separation), (2) the fundamental frequency of the harmonics and frequency separation of intermodulation products (IMP) vary from device to device. While a harmonic detector is an obvious choice to detect the emanations with harmonic patterns, traditional harmonic detectors designed for power systems require apriori knowledge about the fundamental frequency to detect harmonics. Hence, they are infeasible here. Also, frequency separations for intermodulation products are

much smaller than fundamental frequency (=harmonic steps) and will require a second harmonic detector. In the field of audio/speech signal processing, there are many works on pitch (=fundamental frequency) estimation, but they do not detect all the other harmonic components. Also, they are not usable for intermodulation products.

Hence, in this work, we have developed a computational harmonic detection algorithm that doesn't require any apriori knowledge about the fundamental frequency, can detect IMPs simultaneously, and covers a wide range of harmonic patterns found in the experimental data such as regular harmonics, harmonics with one or more missing frequencies, different harmonic groups with 1 common frequency, overlapping IMPs from multiple sources with the same separation, etc. (later, Fig. 6 shows and section VI-A explains these cases in detail). More importantly, the proposed algorithm addresses the limitations of the CNN-based detection method. Fig. 1(d) shows the proposed harmonic-based emanation detection method and its advantages. This algorithm is hardware agnostic, can detect multiple emanation sources simultaneously, and can detect low SNR emanations ( $\sim 1$  dB). Since it works in the signal domain and there is no signal-to-image conversion and heavy CNN, it is computationally much more efficient. The computational harmonic-based emanation detection method provides  $\sim 100\%$  accuracy up to 22.5 m for HDMI emanation, compared to  $\sim 95\%$  accuracy achieved in earlier CNN-based methods. Also, it provides  $\sim 100\%$  accuracy for the IoT and electronic devices that we have experimented with. Fig. 2 shows our complete journey from the traditional threshold-based method (78.89%) to our initial CNN-based method (95%) and from CNN to our latest harmonic-based detection method ( $\sim 100\%$ ). This manuscript represents  $> 60\%$  work compared to the conference version [1], especially in the following aspects: (1) extensive emanation data collection from diverse devices, (2) analysis of those data to reveal device-dependent harmonic patterns with intermodulation products, and (3) development of a computational harmonic detection algorithm towards harmonic-based emanation detection method.

### B. Our Contribution

- In the preliminary study, using 3 types of HDMI cables (unshielded, single shielded, and double shielded) as target and Ettus B210 SDR as receiver, we have collected HDMI emanation data along with background profiling over 3 days from 0.5 m to 22.5 m in an office environment. **Harnessing the power of DSP techniques to improve the SNR and exploiting the advanced image recognition capability of modern CNN, we have improved the emanation detection range from 4 m to 22.5 m for an iso-accuracy of  $\sim 95\%$ . Also,  $\sim 100\%$  accuracy is achieved up to a distance of 16 m from the target.** Comparing the maximum emanation power from HDMI cables with 3 types of shielding, we have evaluated the efficacy of multi-layer shielding for commercially available cables. Also, we have distinguished emanation signals based on their screen content with an accuracy of  $\sim 91.7\%$  at 16 m.

- In this extended version, **we have collected and characterized emanation data from a wide range of IoT devices (Arduino, PSoC, ESP32, and Zigbee), electronic devices (PC and monitor), and cables (HDMI and USB cables).** Our analysis reveals that these emanations have distinct harmonic patterns with intermodulation products.
- Based on our study, **we have developed a computational harmonic detector that is device agnostic, requires no a priori information about the harmonic pattern, can detect low SNR ( $\sim 1$  dB) emanations, covers a wide variety of test cases, and works in the signal domain (unlike CNN-based method, it doesn't require transformation from signal to image).** It provides  $\sim 100\%$  accuracy up to 22.5 m in the office corridor, compared to  $\sim 95\%$  of the CNN-based method. It also achieves  $\sim 100\%$  detection accuracy for emanations from a wide range of electronic devices and cables.
- **The proposed algorithm has been tested in different environments (anechoic chamber, office building with both line-of-sight and non-line-of-sight cases) to ensure its efficacy in practical scenarios.**

### C. Organization of the Paper

The rest of the paper is structured as follows: section II discusses the relevant works published in the literature. Section III describes our experimental setup and measurement results. This includes both earlier data collection from HDMI for the conference version of this work and new data collection from IoT devices (Arduino, PSoC, Zigbee, and ESP32), other day-to-day electronics (PC, monitor), and cable (USB cable). In Section IV, the traditional threshold-based emanation detection method is explored. Section V describes our initially proposed CNN-based detection method in detail. It also analyzes the effect of multi-layer shielding to suppress emanation. Section VI explains the newly proposed harmonic-based emanation detection method. At the heart of this approach, there is a computational harmonic detection algorithm which has been described in detail with pseudocode. Section VII evaluates the performance of the harmonic-based detector, analyzes its device-agnostic detection feature, and compares it with other emanation detection methods proposed in the literature. Also, it is tested in different environments to show its efficacy in various deployment scenarios. Finally, section VIII concludes the paper with a summary.

## II. RELATED WORKS

Unintended electromagnetic leakage or emanation has long been exploited by defense agencies for eavesdropping. During World War II, Bell engineers accidentally noticed such leakage from a 131-B2 mixer that was provided to the Signal Corps by Bell Telephone [20]. With further investigation, the engineers succeeded in recovering 75% of the plain text of so-called encrypted data, proving the extent of the threat posed by such leakage. After that, emanation was studied by different agencies, leading to many policies and security protocols. The codename *TEMPEST* is used to refer to the classified US government program that studies the 'emission security'



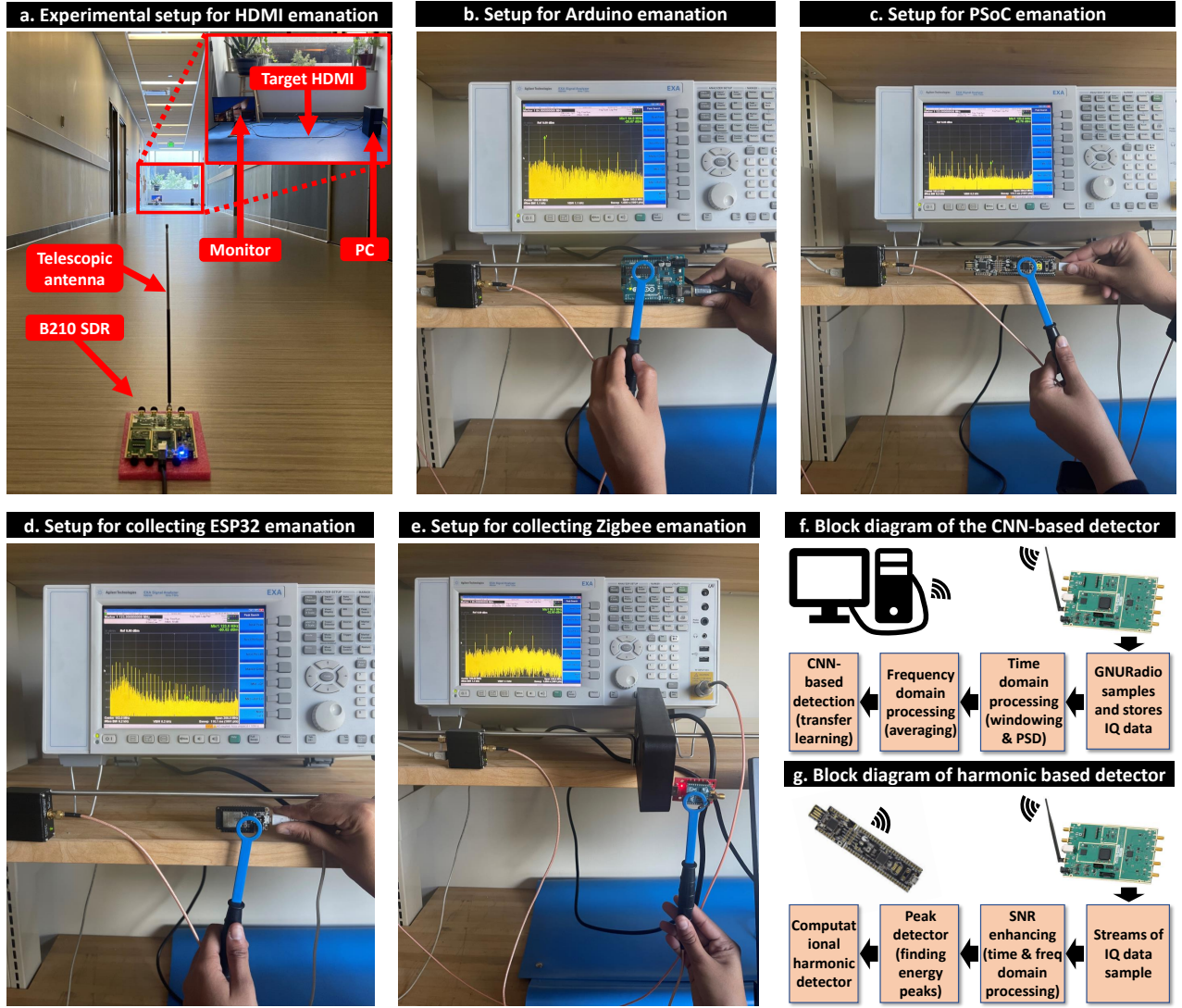


Fig. 3. (a) HDMI emanation data collection setup in the office corridor using Ettus B210 SDR (connected to a wideband telescopic antenna) as a receiver. The target HDMI is connected between a PC and a monitor (shown in inset). (b) (c) (d) (e) physical setup for emanation data collection from Arduino, PSoC, ESP32, and Zigbee respectively. Emanation is picked up using an H20 magnetic probe, amplified using a 40-dB wideband amplifier, and analyzed in a spectrum analyzer. (f) block diagram of the CNN-based emanation detection method that was proposed in the preliminary version of this work [1] (g) block diagram of the newly proposed harmonic-based emanation detection method (this work).

