Accuracy Enhancement of Electromagnetic Side-Channel Attacks on Computer Monitors

Asanka Sayakkara
Forensics & Security Research Group
School of Computer Science
University College Dublin
Ireland
asanka.sayakkara@ucdconnect.ie

Nhien-An Le-Khac
Forensics & Security Research Group
School of Computer Science
University College Dublin
Ireland
an.lekhac@ucd.ie

Mark Scanlon
Forensics & Security Research Group
School of Computer Science
University College Dublin
Ireland
mark.scanlon@ucd.ie

ABSTRACT

Electromagnetic noise emitted from running computer displays modulates information about the picture frames being displayed on screen. Attacks have been demonstrated on eavesdropping computer displays by utilising these emissions as a side-channel vector. The accuracy of reconstructing a screen image depends on the emission sampling rate and bandwidth of the attackers signal acquisition hardware. The cost of radio frequency acquisition hardware increases with increased supported frequency range and bandwidth. A number of enthusiast-level, affordable software defined radio equipment solutions are currently available facilitating a number of radio-focused attacks at a more reasonable price point. This work investigates three accuracy influencing factors, other than the sample rate and bandwidth, namely noise removal, image blending, and image quality adjustments, that affect the accuracy of monitor image reconstruction through electromagnetic side-channel attacks.

CCS CONCEPTS

• **Security and privacy → Side-channel analysis and countermeasures**; *Hardware attacks and countermeasures*;

KEYWORDS

Electromagnetic Side-Channels, Unintentional Hardware Emissions, Software Defined Radio, Eavesdropping

ACM Reference format:
Asanka Sayakkara, Nhien-An Le-Khac, and Mark Scanlon. 2018. Accuracy Enhancement of Electromagnetic Side-Channel Attacks on Computer Monitors. In *Proceedings of International Conference on Availability, Reliability and Security, Hamburg, Germany, August 27–30, 2018 (ARES 2018),* 9 pages.
https://doi.org/10.1145/3230833.3234690

ARES 2018, August 27–30, 2018, Hamburg, Germany

ACM ISBN 978-1-4503-6448-5/18/08…$15.00
https://doi.org/10.1145/3230833.3234690

1 INTRODUCTION

It has been shown that electromagnetic (EM) emissions from computing devices can be used as a side-channel by third parties for eavesdropping on these devices' activities. The information-leaking EM emissions can occur from components including the CPU, data bus lines, network controllers, and video displays [12]. Depending on the EM source, the information that can be revealed by third parties greatly varies. For example, the CPU executing a segment of instructions which handles data in registers and RAM can modulate information about the individual program instructions and variable values into the EM emission. Meanwhile, data bus lines and network drivers emit EM signals which can hint about the memory contents and the network data. Similarly, EM emissions from video displays can reveal the contents shown on screen [15].

The risk of remote eavesdropping on video displays using their EM emissions was first highlighted in 1985 by Van Eck [13]. Later works have shown that the threat still prevails in modern computer displays that employ various technologies to transmit video information from the system unit to the display such as VGA, DVI and HDMI [5, 7]. While the principles of reconstructing display images are similar across eavesdropping techniques, the accuracy and the clarity of the image highly depends on the sampling rate and bandwidth of the EM signal acquisition hardware. Existing techniques for computer display eavesdropping in the literature succeeds in constructing the displayed image with a significant accuracy by relying on high sample rates and bandwidth provided by specialised radio frequency (RF) signal acquisition hardware. Such specialised equipment can be prohibitively expensive for many information security professionals.

While the sample rate and bandwidth of the signal acquisition hardware have an obvious affect on the image reconstruction accuracy, it is important to investigate any other factors, which may help to improve the process. In order to enable low-cost RF signal acquisition hardware to be used, it is necessary to identify these extra factors and their influence. This work explores several potential avenues that can be utilised to improve the image reconstruction accuracy of electromagnetic side-channel attacks on video displays when the RF signal acquisition hardware does not provide ideal conditions.