(EMSEC) issues, possible exploitation, countermeasures, and standardizations (e.g., NATO SDIP-27 Level A, Level B, etc.) [21]. Most information regarding TEMPEST is still classified. The first unclassified research work on EM side-channel emission was published by Wim van Eck in 1985 [22]. In a BBC program titled “Tomorrow’s World”, he demonstrated that the screen content can be successfully reconstructed at a long range using very cheap equipment. Electromagnetic emanations are sometimes called ‘van Eck radiation’ after him [21]. Repaired cables also show such emanation [23]. As mentioned in the introduction, electromagnetic emanation is mostly used for various data exfiltration purposes. However, it can also be used for defensive purposes as well. Authors in [24] have used EM emanation to fingerprint IoT devices. Human-induced EM emanation has been used for access control (touch to unlock) as well [25]. Authors in [26] have utilized such EM leakage to detect the presence of a rogue

device in a secure facility. Emanation signal from mobile devices has been proposed to be used for digital forensics [27]. Authors in [28] have used emanation signals to identify motherboard components to find suspicious ICs (probably counterfeited) on board.

The emanation spectrum varies with hardware (even for different programs being executed on the same device). However, a common feature in almost all of them is harmonic patterns and intermodulation products (IMP) forming upper and lower sidebands. So, harmonic detectors can be used to detect their presence. These detectors are widely studied in power systems where they are deployed in the active power filters to detect the harmonics on the power signal created by nonlinear loads and cancel them (by injecting signals with the same magnitude but opposite phase). There are harmonic detectors based on FFT [29]–[31], wavelets [32]–[35], space vector transformation [36], instantaneous reactive power [37],



TABLE I  
DESCRIPTION OF TARGET EQUIPMENT FOR EMANATION DATA COLLECTION

Equipment type	Target device/cable	Description
IoT Devices	Arduino	It's a microcontroller board used in many academic projects, robotics, home automation, low-cost scientific instruments, etc. Our specific board is Arduino Uno R3 with ATmega328P MCU [49].
	PSoC	It's a family of programmable embedded systems based on the ARM Cortex-M processor. PSoC is used in industrial automation, household appliances, medical devices, security systems, etc. Our specific model is 32-bit PSoC 5LP Arm Cortex-M3 [50] with CY8C58LP family SoC.
	Zigbee	These devices are used to create wireless mesh networks for building automation, lighting, smart city, medical, and asset tracking [51]. It is based on IEEE 802.15.4 specifications. Our specific model is Xbee S2C.
	ESP32	It is a series of low-cost, low-power microcontroller modules with Wi-Fi and Bluetooth connectivity. They are used for a wide range of applications including smart industrial devices, PLCs, smart medical devices, smart energy devices (HVAC, thermostats, etc.), wearable health monitors, etc. We use ESP32-DevKitC with ESP32-WROOM-32E module on board [52].
Other Electronic Devices	Desktop Computer	We have used a Dell OptiPlex PC with an Intel core™ i7-6700 processor and 8 GB of RAM (2400 MHz)
	Monitor	We have used a Dell P2319H monitor which is a 1080p 60Hz LED monitor.
Cables	USB Cable	USB cables are most commonly used to connect USB peripherals. We have used an unshielded USB cable.
	HDMI Cable	HDMI is the most common display cable nowadays [53]. In our preliminary version of this work [1], we used 3 types of HDMI 2.0 cables (shielded, single-shielded, and double-shielded).

[38], adaptive variational mode decomposition (AVMD) [39], ensemble empirical mode decomposition (EEMD) [40], neural networks [41], etc. A common observation on power system harmonic detectors is that the design and system parameters are selected according to the power grid and fundamental frequency (power supply frequency) which is known beforehand. This approach is not feasible for emanation detection as the fundamental frequency can be anywhere in the RF spectrum.

There are extensive studies in audio signal processing to estimate the pitch or fundamental frequency of speech or music [42]–[48]. However, these algorithms also have some assumptions stemming from speech and music signal properties. Also, they don't detect the full harmonic pattern. Hypothetically, it is possible to estimate the pitch using these audio processing algorithms and then use the power harmonic detectors to find the rest of the harmonics. But none of these are designed for the RF spectrum which is humongous (up to  $\sim 300$  GHz) compared to both audio spectra (usually limited to 20 kHz) and power spectra (50/60 Hz fundamental depending on the country, with harmonics within a few kHz range). A slight error in pitch estimation will lead to missing detection of several harmonics. Let's assume a pitch detector with a 2% error. So, a 100 MHz fundamental may be estimated as 98 MHz and the harmonic detector will try to find the 10<sup>th</sup> harmonic at 980 MHz, which is 20 MHz off. Considering the bandwidth of many SDRs, this harmonic may not even get detected at all. Finally, these approaches will not work for intermodulation products. To sum it up, a dedicated harmonic detector is required for electromagnetic emanation detection.

### III. DATA COLLECTION

#### A. Target Equipment

For emanation data collection, the target devices are chosen in such a way that a diverse set of electronic devices with various microcontrollers and system-on-chips (SoC) are included.

It is impossible to cover all types of leaking electronics, but with careful selection, the collected data can be representative of the majority of the electronic devices being used every day without the loss of generality. With that in mind, data were collected from 3 groups of devices (IoT, everyday electronics, and commonly used cables) which are described in Table I.

#### B. Experimental Setup

Fig. 3(a) shows our experimental setup for emanation data collection from an HDMI cable in an office corridor (the inset shows a zoomed-in view of the target HDMI). An Ettus B210 SDR connected with a wideband telescopic antenna is used as a receiver. A GNURadio interface collects the received data, samples at 4 MS/sec, and stores them. Fig. 3(b)–(e) shows our experimental setup for Arduino, PSoC, ESP32, and Zigbee respectively. Emanation signals are picked up by an EM probe (H20), amplified by a 40-dB wideband LNA, and fed to a spectrum analyzer.

Fig. 3(f) shows the block diagram of the CNN-based emanation detection method. Captured samples are processed in the time and frequency domain to improve SNR and converted to images (spectrum plots). These plots are then fed to a CNN to detect the emanation signal. Fig. 3(g) shows the block diagram of the newly proposed harmonic-based emanation detection method. Captured IQ data are processed to improve SNR. But then instead of converting to spectrum images, energy peaks are detected using a peak detector. The peaks are fed to our computational harmonic detector to find the harmonic group(s) and corresponding emanation signal(s), if any.

#### C. Measurement Results and Analysis

1) *Background Measurement:* For the CNN-based method (preliminary version of this work), HDMI emanation was considered as positive class, while RF background data (HDMI

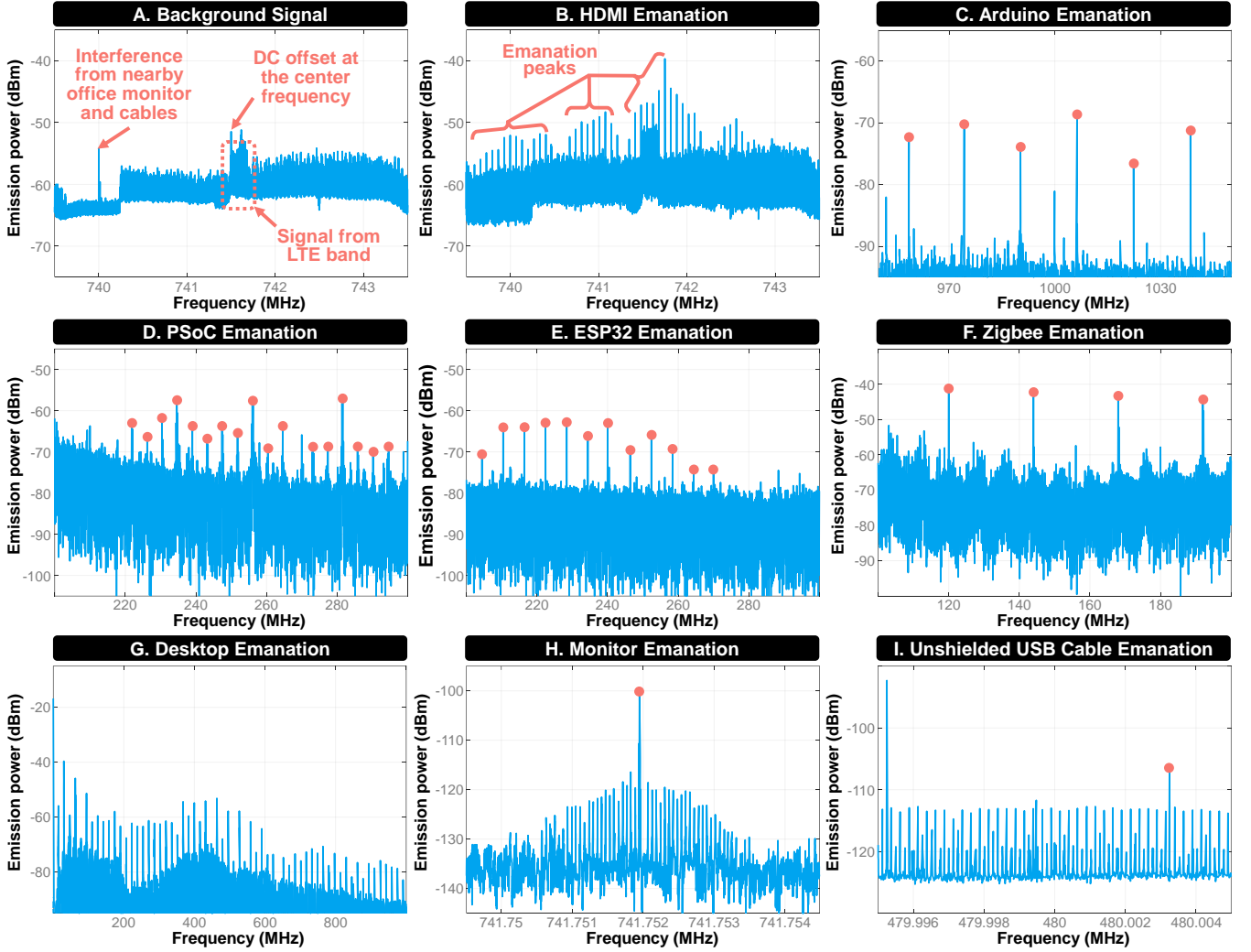


Fig. 4. (a) RF background signal (HDMI disconnected, PC and monitor off) shows the presence of DC offset, LTE band signal, and other interferer. (b)-(i) Unintended electromagnetic emission spectrum for HDMI, Arduino, PSoC, ESP32, ZigBee, Desktop, Monitor, and Unshielded USB cables respectively.

disconnected and there is no HDMI emanation) was labeled as negative class. To make the background profile robust, we collected background data on 3 separate days at 3 separate times: in the morning, at noon, and at night. Fig. 4(a) shows a sample background spectrum. We chose 742.5 MHz or the 5<sup>th</sup> harmonic as the target frequency where HDMI emanation was observed to be the strongest. Coincidentally, it overlaps with the LTE band (lower SMH block, from 729 MHz to 746 MHz). Fig. 4(a) clearly shows the LTE signal energy. Also, there are multiple experimental labs and office rooms on both sides of the corridor, contributing to some additional interference. Furthermore, the DC offset can be seen at the center. For the positive class, HDMI emanation data were collected from 0.5 m to 22.5 m, at 0.5 m intervals for 3 types of cables: unshielded, single-shielded, and double-shielded.

2) *Spectral Analysis*: Fig. 4(B)–(I) shows emission spectra from HDMI, Arduino, PSoC, ESP32, Zigbee, PC, monitor, and USB cables respectively. The key observation is that each device has its distinct electromagnetic leakage with unique harmonic patterns and sidebands (consisting of intermodulation products or IMP). These patterns can be utilized to identify

them uniquely. Table II lists the fundamental frequency and intermodulation product values for each device.

TABLE II  
HARMONIC AND IMP PATTERNS OF TEST DEVICES

Emanation source	Fundamental frequency (MHz)	IMP step (MHz)
HDMI	148.5	0.07
Arduino	16	many IMPs
PSoC	64	1.6
ESP32	6	0.525
ZigBee	24	3
Desktop	3.3	-
Monitor	148.5	0.07
USB	480	0.00025

#### IV. TRADITIONAL THRESHOLD-BASED DETECTION

##### A. Detection Method

Threshold-based peak detection is widely used in literature, including some recent ones [26]. The collected I-Q data are transformed into the frequency domain via FFT and compared

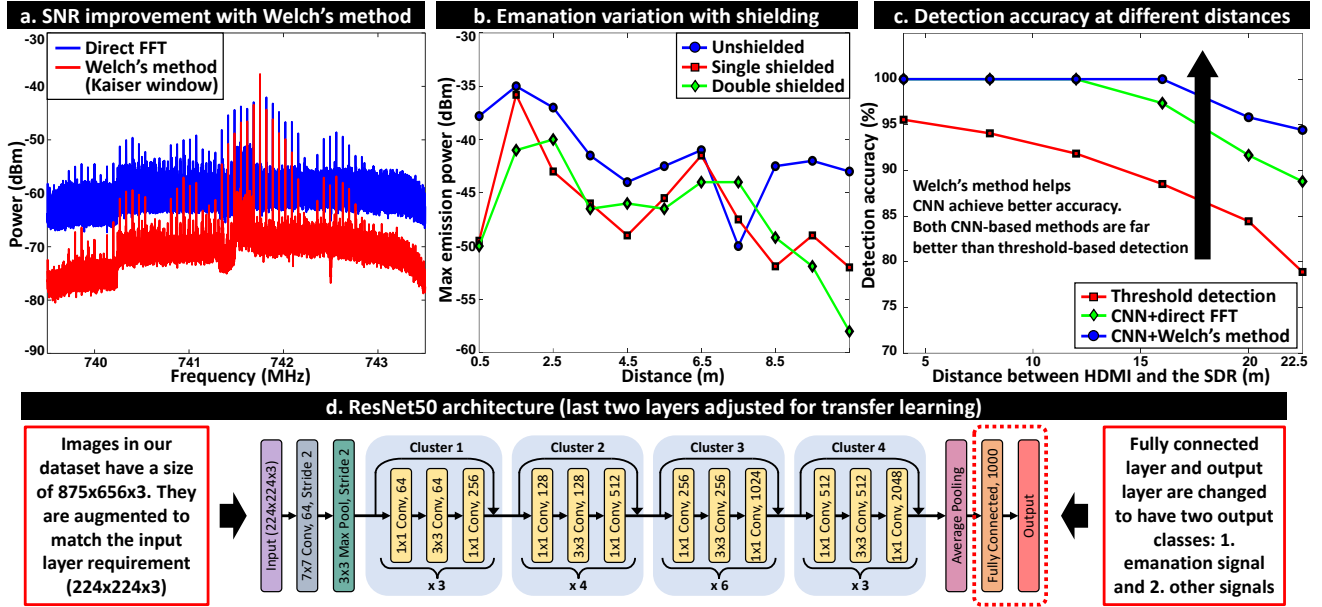


Fig. 5. (a) Using Welch's method of power spectrum estimation (along with Kaiser window), we get  $\sim 15$  dB SNR improvement. (b) Comparison of 3 types of HDMI (unshielded, single-shielded, and double-shielded) in terms of maximum emanation power. The unshielded cable is much louder in most cases while the difference between the other two is trivial. (c) Performance comparison between threshold-based detection (in the best case at  $-55$  dBm threshold) and CNN-based detection (both for direct FFT and Welch's method). SNR improvement provides a better detection range for iso-accuracy and a better accuracy for iso-distance than FFT from raw data. In both cases, the CNN-based method outperforms the threshold-based method by a high margin. (d) ResNet50 network which is used in the CNN-based method. Images in our dataset are augmented to match the input size ( $224 \times 224 \times 3$ ). The fully connected layer and the output layer are modified to classify two groups: emanation vs every other signal.

TABLE III  
PERFORMANCE ANALYSIS OF THRESHOLD-BASED DETECTION

Threshold (dBm)	FP (%)	FN (%)	Accuracy (%)
-45	0	74.07	62.96
-55	26.67	15.56	78.89
-65	100	0	50

against a threshold level. If there is a power peak above the threshold, we detect the presence of an emanation signal.

However, the accuracy is dependent on the threshold. If the threshold is too high, there will be a lot of false negative (FN) values, whereas too-low thresholds result in a lot of false positives (FP). We have tested the detection performance of our dataset for 3 threshold levels. Table III shows that the  $-55$  dBm threshold provides the best accuracy, which is still pretty low (78.89%).

### B. Challenges

Table III shows that threshold-based detection does not perform well (best-case accuracy  $< 80\%$ ). There are several reasons for that. The key issue is the strong interference from other signals (LTE signals, emanations from other cables, etc.). These peaks in the background are falsely detected as emanations for low thresholds, leading to high FP values. On the other hand, raising the threshold does not help much as emanation signals are weak and cannot cross the high threshold bar. This leads to high FN values. Also, the background noise level keeps changing based on the environment. This poses a challenge for adaptive threshold selection. Another

issue is the peak at the center frequency due to DC offset. To address these issues, we resort to CNN-based detection.

## V. CNN-BASED DETECTION

### A. SNR Improvement using DSP Techniques

Before training a CNN, we want to improve the perceived SNR of the collected signal. To that end, we apply some known techniques in the DSP domain.

1) *Windowing in Time Domain*: Our data is finite in the time domain, which is equivalent to applying a rectangular window to an infinite time sequence of data. However, the rectangular window has a significant spectral leakage from the main lobe to the side lobe [54]. There are better windows (Hanning, Hamming, Kaiser, etc.) with lower spectral leakage. The downside is the larger main lobe width. However, the main lobe width is inversely proportional to the data length and we have significantly long data to overcome this limitation. The spectral leakage for the Kaiser window ( $\beta = 5.66$ ) is only 0.01% compared to 9.28% for the rectangular window. Also, relative side-lobe attenuation reduces from  $-13.3$  dB to  $-41.4$  dB. We have windowed our data with the designed Kaiser window ( $\beta = 5.66$ ).

2) *Power Spectrum Estimation using Welch's Method*: We have used Welch's method of power spectrum estimation (modified periodogram with averaging) as a better spectrum estimate. A sequence of  $4 \times 10^5$  samples (0.1 s data) is taken and divided into 8 segments with 50% overlap. A modified periodogram (FFT of autocorrelation, instead of direct FFT) is applied to each segment and the output is averaged. Fig. 5(a) compares the spectrum of I-Q data corresponding to emanations from unshielded HDMI cable at 1 m distance, found



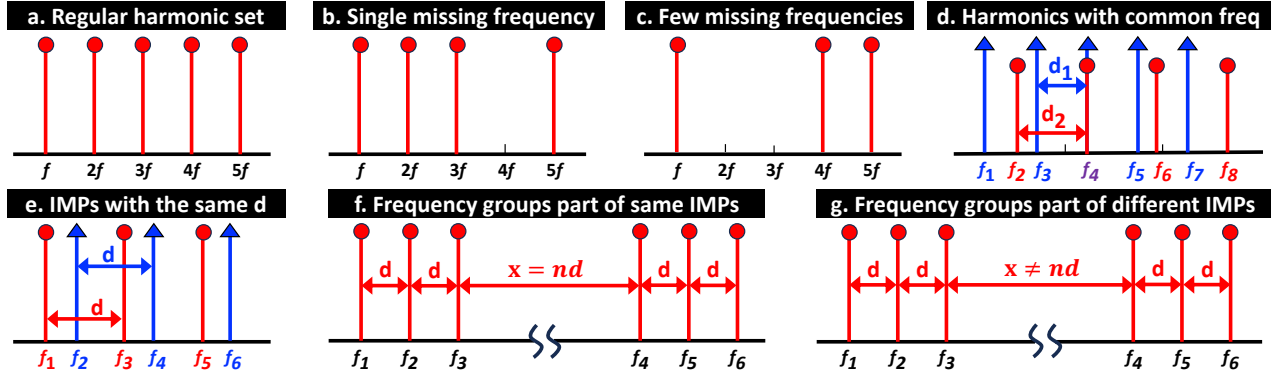


Fig. 6. (a) Regular harmonic frequencies with fundamental frequency  $f$ . (b) Missing single harmonic (here,  $4^{th}$  harmonic is missing). (c) Missing multiple harmonic frequencies (here,  $2^{nd}$  and  $3^{rd}$  harmonics are missing). (d) Two harmonic groups have a common frequency ( $f_4$ ) in them. (e),(f),(g) are more specific to IMPs only. (e) Two overlapping IMP groups with same frequency separation  $d$ . (f) Two separate IMP groups with same frequency separation  $d$ , but far away from each other (group separation  $x = nd$ , where  $n$  is large. Essentially, they are part of same IMP group. (g) Similar to the previous case, two separate IMP groups with same frequency separation  $d$ , but far away from each other. However, group separation  $x \neq nd$ , where  $n$  is large. Hence, they are two distinct IMP groups.

using direct FFT and Welch's method. It is shown that the maximum peak is similar for both, but the noise level is reduced. We gain  $\sim 15$  dB SNR improvement.