The contributions of this paper can be summarised as follows:

- Evaluation of several approaches to increase the reconstructed image quality and the discussion of their respective pros and cons. The approaches evaluated include (1) noise reduction of RF signals, (2) changing properties of the reconstructed

images such as brightness and contrast, and (3) blending multiple reconstructed images together.
- Discussion on the challenges associated with image quality enhancement with limited sampling rates, such as image frame misalignments and outlier detection.
- Discussion on the possible directions for future improvements of EM side-channel attacks on computer monitors.

In this paper, Section 2 provides the background of EM side-channel analysis. Section 3 provides an overview of the experimental methodology followed. Finally, Section 4 explains the results of the empirical study, and the conclusions and avenues for future work are highlighted in Section 5.

2 RELATED WORK

2.1 Side-Channel Attacks

The topic of side-channel attacks spans a wide variety of techniques. Each side-channel attack on a computer system focuses on a specific unintentional emission of either hardware or software. The amount of memory and cache spaces shared between different software, the time a program takes to respond to different inputs, the sounds different components of computer hardware make, the amount of electricity a computer system draws, and the EM radiation a computer hardware emits are examples of such side-channels [12].

It has been shown that acoustic emanations from various components and peripherals of computer systems can be used to exfiltrate information [9]. Genkin et al. showed that it is possible to distinguish between CPU operations by listening to acoustic emanations resulting in an attack on the encryption key of the RSA algorithm [3].

2.2 Unintentional Electromagnetic Emissions

EM radiation is the underlying technology for numerous of wireless communication. The EM radiation used in each communication technology is chosen based on the distance that needs to be covered, the data throughput rate desired, the frequency of the signal, the amount of bandwidth required, the data modulation technique, and how powerful the transmitted signal need be [6]. WiFi, Bluetooth, cellular network technologies, e.g., GSM or CDMA, and terrestrial/satellite television networks are examples of such technologies that each employ their own specification of EM radiation.

While the devices being used for wireless communication purposes are designed to generate EM radiation on the frequency and amplitude appropriate for the communication technology, these devices also generate EM radiation on unintended frequencies as a side effect of their internal operations [4]. Such unintended EM radiation are regulated by government agencies, such as the *Federal Communications Commission* (FCC) in the USA, due to the possible interference they can make on legitimate wireless communication on those frequencies and the potential health issues they can cause to the users of these devices. Even though consumer devices, such as mobile phones and computers, are under these unintentional EM emission regulations, it is not possible to entirely avoid such emissions, but the equipment manufacturers attempt to minimise it as much as possible [11].

Unintentional EM emissions of a computer can be generated from various parts of the system. The nature of these EM signals and the kind of side-channel information they carry depends on the source of each of the EM signals. Throughout the rest of this section, how EM signals are generated from the video display of a computer, what kind of information they may carry, and what types of methods and tools can be used to capture these signals are discussed.

2.3 Computer Monitor Electromagnetic Emissions

The risk of remote eavesdropping attacks on video displays was pointed out first by Van Eck more than three decades ago [13]. It was revealed that a modified television set can be used to capture and visualise video streams being displayed on a nearby television screen. The technique requires suitably modified hardware available to the attacker, which poses a limitation to the possibility of executing such an attack. The video displays used in computing uses different protocols to transmit video data to the monitor that require more flexibility than dedicated hardware based attack.

Improving the video display eavesdropping concept, Kuhn provides a comprehensive analysis on EM side-channel eavesdropping on modern video display technologies [7]. This work uses RF acquisition hardware with fast sampling rates, such as $500MHz$, to monitor EM emissions from computer displays to show that eavesdropping risk persists in modern computer video displays. Moreover, his work demonstrates the possibility of intentionally modulating data into the EM emissions of a monitor by displaying carefully designed content on-screen. This possibility opens up opportunities for a new generation of malware which can leak information through the EM emissions of a monitor. The behaviour of the malware may not be suspicious unless the EM emission signal patterns are correlated with the contents placed on the screen by the malware. Furthermore, Kuhn's work demonstrates that readable text can be extracted from various types of computer screens by averaging adjacent frames together.

Elibol et al. presented a monitor eavesdropping system which uses a RF acquisition hardware for reconstructing screen images remotely [2]. The hardware for signal acquisition is a portable platform which supports a huge RF frequency range. Similar to the approach used by Kuhn, this work uses the averaging of adjacent frames to improve the readability of the text.

Hayashi shows that EM emissions from mobile device video displays also leaks information [5]. While acknowledging the fact that EM side-channel attacks on computer displays are an emerging threat, it was pointed out that such attacks require sophisticated hardware that is not commonly available for professionals outside military and government establishments. Furthermore, it is highlighted that standards and regulations of electromagnetic compatibility (EMC) in consumer products have been updated in recent years to accommodate the emerging threat from eavesdropping attacks using EM side-channels. For example, ITU-T advisory notice K.84[1] introduced by the International Organisation for Standardisation (ISO)/IEC) states that it is necessary to consider information leakage from EM emissions when considering the EMC requirements of consumer devices.

[1] https://www.itu.int/rec/T-REC-K.84/en

The most significant contributing factor to the accuracy of the display's image reconstruction is the sampling rate of the RF acquisition hardware. While oscilloscopes and other hardware supports extremely fast sampling rates, such devices are not commonly available for many information security specialists. In contrast, software defined radios (SDR) provide increased flexibility for lower costs, but do provide a lower sampling rate compared to dedicated RF acquisition hardware. *TempestSDR* is an open-source software library that facilitates the use of SDR platforms for EM side-channel attacks on computer displays [8]. The library is capable of automatically detecting the dimensions and frame rate of a target when the target monitor details are unknown. This is achieved by identifying the repeating patterns in the EM signal that correspond to the individual frames of the video. While the *TempestSDR* library facilitates screen image reconstruction, the results show that sampling rate is the limiting factor in SDR-based EM side-channel eavesdropping. The readable text can be extracted from a target screen only when the sampling rate is extremely high and the screen resolution is low enough to have a lower pixel frequency. This situation demands for further studies on enhancing the text readability of eavesdropped screens.

3 METHODOLOGY

In order to explore the factors that affect the accuracy of eavesdropped computer displays, multiple experiments were conducted using an SDR-based platform. This section explains the details of how EM emissions leak information from computer monitors and the technique of reconstructing the screen by observing EM signals. Accordingly, the experimental setup was designed to evaluate those aspects.

3.1 Nature of Electromagnetic Emissions

A computer monitor consists of a collection of pixels arranged in multiple rows across the display. These monitors display images by regularly updating the intensity of pixels in a sequence. Each pixel on a colour display is represented as three colour spots; red, blue, and green (RGB). The pixels are refreshed in an order which starts at the left corner of the uppermost row and proceeds along each horizontal line left to right, top to bottom. The information to update the intensity of each pixel is transmitted through the video cable that connects the computer to the monitor. In an analogue video cable, each pixel intensity is modulated as an amplitude value in the video signal. In digital video cables, the pixel intensity is represented as a binary value that consists of multiple bits. Furthermore, in order to separate the picture frames from each other, a blank in the video signal is used.

When video information is transmitted through the cable to the monitor, both the video controller of the computer and the monitor must stay synchronised in order to precisely interpret which intensity value signalled corresponds to which pixel on the monitor. While this is being done, the associated components of video information processing and transmission causes the EM signals to radiate. It has been shown that the fundamental frequency component of a computer monitor EM emission is equal to the rate of pixel information being transmitted through the cable. Therefore, this frequency is called *pixel frequency*, F_p, which can be calculated

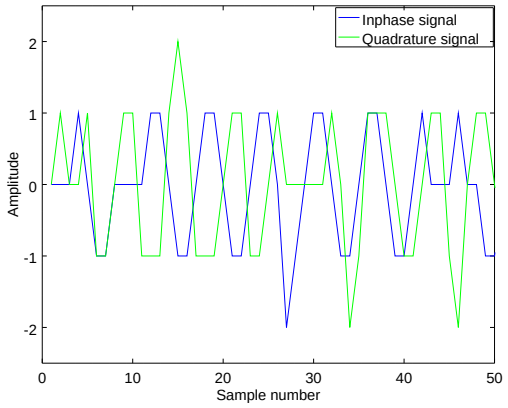

Figure 1: Data samples acquired from a *HackRF* software defined radio.