3) *Averaging in Frequency Domain*: Frequency domain averaging reduces noise power, keeping the signal peaks almost intact. We apply Welch's method for 9 consecutive sequences with 50% overlap in the time domain. The spectra of the sequences are averaged to reduce the noise power.

### B. Effect of Multi-Layer Shielding on Emanation

After improving the SNR, we want to check the efficacy of multi-layer shielding before moving on to training CNN. Fig. 5(b) shows the emanation power for 3 types of HDMI cables from 0.5 m to 10.5 m at 1 m intervals. Except for a few outliers, the maximum emanation power for the unshielded cable (blue line) is significantly higher than the other two, which is expected. However, the difference between the single and double-shielded cables is trivial.

### C. Transfer Learning using ResNet50

Our final step is to evaluate the performance of the CNN-based detection method. For that, we have used transfer learning approach where a widely used, pretrained CNN (e.g. VGG16 [55], AlexNet [56], GoogLeNet [57], ResNet50 [58], etc.) is retrained [59], [60] with a new dataset. These networks are carefully designed and reviewed by experts in the field and are known to classify images in standard datasets (e.g. ImageNet) with high accuracy. Our initial testing shows that ResNet50 works best for our case.

Residual Neural Network or ResNet revolutionized the use of the ultra-deep network by using 'skip connection' to address the issue of 'vanishing gradient' and 'degradation problem'. It performed much better compared to VGG or GoogLeNet on the 'ImageNet dataset' [61]. We will exploit the enhanced image classification capability of ResNet50 for our dataset. For training purposes, we have used the frequency domain plots as images. The rationale behind using the plots instead of the 1D sequence is to exploit the advanced image classification

capability of CNN (ResNet50). Our images are augmented to match the input size. The fully connected layer and the output layer are adjusted for binary classification (emanation vs others). The train, test, and validation data ratio was 70:20:10. We have used an initial learning rate = 0.001, mini-batch size = 8, and max epoch = 30. Data are shuffled at each epoch.

### D. Performance Evaluation

Fig. 5(c) shows the performance of ResNet50 via transfer learning for a distance of 4 m to 22.5 m. For data with better SNR (thanks to Welch's method), we get  $\sim 100\%$  accuracy up to 16 m which gradually reduces to  $\sim 95\%$  at 22.5 m. This figure also compares the performance benefit with improved SNR. Compared to direct FFT, we get a longer distance for iso-accuracy (e.g. for 100% accuracy, we get 16 m compared to 12 m) and higher accuracy for the same distance (e.g. at 22.5 m, we get  $\sim 95\%$  accuracy compared to  $\sim 88.9\%$ ). In both cases, the CNN-based method outperforms the threshold-based method by a high margin.

### E. Monitor Content Type Detection - Still vs Video

In the literature review section, we have discussed that some works have reconstructed screen images with plain text and some geometric shapes. Some recent works have tried to reconstruct video signals. However, these works assume that the monitor is running solely a video or just an image. An automated method is necessary to detect the content type of the monitor (still image vs video) and switch to the corresponding detection algorithm. In this subsection, we try to fill that void.

Our data collection method is the same as before, except that a video was playing on the monitor. The emanation signal captures the changes due to the video playback. We have used the same data processing steps before training ResNet50 with the data to check whether it can distinguish between the two. Our evaluation shows that we get 91.7% accuracy at a distance of 16 m which gradually drops at a further distance.



pixel values while keeping their original indices with them. To achieve this, a modified version of the well-known quicksort algorithm is implemented where the comparison is made based on 1<sup>st</sup> row values, but during binary grouping, the whole column is appended. Algorithm 1 shows this custom quicksort method.

In the experimental data, harmonic values are often not exact multiples of each other. Rather, the harmonics have slightly different frequencies than expected. To address this, a second helper function is defined which takes a tolerance limit and finds the group of values that differ within that tolerance range. Then it replaces the whole group with the average of it. Algorithm 2 shows the pseudocode of this function.

---

**Algorithm 1** Customized Quicksort Algorithm

---

```

1: function CUSTOM_QUICKSORT( $X$ )
2:    $r \leftarrow$  no of rows in  $X$ 
3:    $c \leftarrow$  no of columns in  $X$ 
4:   if  $c < 2$  then
5:     return  $X$ 
6:    $X1, X2 \leftarrow []$ 
7:   for  $n = 0, \dots, c - 2$  do
8:     if  $X[0][i] \leq X[0][c - 1]$  then
9:        $\text{append}(X1, X[:, i])$ 
10:    else
11:       $\text{append}(X2, X[:, i])$ 
12:   return  $\text{append}(\text{CUSTOM\_QUICKSORT}(X1),$ 
     $X[:, c - 1], \text{CUSTOM\_QUICKSORT}(X2))$ 

```

---



---

**Algorithm 2** Function to Fix Differences in Harmonic Steps

---

```

1: function FIX_FREQ_VAR( $D, D_{index}, \epsilon_{freq}$ )
2:    $i \leftarrow 0$ 
3:   while  $i < D_{index} - 1$  do
4:      $j \leftarrow i$ 
5:     while  $|D[0][i] - D[0][j + 1]| \leq \epsilon_{freq} \times D[0][j + 1]$ 
6:       do
7:          $j \leftarrow j + 1$ 
8:         if  $j == D_{index} - 1$  then break
9:         if  $j > i$  then
10:           $D[0][i : j + 1] \leftarrow \text{average}(D[0][i : j + 1])$ 
11:         $i \leftarrow j + 1$ 
12:   return  $D$ 

```

---

### E. Computational Harmonic Detector

Fig. 7(b) shows the logical flow diagram of the algorithm and Algorithm 3 shows its pseudocode. It works in the following steps:

**Step1:** A list of frequencies  $F = \{f_j \mid j = 1, 2, \dots, n\}$  is taken as the input. From this frequency list, differences between every possible pair of frequencies are calculated ( $d_{jk} = f_j - f_k \mid j, k = 1, 2, \dots, n$ ) to form a difference matrix  $D$ . However, such a matrix will be symmetric, with the principal diagonal being all '0'. Hence, for computational efficiency,  $d_{jk}$  is calculated only for  $j < k$ . The values are stored as a  $3 \times n$  array with differential values ( $d_{jk}$ ) in the first

row and the frequency indices ( $j, k$ ) in the second and third rows. Now, if there is only 1 column in the difference array, then there are no harmonics and the process is terminated. Otherwise, the algorithm moves on to the next step.

**Step2:** In this step, the helper functions that were developed before are used. First, the difference array is sorted using our custom quicksort function, keeping frequency indices tracked. Next, for the harmonic detection case (not IMP), the slight variation in difference values is fixed using our helper function.

**Step3:** Certain  $d_{jk}$  values are unique, while other values are multiples of these. Next, these unique difference values are found. For each unique value, its integer products are taken with it to form a product group. From each of these groups, one or more harmonic sets are found using the FIND\_HARMONICS function. But before calling that function, certain groups are ignored.

Assume 3 frequencies ( $f_1, f_2$ , and  $f_3$ ) with 2 difference values:  $d_{12} = d$  and  $d_{23} = Nd$ , where  $N \in \mathbb{Z}$ . However, there must be another differential value  $d_{13} = (N+1)d$  in the group. In other words, there cannot be only 2 values in the product group in practical scenarios. Groups with  $\leq 2$  elements are created numerically, while they cannot exist experimentally. Hence, such groups are discarded. Also, specifically for IMPs, there might be some groups with  $> 2$  elements while all of them are the same. Let's assume  $(N+1, N \in \mathbb{Z})$  IMP frequencies with  $N$  number of difference values, all being  $d$ . It's apparent that such  $N$  element group can not exist in reality as there must be at least another element with a differential value  $Nd$ . Hence, such groups are discarded.

**Step4:** For each group formed in the previous step, FIND\_HARMONICS function is called. Its pseudocode is given in Algorithm 4. For the first column of the group, a new harmonic list is formed with the 2 frequency indices of that column. For all other columns, if any (or both) of the frequency indices are already in an existing list, it's simply part of that harmonic or IMP group. If only one frequency index matches, the other frequency index is appended to that list. But what happens if none of the indices are part of any existing harmonic lists? That can never happen for harmonics because 2 harmonic groups with the same difference (=fundamental frequency) are basically the same harmonic group.

However, this condition may arise for IMPs with 2 possible scenarios as was described in Fig. 6(f) and Fig. 6(g). Firstly, if the difference between any frequency in one of the existing lists and the test frequency indices is a multiple of the fundamental step of that list, the 2 frequency indices of the test column are part of it (similar to Fig. 6(f)). So the test column's indices are appended to that list. However, if the difference is not a multiple of the fundamental step, the test column is part of a new IMP group as was shown in Fig. 6(g). So, a new harmonic list is formed with those two frequency indices. The loop keeps running till the last column of the group. In the end, it discards any harmonic list with only 2 frequency elements and returns the other harmonic lists. In the main harmonic detector function, harmonic lists returned by the FIND\_HARMONICS function (for each unique element group) are appended together to form a final harmonic or IMP list.