easily using the number of pixels per horizontal line, W_p, number of pixel lines, H_p, and the frame rate, or frames per second (FPS) as shown in Equation 1. Though *FPS* can slightly vary over time, it can be assumed to be a constant in order to roughly calculate EM emission frequency of a particular monitor.

$$F_p = W_p \times H_p \times FPS \tag{1}$$

As it is evident from the manner that pixel frequency is calculated, displays with smaller dimensions have a lower EM emission frequency compared to displays with larger dimensions. Furthermore, while the fundamental emission frequency of a computer monitor is at the pixel frequency, it is possible to observe multiple strong harmonics of the same signal at higher frequencies. This phenomenon can pose two advantages to an attacker. Firstly, when the fundamental EM emission frequency falls at a noisy area in the RF spectrum (making it more difficult to reconstruct the target monitor screen), the attacker has the ability to tune into a higher harmonic of the EM signal that may reside in a quieter area of the RF spectrum. Secondly, capturing the EM signal at multiple harmonics separately and combining the information at the end may lead to more accurate reconstruction of the target screen.

3.2 Capturing Electromagnetic Emissions

Perhaps the simplest approach to capturing the EM emissions from a computer monitor would be to have an analogue AM radio receiver tuned to the pixel frequency of the target. However, due to the large variety of computer monitors available with different dimensions and frame rates, it is not possible to ensure that the EM emission frequency of a target monitor will fall within the tuneable frequency range of the radio receiver. This limitation leads to the requirement of employing general purpose RF signal acquisition hardware, such as oscilloscopes with RF probes, to acquire and digitise the EM emission signal.

Software defined radios (SDRs) have recently emerged as the weapon of choice for wireless hackers. The most primitive SDR

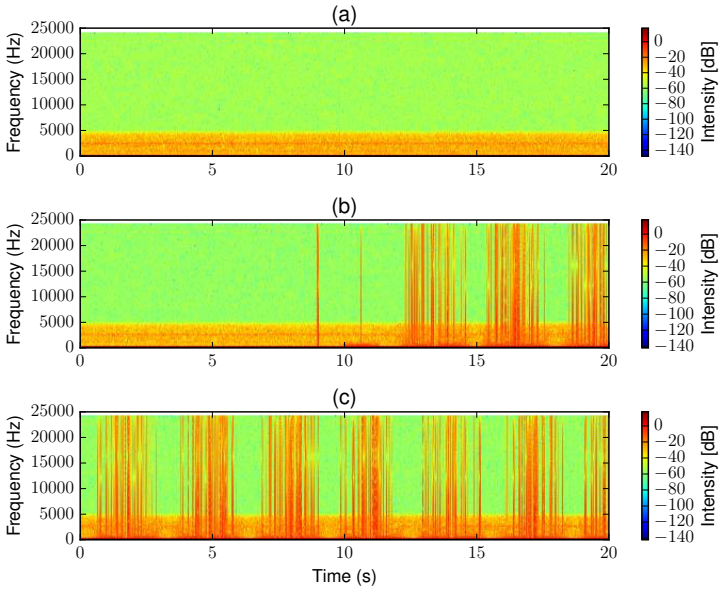

Figure 2: Spectrograms of AM demodulated EM emissions acquired from an Arduino device that were captured while (a) a program was running, (b) being reprogrammed to run a different program, and (c) running the new program.

devices available in the market are hacked TV tuners called RTL-SDRs. These provide a reasonable sample rate of approximately $2MHz$ and a tuneable frequency range within the sub-GHz range to operate for a price tag of ~$10. On the other end of the spectrum lies the expensive and powerful SDR platforms, such as the universal software radio peripheral (USRP) with extensible modules supporting a large range of sample rates and tuneable frequencies.