**Algorithm 3** Harmonic and Intermodulation Products Detection Algorithm

---

```

1: # Initializing variables and arrays
2:  $Freq\_list \leftarrow$  Frequencies where peaks are found
3:  $D_{min} \leftarrow$  Minimum difference
4:  $D_{max} \leftarrow$  Bandwidth/2
5:  $\epsilon_{freq} \leftarrow$  Tolerance for frequency variation

6: function DETECTOR( $Freq\_list, D_{min}, D_{max}, \epsilon_{freq}$ )
7:    $harmonic\_freqz \leftarrow \{ \}$  # Empty Python Dictionary
8:    $harmonic\_steps \leftarrow [ ]$ 
9:    $unique\_steps \leftarrow [ ]$ 
10:   $D \leftarrow [ ]$ 
11:   $n\_harmonic\_group, D_{index} \leftarrow 0$ 
12:  # Difference matrix D formation in a  $(3 \times n)$  array
13:  for  $i$  in  $range(len(Freq\_list))$  do
14:    for  $j$  in  $range(len(Freq\_list))$  do
15:       $difference = |Freq\_list(j) - Freq\_list(i)|$ 
16:      if  $i \geq j$  or  $difference < D_{min}$  or  $difference > D_{max}$  then
17:        continue
18:      else
19:         $append(D, [difference, i, j])$ 
20:         $D_{index} += 1$ 
21:  # If D has 1 column, return empty array and dictionary as there are no harmonics
22:  if  $D_{index} < 2$  then
23:    return  $harmonic\_steps, harmonic\_freqz$ 
24:  # Sorting difference matrix columns based on difference values (first row) from small to large
25:   $D \leftarrow CUSTOM\_QUICKSORT(D)$  # CUSTOM\_QUICKSORT() function is defined in algorithm 2
26:  if  $\sim flag\_subband$  then
27:     $D \leftarrow FIX\_FREQ\_VAR(D, D_{index}, \epsilon_{freq})$  # FIX\_FREQ\_VAR() function is defined in algorithm 3

28:  # Find harmonics or intermodulation products
29:  for  $i$  in  $range(len(D[0]))$  do
30:    if  $i == 0$  then
31:       $append(unique\_steps, D[0, 0])$ 
32:       $group \leftarrow D[:, (D[0] \% D[0][0]) == 0]$ 
33:    else if  $(D[0, i] \% unique\_steps) == 0$  then
34:       $append(unique\_steps, D[0, i])$ 
35:       $group \leftarrow D[:, (D[0] \% D[0][i]) == 0]$ 
36:    else
37:      continue
38:    if  $len(group) \leq 2$  then
39:      continue
40:    else if  $flag\_subband$  and  $len(set(group)) < 2$  then
41:      continue
42:    else
43:      # FIND_HARMONICS() function is defined in algorithm 4
44:       $temp\_harmonic \leftarrow FIND\_HARMONICS(group, Freq\_list)$ 
45:       $n\_temp\_harmonic \leftarrow len(temp\_harmonic)$ 
46:      if  $n\_temp\_harmonic == 0$  then continue
47:      else
48:         $append(harmonic\_steps, group[0][0] * n\_temp\_harmonic)$ 
49:        for  $(j = n\_harmonic\_group, \dots, n\_harmonic\_group + n\_temp\_harmonic)$  do
50:           $harmonic\_freqz[j] = sort(temp\_harmonic[j - n\_harmonic\_group])$ 
51:           $n\_harmonic\_group += n\_temp\_harmonic$ 
52:  return  $harmonic\_steps, harmonic\_freqz$ 

```

---

**Algorithm 4** FIND\_HARMONICS Function to Find IMPs of Same Differential Values and Harmonics

---

```

1: function FIND_HARMONICS(group, Freq_list)
2:   harmonic_subfreqz  $\leftarrow \{ \}$ 
3:   n_harmonic  $\leftarrow 0$ 
4:   FLAG = False
5:   for i in range(len(group[0])) do
6:     if i == 0 then
7:       harmonic_subfreqz[n_harmonic] = [group[1][0], group[2][0]]
8:       n_harmonic += 1
9:     else
10:      for j in range(n_harmonic) do
11:        flag_match_first  $\leftarrow$  (harmonic_subfreqz[j] == group[1][i])
12:        flag_match_second  $\leftarrow$  (harmonic_subfreqz[j] == group[2][i])
13:        if flag_match_first == True and flag_match_second == True then
14:          FLAG = True
15:          break
16:        else if flag_match_first == True and flag_match_second == False then
17:          FLAG = True
18:          append(harmonic_subfreqz[j], group[2][i])
19:          break
20:        else if flag_match_first == False and flag_match_second == True then
21:          FLAG = True
22:          append(harmonic_subfreqz[j], group[1][i])
23:          break
24:        else
25:          separation  $\leftarrow$  Freq_list[harmonic_subfreqz[j][-1]] - Freq_list[group[1][i]]
26:          if (separation % group[0][0]) == 0 then
27:            FLAG = True
28:            append(harmonic_subfreqz[j], [group[1][i], group[2][i]])
29:            break
30:          else
31:            continue
32:      if FLAG == True then
33:        FLAG = False
34:      else
35:        harmonic_subfreqz[n_harmonic] = [group[1][i], group[2][i]]
36:        n_harmonic += 1
37:   Final_Dict  $\leftarrow \{ \}$ 
38:   j  $\leftarrow 0$ 
39:   for i in range(n_harmonic) do
40:     if len(harmonic_subfreqz[i]) > 2 then
41:       Final_Dict[j] = harmonic_subfreqz[i]
42:       j += 1
43:     else
44:       continue
45:   return Final_Dict

```

---

## VII. RESULTS AND DISCUSSION

## A. Performance Evaluation of Harmonic-based Detector

Applying our harmonic-based emanation detection method, we achieve  $\sim 100\%$  accuracy for all the test devices. However, the distance up to which this accuracy is achieved varies from device to device. Hence, accuracy alone doesn't paint the full picture. Both the accuracy and the distance at which that accuracy is achieved are required for the complete performance evaluation. Table IV shows the maximum detection range up

to which  $\sim 100\%$  accuracy is achieved for various types of devices that we tested.

TABLE IV  
PERFORMANCE ANALYSIS OF THRESHOLD-BASED DETECTION

Device type	Maximum range (m)
IoT device (Arduino Uno)	5
Everyday electronics (desktop)	3
Cables (HDMI)	22.5

TABLE V  
COMPARISON OF UNINTENDED RF EMISSION DETECTION METHODS

Paper	Method	Target devices	Accuracy (%)	Detection range (m)	Environment(s)
Guardiola et al. [64]	Nonparametric method	Two-way talk radios	63.6	3	Unspecified
Hegarty et al. [65]	CNN	Arduino Uno	100	0.3	Lab
Vuagnoux et al. [66]	Short Time Fourier Transform (STFT)	PS2 Keyboard	95	20	Anechoic chamber, office, & residential building
Friedel et al. [67]	Simple Additive Weighting (SAW)	IED	86.1	0.2	Anechoic chamber
Liu et al. [68]	Correlation between external stimulus and spectral pattern change	Small camera (FLIR USB camera)	93.23	0.1	Lab
Alexander et al. [69]	Emanation Model Analytics (SVM-based)	Arduino Uno, Raspberry Pi B+, Teensy LC	100	0.3	RF Shield Box
Mo et al. [70]	Support Vector Machine (SVM)	LCD monitors	98.95	0.1	Semi-anechoic chamber
Hertenstein et al. [71]	Cross-correlation and Hurst parameter thresholding	RC toy car, wireless doorbell	97.6 (ROC)	0.25	Unspecified
Göksu et al. [72]	Wavelet Packet Analysis (WPA) and MLP	Cars	97	1 to 3	Lab
Acharya et al. [73]	Principal Component Analysis (PCA)	Two-way radios	Unspecified	3	Unspecified
Weng et al. [74]	Neural Network or Multilayer Perceptron (MLP)	RC toy truck, wireless doorbell	98.99 (Avg)	10	Anechoic chamber, office corridor
<b>This work</b>	<b>harmonic and IMP pattern-based detection</b>	<b>IoT devices, everyday electronics, and cables</b>	<b>100</b>	<b>22.5</b>	<b>Lab, office room, open space, &amp; anechoic chamber</b>

Applying our computational harmonic detector-based emanation detection method to our previously collected HDMI dataset (emanation from 3 types of HDMI cable in an office corridor [1]),  $\sim 100\%$  accuracy has been achieved up to 22.5 m range. If we compare this result with our earlier CNN-based method, for iso-accuracy of  $\sim 100\%$ , harmonic method has an extended detection range of 22.5 m, compared to 16 m for CNN approach. Also, for iso-distance of 22.5 m, harmonic method has a better detection accuracy ( $\sim 100\%$  vs  $\sim 95\%$ ). The following subsection compares our harmonic-based emanation detection method to other methods proposed in literature.

### B. Performance Comparison

Table V compares our work with other notable works for unintended electromagnetic emission detection. Before delving into a detailed discussion, two essential factors must be considered regarding this comparison. Firstly, older devices used to have much higher EM emanation than newer ones. For example, PS2 keyboards (used in [66]) had clock signals and often no shielding. So they used to have much higher emissions compared to modern USB keyboards that use differential signals (no clock) and shielding. Secondly, the primary goal of some of these works was not just to detect the emanation itself but to use it for other applications (covert communication [65], hidden camera detection [68], vehicle identification [72], etc.). Despite that, these works provide diverse insight towards emanation detection and are kept in this table.

The comparison is made in terms of 5 parameters: (1) detection method, (2) target devices, (3) accuracy, (4) maximum detection range, and (5) test environments. Several observations can be made from this table. Firstly, while other works focus on a specific type of device and a small test set,

we have covered a wide range of devices (eight devices in three categories). Since emanation properties are hardware-dependent, a generalized, device-agnostic method is advantageous over device-specific methods in practical scenarios. Secondly, we have one of the best accuracies (100%) reported among published works. While Hegarty et al. [65] and Alexander et al. [69] also achieved 100% accuracy, their detection range was very short, well below a meter (0.3 m). Combining accuracy and maximum detection range, our method clearly renders better performance than others. Finally, our method is rigorously tested in different environments (anechoic chamber, lab, office room, open space out of office room, etc.) where RF background profiles vary widely. The only work that was found to perform this level of testing was done by Vuagnoux et al. [66].