The composition of an SDR platform can be divided into two parts; the hardware layer and the software layer. The hardware layer is an RF front-end that is composed of an RF amplifier and a fast analogue-to-digital converter (ADC). The duty of the RF front-end is to convert the analogue RF signal into digitised samples in a rapid phase that can be processed by the software layer. Each digitised sample produced by the RF front-end is a complex number in the I/Q data format, where the real value represents *In-phase* component of the signal while the imaginary value represents the *Quadrature* component of the EM signal. Figure 1 illustrates a set of I/Q data samples acquired using the *HackRF* SDR platform [10]. It produces I/Q data with 8-bit signed integers for each component in a complex number.

A simple set-up can be used to demonstrate the unintentional EM signals that can be observed using an SDR platform. An *Arduino Leonardo* prototyping board is loaded with a simple program to blink an LED connected to it via the general purpose I/O pins. An antenna connected to an RTL-SDR dongle is placed close to the Arduino board in order to receive unintentional EM signals emitted from the board. The Arduino board consists of a microcontroller chip that operates at 16 MHz. However, the RTL-SDR dongle cannot tune to frequencies below 22 MHz and therefore a GNURadio script was programmed to tune the RTL-SDR dongle to the first harmonic of the Arduino clock, i.e., 32 MHz. Figure 2 illustrates the spectrograms of three different EM signal samples gathered. When two different LED blinking patterns are performed by two different programs separately, the Arduino emitted two completely different EM signal patterns as can be seen from the spectrograms shown in Figure 2 (a) and Figure 2 (c). The transition from executing first program to the second program is visible in the spectrogram in Figure 2 (b).

3.3 Evaluation Plan

When attempting to enhance the EM side-channel based eavesdropping attacks to computer monitors using a SDR, it is necessary to consider the limit for the sampling rate. Considering the capability and price tags of the SDR devices in the market and the capability of tools used in previous works by Kuhn [7], Elibol [2] and Hayashi [5], it is considered reasonable to set the sampling rate threshold to $20MHz$ for the EM signal acquisition task. Within that hardware limit, the following three aspects were evaluated to identify their impact on the reconstructed images by eavesdropping on computer monitors:

- The impact from using narrow-band signals for image reconstruction instead of wide-bands.
- The impact of image quality (e.g., brightness, contrast) to the identifiability of the text on eavesdropped screens.
- The impact of blending multiple images together to enhance the clarity of the reconstructed image.

In order to measure the accuracy of the reconstructed images, an automatic similarity detection metric was used. The *Structural Similarity Index Measure* (SSIM) measures the similarity of the original screen to the reconstructed screen [14]. It returns a value

Figure 3: Hardware components of an EM eavesdropping attack on a computer monitor.

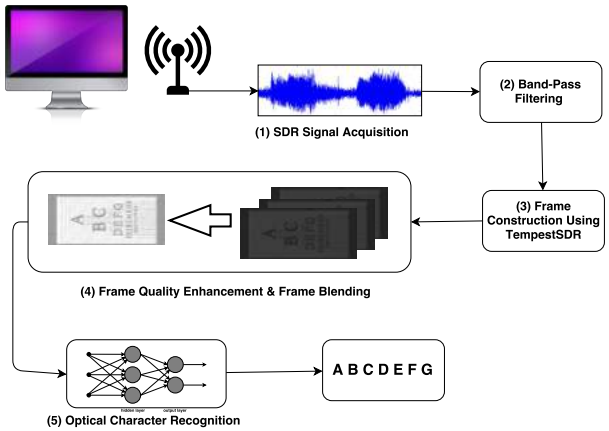

Figure 4: The steps to acquire EM signals, filter EM data, construct display image, feed to the machine learning model, and to classify the screen contents.

of 1 for exactly similar images and 0 for completely different images. Any intermediate value indicates the similarity of the two images.

3.4 Experimental Setup

In order to evaluate the parameters listed in the evaluation plan, an experimental setup was designed and implemented accordingly. In this setup, different data processing components were implemented in a modular fashion with configurable settings. RF signal preprocessing and reconstructed screen image post-processing functionality may be necessary for an effective eavesdropping attack in a real-world scenarios. However, for the sake of ease of debugging and monitoring the complete process, the setup used in the experiments was designed to run offline, where each individual processing state operates on its own data files and produces log files.