### C. Device Agnostic Detection

The properties of emanation signals are hardware-dependent. So, an EM emanation detection method developed for one type of device will not work with other types. This limits the deployment feasibility of such methods. Our previous CNN-based method was also limited to the device data with which it was trained. However, the harmonic-based method is more device-agnostic. It has been tested to achieve 100% accuracy for IoT devices (Arduino, PSoC, ESP32, and ZigBee), everyday electronics (desktop and monitor), and cables (HDMI and USB). Additionally, it has been tested for collected data from three other devices (RockPi 4 B+, webcam, and thumb drive) in our funding agency's testbed, where it also achieved  $\sim 100\%$  accuracy in emanation detection. So, it is of statistical significance to claim that our proposed harmonic-based emanation detection method is mostly device-agnostic.



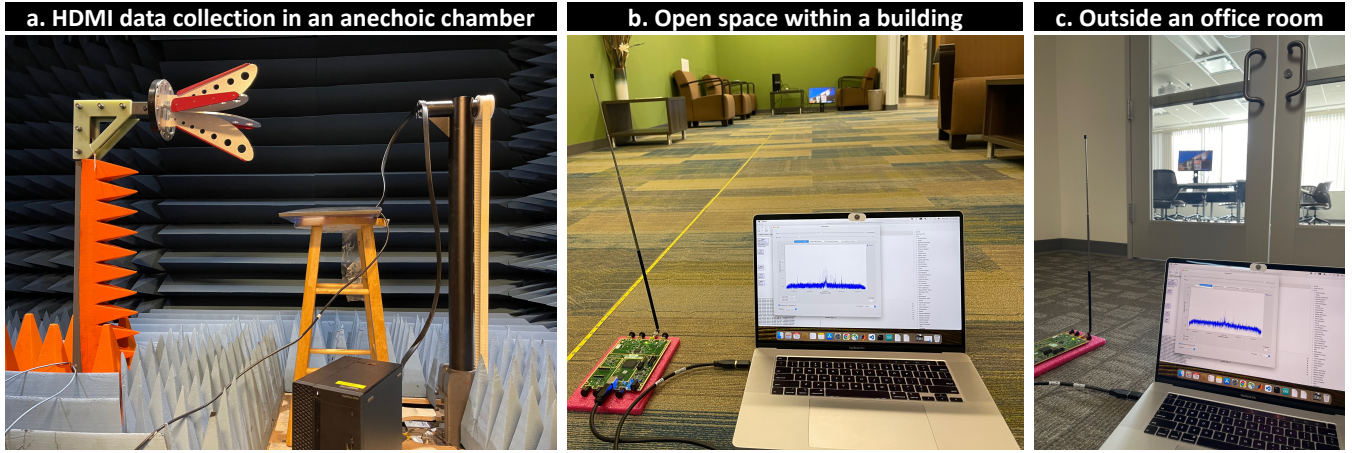


Fig. 8. To test the efficacy of the proposed algorithm in different environments, HDMI emanation data are being collected in (a) an anechoic chamber, (b) open space in a building (line-of-sight or LOS), and (c) outside of an office room (non-line-of-sight or NLOS).

#### D. Emanation Detection in Other Environments

Environmental variation is a crucial factor as noise and interference levels change significantly. Also, EM emanation couples with long metallic elements to travel further. The presence of such elements also varies with the environment. To test our algorithm in different environments, an HDMI cable is used as the target in 3 new environments (in addition to the previous lab setup), which are shown in Fig. 8.

- **An anechoic chamber:** The whole setup (both target HDMI and receiver B210) is placed within the chamber. Data are collected using an extended USB cable connecting the B210 SDR from inside to a capturing Macbook outside. The maximum data collection range in our anechoic chamber is  $\sim 5$  m.
- **An open space within a building (line-of-sight transmission):** EM emanation can couple with various conducting elements surrounding the emanation source and travel further. An open space has limited coupling elements. Hence, the emanation range in such an environment is more conservative than others. However, due to the room size, the maximum range for data collection in this environment is 11 m.
- **Outside of an office room (non-line-of-sight transmission):** Here, the target HDMI (with the monitor and PC) is kept inside an office room. The receiving antenna, along with B210 SDR, was kept outside to mimic practical eavesdropping scenarios. The target setup is kept 1.5 m away from the separating wall and door. Again, due to the building geometry, the outside data collection range was limited to 6 m. Hence, the total separation between the target and receiver is 7.5 m.

In all cases, our harmonic-based emanation detector renders  $\sim 100\%$  accuracy. This shows its robustness against environmental variability.

## VIII. CONCLUSION

In this work, we have extended our preliminary work on emanation detection by collecting data from a wide range of

carefully chosen IoT devices (Arduino, PSoC, Zigbee, and ESP32), day-to-day electronic devices (PC and monitor), and cables (HDMI and USB). Data analysis reveals that each device's emanation has a unique harmonic pattern with inter-modulation products, unlike communication signals with fixed frequency bands, distinct spectra, and modulation patterns. Leveraging this, we propose a harmonic-based emanation detection method by developing a computational harmonic detector. The proposed method addresses all the weaknesses of the previously proposed CNN-based method. It can detect multiple emanation sources simultaneously, performs well even at low SNR ( $\sim 1$  dB), has a lower computation cost, and is hardware-agnostic. This method provides  $\sim 100\%$  accuracy up to 22.5 m, compared to  $\sim 95\%$  accuracy at the same distance using the CNN-based method. It also achieves  $\sim 100\%$  accuracy for all the tested devices, including IoT devices. The maximum detection ranges for such accuracy are reported. Furthermore, the performance of our method is compared with other emanation detection methods reported in the literature in terms of 5 parameters. Finally, the proposed method has been tested in 3 new environments to check its practical efficacy: in an anechoic chamber, an open space (direct line-of-sight transmission), and outside of an office room (non-line-of-sight transmission). This work paves the way for a smart and automated spectrum monitoring system to detect EM side-channel leakage from electronic devices.

## ACKNOWLEDGMENTS

This research was supported by the Office of the Director of National Intelligence (ODNI), Intelligence Advanced Research Projects Activity (IARPA), via contract: 2021-21062400006. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the ODNI, IARPA, or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright annotation thereon.

## REFERENCES

- [1] M. F. Bari, M. R. Chowdhury and S. Sen, "Long Range Detection of Emanation from HDMI Cables Using CNN and Transfer Learning," 2023 Design, Automation & Test in Europe Conference & Exhibition (DATE), Antwerp, Belgium, 2023, pp. 1-6, doi: 10.23919/DATE56975.2023.10137263.
- [2] G. Camurati, S. Poeplau, M. Muench, T. Hayes, and A. Francillon, "Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers," in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2018, pp. 163–177, doi: 10.1145/3243734.3243802.
- [3] J. Danial, D. Das, A. Golder, S. Ghosh, A. Raychowdhury, and S. Sen, "EM-X-DL: Efficient Cross-device Deep Learning Side-channel Attack With Noisy EM Signatures," ACM Journal on Emerging Technologies in Computing Systems, vol. 18, no. 1, pp. 1–17, Jan. 2022, doi: <https://doi.org/10.1145/3465380>.
- [4] G. Haas and A. Aysu, "Apple vs. EMA: electromagnetic side channel attacks on apple CoreCrypto," In Proceedings of the 59th ACM/IEEE Design Automation Conference (DAC '22), Association for Computing Machinery, New York, NY, USA, 247–252. <https://doi.org/10.1145/3489517.3530437>
- [5] M. Vuagnoux, and S. Pasini, "Compromising electromagnetic emanations of wired and wireless keyboards," In USENIX security symposium, 2009, Vol. 8, pp. 1-16.
- [6] W. Jin, S. Murali, H. Zhu, and M. Li, "Periscope: A Keystroke Inference Attack Using Human Coupled Electromagnetic Emanations," Nov. 2021, doi: <https://doi.org/10.1145/3460120.3484549>.
- [7] B. Liu, Y. Xu, W. Huang and S. Guo, "Detecting USB Storage Device Behaviors by Exploiting Electromagnetic Emanations," ICC 2022 - IEEE International Conference on Communications, 2022, pp. 4980-4985, doi: 10.1109/ICC45855.2022.9839155.
- [8] S. Liang, Z. Zhan, F. Yao, L. Cheng and Z. Zhang, "Clairvoyance: Exploiting Far-field EM Emanations of GPU to "See" Your DNN Models through Obstacles at a Distance," 2022 IEEE Security and Privacy Workshops (SPW), 2022, pp. 312-322, doi: 10.1109/SPW54247.2022.9833894.
- [9] B. B. Yilmaz, E. M. Ugurlu, A. Zajić and M. Prvulovic, "Cell-Phone Classification: A Convolutional Neural Network Approach Exploiting Electromagnetic Emanations," ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2020, pp. 2862-2866, doi: 10.1109/ICASSP40776.2020.9054006.
- [10] M. R. Zunaiddi, A. Sayakkara, and M. Scanlon, "Revealing IoT Cryptographic Settings through Electromagnetic Side-Channel Analysis," Electronics, vol. 13, no. 8, p. 1579, Jan. 2024, doi: <https://doi.org/10.3390/electronics13081579>.
- [11] S. Sangodoyin et al., "Remote Monitoring and Propagation Modeling of EM Side-Channel Signals for IoT Device Security," Mar. 2020, doi: <https://doi.org/10.23919/eucap48036.2020.9135387>.
- [12] N. Sehatbakhsh, B. B. Yilmaz, A. Zajić and M. Prvulovic, "A New Side-Channel Vulnerability on Modern Computers by Exploiting Electromagnetic Emanations from the Power Management Unit," 2020 IEEE International Symposium on High Performance Computer Architecture (HPCA), San Diego, CA, USA, 2020, pp. 123-138, doi: 10.1109/HPCA47549.2020.00020.
- [13] M. F. Bari and S. Sen, "NoiseHopper: Emission Hopping Air-Gap Covert Side Channel with Lower Probability of Detection," 2024 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Tysons Corner, VA, USA, 2024, pp. 21-32, doi: 10.1109/HOST55342.2024.10545402.
- [14] H. S. Lee, D. H. Choi, K. Sim and J. -G. Yook, "Information Recovery Using Electromagnetic Emanations From Display Devices Under Realistic Environment," in IEEE Transactions on Electromagnetic Compatibility, vol. 61, no. 4, pp. 1098-1106, 2019, doi: 10.1109/TEMC.2018.2855448.
- [15] M. G. Kuhn, "Electromagnetic eavesdropping risks of flat-panel displays," in International Workshop on Privacy Enhancing Technologies, 2004, pp. 88-107. doi: [https://doi.org/10.1007/11545262\\_20](https://doi.org/10.1007/11545262_20)
- [16] M. G. Kuhn, "Compromising emanations of LCD TV sets," in IEEE Transactions on Electromagnetic Compatibility, 2013, 55, no. 3, pp 564-570. doi: 10.1109/TEMC.2013.2252353.
- [17] M. G. Kuhn, "Eavesdropping attacks on computer displays," in Information Security Summit, 2006, 24-25.
- [18] M. Carroll, "Connected IoT devices tipped to approach 19B in 2024," Mobile World Live, Sep. 03, 2024. <https://www.mobileworldlive.com/industry/connected-iot-devices-tipped-to-approach-19b-in-2024/#:~:text=IoT%20Analytics%20forecast%20the%20number> (accessed Sep. 04, 2024).
- [19] "SCISRS - Securing Compartmented Information with Smart Radio Systems," IARPA. [Online]. Available: <https://www.iarpa.gov/index.php/research-programs/scisrs>. (Accessed Sep. 04, 2024)
- [20] "TEMPEST," Cipharmachinesandcryptology.com, 2022. <https://www.cipharmachinesandcryptology.com/en/tempest.htm> (accessed Sep. 05, 2024).
- [21] "Tempest (codename)," Wikipedia. [https://en.wikipedia.org/wiki/Tempest\\_\(codename\)](https://en.wikipedia.org/wiki/Tempest_(codename)). (Accessed Jan. 25, 2023).
- [22] W. Van Eck, "Electromagnetic radiation from video display units: An eavesdropping risk?," Computers & Security 4, no. 4, 1985, 269-286.
- [23] M. F. Bari, M. R. Chowdhury and S. Sen, "Is Broken Cable Breaking Your Security?," 2023 IEEE International Symposium on Circuits and Systems (ISCAS), Monterey, CA, USA, 2023, pp. 1-5, doi: 10.1109/IS-CAS46773.2023.10181751.
- [24] J. Feng et al., "Fingerprinting IoT Devices Using Latent Physical Side-Channels," Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies, vol. 7, no. 2, pp. 1–26, Jun. 2023, doi: <https://doi.org/10.1145/3596247>.
- [25] Y. Liu, Z. Xu, Z. Qin, L. Ou and W. Jin, "TouchAccess: Unlock IoT Devices on Touching by Leveraging Human-Induced EM Emanations," in IEEE Transactions on Mobile Computing, doi: 10.1109/TMC.2024.3414992.
- [26] M. F. Bari, M. R. Chowdhury, B. Chatterjee and S. Sen, "Detection of Rogue Devices using Unintended Near and Far-field Emanations with Spectral and Temporal Signatures," 2022 IEEE/MTT-S International Microwave Symposium - IMS 2022, Denver, CO, USA, 2022, pp. 591-594, doi: 10.1109/IMS37962.2022.9865347.
- [27] A. P. Sayakkara and N. -A. Le-Khac, "Electromagnetic Side-Channel Analysis for IoT Forensics: Challenges, Framework, and Datasets," in IEEE Access, vol. 9, pp. 113585-113598, 2021, doi: 10.1109/ACCESS.2021.3104525.
- [28] E. J. Jorgensen, F. T. Werner, M. Prvulovic, and A. Zajić, "Deep Learning Classification of Motherboard Components by Leveraging EM Side-Channel Signals," Journal of Hardware and Systems Security, vol. 5, no. 2, pp. 114–126, Jun. 2021, doi: <https://doi.org/10.1007/s41635-021-00116-2>.
- [29] O. V. S. R. Varaprasad, D. V. S. S. Siva Sarma and R. K. Panda, "Advanced windowed interpolated FFT algorithms for harmonic analysis of electrical power system," 2014 Eighteenth National Power Systems Conference (NPSC), Guwahati, India, 2014, pp. 1-6, doi: 10.1109/NPSC.2014.7103877.
- [30] F. Zhang, Z. Geng and W. Yuan, "The algorithm of interpolating windowed FFT for harmonic analysis of electric power system," in IEEE Transactions on Power Delivery, vol. 16, no. 2, pp. 160-164, April 2001, doi: 10.1109/61.915476.
- [31] Q. Tang, Y. Wang and S. Guo, "Design of Power System Harmonic Measurement System Based on LabVIEW," 2008 Fourth International Conference on Natural Computation, Jinan, China, 2008, pp. 489-493, doi: 10.1109/ICNC.2008.230.
- [32] J. Barros and R. I. Diego, "Analysis of Harmonics in Power Systems Using the Wavelet-Packet Transform," in IEEE Transactions on Instrumentation and Measurement, vol. 57, no. 1, pp. 63-69, Jan. 2008, doi: 10.1109/TIM.2007.910101.
- [33] A. H. Ghaemi, H. A. Abyaneh and K. Mazlumi, "Harmonic indices assessment by wavelet transform," International Journal of Electrical Power & Energy Systems 33, no. 8 (2011): 1399-1409.
- [34] Y. Chen, "Harmonic Detection in Electric Power System Based on Wavelet Multi-resolution Analysis," 2008 International Conference on Computer Science and Software Engineering, Wuhan, China, 2008, pp. 1204-1207, doi: 10.1109/CSSE.2008.18.
- [35] S. Zhao, C. Wang and X. Bian, "Research on Harmonic Detection Based on Wavelet Threshold and FFT Algorithm," Systems Science & Control Engineering 6 (3): 339–45. doi:10.1080/21642583.2018.1558420.
- [36] L. Asiminoaei, F. Blaabjerg and S. Hansen, "Evaluation of harmonic detection methods for active power filter applications," Twentieth Annual IEEE Applied Power Electronics Conference and Exposition, 2005. APEC 2005., Austin, TX, USA, 2005, pp. 635-641 Vol. 1, doi: 10.1109/APEC.2005.1453014.
- [37] Y. Teng, C. Xiong, C. Li, Z. Zhang, Y. Zhou and D. Si, "Harmonic current detection based on the generalized instantaneous reactive power theory," 2015 IEEE International Conference on Progress in Informatics and Computing (PIC), Nanjing, China, 2015, pp. 468-471, doi: 10.1109/PIC.2015.7489891.
- [38] G. W. Chang and Tai-Chang Shee, "A comparative study of active power filter reference compensation approaches," IEEE Power Engineering Society Summer Meeting, Chicago, IL, USA, 2002, pp. 1017-1021 vol.2, doi: 10.1109/PESS.2002.1043556.