Throughout the experiments, a monitor manufactured by *Samsung* was used as the target device. The operating system of the target computer was configured to drive the monitor with a pixel width of 1784 and height of 798 while the frame rate was running approximately at 60 per second. Therefore, the pixel clock frequency of the target device was observed as an EM emission at approximately $85.25Hz$. As this fundamental frequency of the EM emission lies in a busy range of the radio spectrum, where FM radio transmissions take place, a harmonic of the signal was used for the eavesdropping attacks which was observed at approximately $346.5MHz$.

In the experimental setup, a *HackRF* SDR hardware is used as the RF signal acquisition device. It provides a sample rate up to $20MHz$, which is the preferred upper limit of the data sampling rate in these experiments. The SDR device is connected to the attackers computer over a USB port and a small antenna connected to the SDR device is placed closer to the monitor of the target computer, as can be seen in Figure 3. In order to feed I/Q data streams into the experimental setup, a utility program was used, *hackrf_transfer*, which is distrobuted with the default *HackRF* tools for the *Linux* platform. The two built-in amplifiers were required to be set to fixed values throughout the experiments in order maintain the internal settings of the SDR device consistent. Setting amplifier values too high causes the noise floor to increase, while setting them too low results in the EM signal going undetected in both cases affecting the signal-to-noise ratio (SNR) required for a successful signal reception. Therefore, suitable values to resolve this issue were decided by trial-and-error. The low-noise amplifier (LNA) was set to $24dB$ while the base-band variable gain amplifier (BB-VGA) was set to $20dB$.

Figure 4 illustrates the data processing stages of the experimental setup in detail. Step (1) handles the configuration settings of the SDR hardware and produces a steam of I/Q data samples that is passed onto the next stage. Even when the EM signal harmonic to be tuned to is carefully selected, it is not possible to completely avoid unnecessary RF signals from getting into the data samples. This is due to the $20MHz$ bandwidth of *HackRF* device in which the interested EM signal lies only in a smaller fraction of that spectrum. Therefore, in order to extract only a selected region of the acquired signal spectrum, a band-pass filter is applied as Step (2), which outputs a new I/Q data stream with attenuated signals except the region of interest.

For the purpose of reconstructing screen images using the I/Q data of an EM emission, this work uses *TempestSDR* library [8] at Step (3) of the experimental setup. This library produces a stream of image files at a configurable rate by locking into the frame rate and the pixel line changing frequency. It is possible for the library to automatically detect the dimensions and frame rate of a target monitor, our setup provides the details of the target monitor to the library. This is to prevent the impact from erroneous detection of target monitor details by the library, which results in unusable screen images.

The stream of the screen images produced at Step (3) are passed to image post-processing at Step (4). Multiple activities were performed at this stage to meet the evaluation plan. Adjustments are applied to two image quality parameters, *brightness* and *contrast*, in a sequence and the SSIM index was calculated between the quality enhanced images and a screenshot from the original target computer screen. The purpose of the use of SSIM metric is two fold. As the image quality parameters are adjusted to find the best setting, a huge number of resulting images are produced, which are nearly impossible to be manually inspected to find the most quality output. The SSIM index makes it possible to automate the inspection process by assigning a number to the similarity. The other aspect is the subjective nature of human observation. Instead of relying on

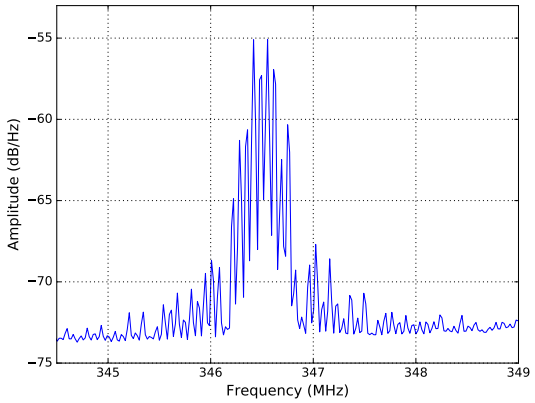

Figure 5: Power spectral density (PSD) of an EM emission signal from a computer monitor. The peak signal is available at $346.5MHz$ which is a harmonic of the pixel frequency of the target monitor.

visual judgement for the clarity of an image, SSIM helps for objective comparison to identify how successful an image enhancement setting was.