- [39] G. Cai, L. Wang, D. Yang, Z. Sun and B. Wang, "Harmonic Detection for Power Grids Using Adaptive Variational Mode Decomposition," *Energies* 12, no. 2: 232. <https://doi.org/10.3390/en12020232>
- [40] J. Shi and Z. Liu, "Harmonic Detection Technology for Power Grids Based on Adaptive Ensemble Empirical Mode Decomposition," in *IEEE Access*, vol. 9, pp. 21218-21226, 2021, doi: 10.1109/ACCESS.2021.3055553.
- [41] H. C. Lin, "Intelligent Neural Network-Based Fast Power System Harmonic Detection," in *IEEE Transactions on Industrial Electronics*, vol. 54, no. 1, pp. 43-52, Feb. 2007, doi: 10.1109/TIE.2006.888685.
- [42] R. J. McAulay and T. F. Quatieri, "Pitch estimation and voicing detection based on a sinusoidal speech model," *International Conference on Acoustics, Speech, and Signal Processing*, Albuquerque, NM, USA, 1990, pp. 249-252 vol.1, doi: 10.1109/ICASSP.1990.115585.
- [43] D. Wang, C. Yu and J. H. L. Hansen, "Robust Harmonic Features for Classification-Based Pitch Estimation," in *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, vol. 25, no. 5, pp. 952-964, May 2017, doi: 10.1109/TASLP.2017.2667879.
- [44] S. Karimian-Azari, N. Mohammadiha, J. R. Jensen and M. G. Christensen, "Pitch estimation and tracking with harmonic emphasis on the acoustic spectrum," 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), South Brisbane, QLD, Australia, 2015, pp. 4330-4334, doi: 10.1109/ICASSP.2015.7178788.
- [45] E. Azarov, M. Vashkevich and A. Petrovsky, "Instantaneous pitch estimation based on RAPT framework," 2012 Proceedings of the 20th European Signal Processing Conference (EUSIPCO), Bucharest, Romania, 2012, pp. 2787-2791.
- [46] E. Vincent, N. Bertin and R. Badeau, "Adaptive Harmonic Spectral Decomposition for Multiple Pitch Estimation," in *IEEE Transactions on Audio, Speech, and Language Processing*, vol. 18, no. 3, pp. 528-537, March 2010, doi: 10.1109/TASL.2009.2034186.
- [47] S. Godsill and M. Davy, "Bayesian harmonic models for musical pitch estimation and analysis," 2002 IEEE International Conference on Acoustics, Speech, and Signal Processing, Orlando, FL, USA, 2002, pp. II-1769-II-1772, doi: 10.1109/ICASSP.2002.5744965.
- [48] T. Abe, T. Kobayashi and S. Imai, "Robust pitch estimation with harmonics enhancement in noisy environments based on instantaneous frequency," *Proceeding of Fourth International Conference on Spoken Language Processing*, ICSLP '96, Philadelphia, PA, USA, 1996, pp. 1277-1280 vol.2, doi: 10.1109/ICSLP.1996.607843.
- [49] ARDUINO, "Arduino Uno Rev3," Arduino Official Store, 2021. <https://store.arduino.cc/products/arduino-uno-rev3> (accessed Sep. 05, 2024).
- [50] Infineon Technologies AG, "32-bit PSocTM 5 LP Arm® Cortex®-M3 - Infineon Technologies," Infineon.com, 2024. <https://www.infineon.com/cms/en/product/microcontroller/32-bit-psoc-arm-cortex-microcontroller/32-bit-psoc-5-lp-arm-cortex-m3/> (accessed Sep. 05, 2024).
- [51] Wikipedia Contributors, "Zigbee," Wikipedia, Apr. 05, 2019. <https://en.wikipedia.org/wiki/Zigbee> (accessed Sep. 05, 2024).
- [52] Espressif, "ESP32 Overview — Espressif Systems," [www.espressif.com](http://www.espressif.com), 2023. <https://www.espressif.com/en/products/socs/esp32>
- [53] L. Knerl, "What are the most popular computer monitor cable types?," HP.com. <https://www.hp.com/us-en/shop/tech-takes/most-popular-computer-cable-types> (accessed Sep. 05, 2024).
- [54] J. G. Proakis and D. G. Manolakis, "Digital Signal Processing: Principles, algorithms, and applications," 3rd ed. Upper Saddle River, NJ: Pearson Prentice Hall, 2007.
- [55] K. Simonyan, and Z. Andrew, "Very deep convolutional networks for large-scale image recognition," in *arXiv preprint*, 2014, arXiv:1409.1556.
- [56] A. Krizhevsky, S. Ilya, and H.E. Geoffrey, "Imagenet classification with deep convolutional neural networks," in *Communications of the ACM*, 2012, 60(6), 84-90.
- [57] C. Szegedy, et al. "Going deeper with convolutions." *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2015, pp. 1-9, doi: 10.1109/CVPR.2015.7298594.
- [58] K. He, X. Zhang, S. Ren and J. Sun, "Deep Residual Learning for Image Recognition," in *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016, pp. 770-778, doi: 10.1109/CVPR.2016.90.
- [59] "Transfer learning," Wikipedia, 22-Jul-2022. [Online]. Available: [https://en.wikipedia.org/wiki/Transfer\\_learning](https://en.wikipedia.org/wiki/Transfer_learning). (Accessed Sep. 05, 2024).
- [60] L. Torrey and S. Jude, "Transfer learning," in *Handbook of research on machine learning applications and trends: algorithms, methods, and techniques*, IGI global, 2010, pp. 242-264.
- [61] I. Rajagopal, "Intuition behind residual neural networks," Medium, 22-Jul-2020. [Online]. Available: <https://towardsdatascience.com/intuition-behind-residual-neural-networks-fa5d2996b2c7>. (Accessed Jan. 25, 2023).
- [62] P. Du, W. A. Kibbe, and S. M. Lin, "Improved peak detection in mass spectrum by incorporating continuous wavelet transform-based pattern matching," *Bioinformatics*, vol. 22, no. 17, pp. 2059-2065, Jul. 2006, doi: <https://doi.org/10.1093/bioinformatics/btl355>.
- [63] "scipy.signal.find\_peaks\_cwt — SciPy v1.7.1 Manual," [docs.scipy.org. https://docs.scipy.org/doc/scipy/reference/generated/scipy.signal.find\\_peaks\\_cwt.html](https://docs.scipy.org/doc/scipy/reference/generated/scipy.signal.find_peaks_cwt.html) (Accessed Sep. 05, 2024).
- [64] I. G. Guardiola and F. Mallor, "A Nonparametric Method for Detecting Unintended Electromagnetic Emissions," in *IEEE Transactions on Electromagnetic Compatibility*, vol. 55, no. 1, pp. 58-65, Feb. 2013, doi: 10.1109/TEM.2012.2203602.
- [65] M. Hegarty, Y. E. Sagduyu, Tugba Erpek, and Y. Shi, "Deep Learning for Spectrum Awareness and Covert Communications via Unintended RF Emanations," pp. 27-32, May 2022, doi: <https://doi.org/10.1145/3522783.3529531>.
- [66] M. Vuagnoux and S. Pasini, "An improved technique to discover compromising electromagnetic emanations," 2010 IEEE International Symposium on Electromagnetic Compatibility, Fort Lauderdale, FL, USA, 2010, pp. 121-126, doi: 10.1109/ISEMC.2010.5711257.
- [67] J. E. Friedel, T. H. Holzer and S. Sarkani, "Development, Optimization, and Validation of Unintended Radiated Emissions Processing System for Threat Identification," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 6, pp. 2208-2219, June 2020, doi: 10.1109/TSMC.2018.2810305.
- [68] Z. Liu et al., "CamRadar: Hidden Camera Detection Leveraging Amplitude-modulated Sensor Images Embedded in Electromagnetic Emanations," *Proceedings of the ACM on Interactive Mobile Wearable and Ubiquitous Technologies*, vol. 6, no. 4, pp. 1-25, Dec. 2022, doi: <https://doi.org/10.1145/3569505>.
- [69] S. Alexander et al., "CASPER: an efficient approach to detect anomalous code execution from unintended electronic device emissions," *Proc. SPIE 10630, Cyber Sensing 2018*, 106300V, pp. 32-32, May 2018, doi: <https://doi.org/10.1117/12.2500234>.
- [70] F. Mo, Y.-H. Lu, J.-L. Zhang, Q. Cui, and S. Qiu, "A support vector machine for identification of monitors based on their unintended electromagnetic emanation," *Progress In Electromagnetics Research M*, vol. 30, pp. 211-224, Jan. 2013, doi: <https://doi.org/10.2528/PIERM12122406>.
- [71] J. Hertenstein and S. Jagannathan, "Detection of unintended electromagnetic emissions from super-regenerative receivers," *Proceedings of SPIE, the International Society for Optical Engineering/Proceedings of SPIE*, vol. 8017, pp. 80170F80170F, May 2011, doi: <https://doi.org/10.1117/12.883223>.
- [72] H. Göksu, D. C. Wunsch, X. Dong, A. Kökce and D. G. Beetner, "Detection and Identification of Vehicles Based on Their Spark-Free Unintended Electromagnetic Emissions," in *IEEE Transactions on Electromagnetic Compatibility*, vol. 60, no. 5, pp. 1594-1597, Oct. 2018, doi: 10.1109/TEM.2017.2773706.
- [73] S. P. Acharya and I. G. Guardiola, "Detection of RF devices based on their unintended electromagnetic emissions using Principal Components Analysis," 2013 Wireless Telecommunications Symposium (WTS), Phoenix, AZ, USA, 2013, pp. 1-5, doi: 10.1109/WTS.2013.6566247.
- [74] H. Weng, X. Dong, X. Hu, D. G. Beetner, T. Hubing and D. Wunsch, "Neural network detection and identification of electronic devices based on their unintended emissions," 2005 International Symposium on Electromagnetic Compatibility, 2005. EMC 2005., Chicago, IL, USA, 2005, pp. 245-249 Vol. 1, doi: 10.1109/ISEMC.2005.1513508.





**Md Faizul Bari** received his Ph.D. from the Elmore Family School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN, USA in 2024. He completed his B.Sc. and M.Sc. in Electrical and Electronic Engineering from Bangladesh University of Engineering and Technology, Dhaka, in 2017 and 2020, respectively. He worked as a Design Engineer at Neural Semiconductor Limited, Dhaka, for more than a year. Later, he joined the University of Asia Pacific, Dhaka, as a lecturer and worked there for almost a year before coming to the USA to pursue his doctoral studies. He was a Research Scientist Intern at Intel in the Summer of 2020 and an Embedded Security Applications Intern at Analog Devices in the Summer of 2024.

Dr. Bari is a recipient of the Computer and Information Systems Fellowship (CISE) and the Magoon Award for Excellence in Teaching. His works were nominated for best paper awards in the 2024 IEEE HOST conference and the 2019 IEEE NANO conference. His research interests include hardware security, AI-assisted system design, radio frequency machine learning systems, etc.



**Meghna Roy Chowdhury** (Student Member, IEEE) received her B.Tech. degree in Electronics and Communication Engineering from Vellore Institute of Technology, India, in 2020. She is currently pursuing a Ph.D. degree in Electrical and Computer Engineering at Purdue University, West Lafayette, USA. Her research interests include low-power wearable technologies, machine learning for healthcare applications, and system-level integration of AI for embedded and edge computing.



**Shreyas Sen** is an Elmore Associate Professor of ECE & BME, Purdue University. His current research interests span mixed-signal circuits/systems and electromagnetics for the Internet of Bodies (IoB) and Hardware Security. He has authored/co-authored 3 book chapters, over 200 journal and conference paper and has 25 patents granted/pending. Dr. Sen serves as the Director of the Center for Internet of Bodies (C-IoB) at Purdue. Dr. Sen is the inventor of the Electro-Quasistatic Human Body Communication (EQS-HBC), or Body as a Wire technology,

for which, he is the recipient of the MIT Technology Review top-10 Indian Inventor Worldwide under 35 (MIT TR35 India) Award in 2018 and Georgia Tech 40 Under 40 Award in 2022. To commercialize this invention Dr. Sen founded Ixana and serves as the Chairman and CTO and led Ixana to awards such as 2x CES Innovation Award 2024, EE Times Silicon 100, Indiana Startup of the Year Mira Award 2023. His work has been covered by 250+ news releases worldwide, invited appearance on TEDx Indianapolis, NASDAQ live Trade Talks at CES 2023, Indian National Television CNBC TV18 Young Turks Program, NPR subsidiary Lakeshore Public Radio and the CyberWire podcast. Dr. Sen is a recipient of the NSF CAREER Award 2020, AFOSR Young Investigator Award 2016, NSF CISE CRII Award 2017, Intel Outstanding Researcher Award 2020, Google Faculty Research Award 2017, Purdue CoE Early Career Research Award 2021, Intel Labs Quality Award 2012 for industrywide impact on USB-C type, Intel Ph.D. Fellowship 2010, IEEE Microwave Fellowship 2008, GSRC Margarida Jacome Best Research Award 2007, and nine best paper awards including IEEE CICC 2019, 2021 and in IEEE HOST 2017-2020, for four consecutive years. Dr. Sen's work was chosen as one of the top-10 papers in the Hardware Security field (TopPicks 2019). He serves/has served as an Associate Editor for IEEE Solid-State Circuits Letters (SSC-L), Nature Scientific Reports, Frontiers in Electronics, IEEE Design & Test, Executive Committee member of IEEE Central Indiana Section and Technical Program Committee member of TPC member of ISSCC, CICC, DAC, CCS, IMS, DATE, ISLPED, ICCAD, ITC, and VLSI Design. Dr. Sen is a Senior Member of IEEE.