Step (4) attempts to further enhance the reconstructed image by blending adjacent screen images together. The success of image blending depends on two factors of the image reconstruction process. If the contents of the target monitor changes rapidly, such as displaying a video, the adjacent reconstructed images will have different content that are unsuitable for merging. However, in this experimental setup, a static screen content was used in each signal acquisition trial, which facilitates adjacent image blending for any selected number of images. Meanwhile, the reconstructed images produced at Step (3) may have slight misalignment, which causes the blended images to be distorted and lose information. This issue was dealt with by manually removing misaligned images from the dataset in between Step (3) and (4). However, an automated way to fix the misalignment issue by either removing misaligned images or by realigning them based on common features as markers is desirable in a practical use case.

As the final stage, selected sets of reconstructed screen images are planned to be passed to an OCR at Step (5). The objective is to see the identifiability of characters shown on screen before and after applying the enhancements. The reconstructed images with an *eye chart* as the target monitor content can be used in the the OCR based tests, while the *checkerboard* target was used only at the earlier stages for SSIM value based comparisons. The OCR-based detection phase was not evaluated for the purpose of this paper.

4 RESULTS AND DISCUSSION

Figure 5 illustrates the EM emission of the target monitor which was captured using the SDR device and sent through a band-pass filter. The information regarding the pixel intensities are modulated to the amplitude of the signal, which is centred at approximately $346.5MHz$. However, there are tiny peaks distributed in both sides of the strong signal that may carry amplitude modulated pixel intensity information, These are important to successfully reconstruct the target screen. In this section, the results of evaluation parameters are presented.

4.1 Impact from Band-Pass Filtering

There is an inherent relationship between the *sampling rate* and the *bandwidth* of SDR tools, which causes an issue when using higher sample rates. For example, when the *HackRF* is configured to sample data at a rate of $20MHz$, it produces 20 million samples per second, while capturing a width of $20MHz$ around the centre frequency it is tuned to. This means, if the device is tuned to $343MHz$ for the centre frequency, it captures a $20MHz$ wide spectrum which includes signal frequencies from $333MHz$ to $353MHz$. Furthermore, there is always a peak at the centre frequency, which is called *DC Spike*, caused by the internal noise of the SDR device that should be avoided. When the interested EM emission signal of the target monitor is at $346.5MHz$, tuning the SDR device to $343MHz$ helps to avoid the DC spike from falling on top of the EM emission signal. However, the direct use of the captured spectrum for image reconstruction may include unnecessary signals including the DC spike and various other external RF sources. A Butterworth band-pass filter is used to extract the interested region of EM signal from the captured signal spectrum [1].

Figure 6 illustrates the reconstructed screen images with and without band-pass filtering the EM data. As evident from the images, filtering has smoothed the pixels from the reconstructed image in contrast to the unfiltered approach where external noise has contributed to the distortion of the details. The SSIM index comparison with the original screen content indicates that filtered image is indeed more similar to the original content than the unfiltered version. The SSIM index of the filtered EM data based image is 0.46, while the unfiltered EM data based image has 0.01.

4.2 Impact from Image Quality Adjustment

The reconstructed images were updated to have different brightness and contrast settings that varied between 0 and 255 for 8-bit greyscale images used as the inputs. Due to the large number of possible combinations available, it was designed to increase the brightness/contrast value in 10 point steps. The resulting images were compared to the original screen content by calculating the SSIM index for each image with a unique brightness/contrast setting.

Figure 9 illustrates how the SSIM index of the resulting images were changed along with brightness/contrast variations. It is evident that the SSIM index of the reconstructed images improves with an increase in brightness. However, after the brightness level above 130, the SSIM index gets stabilised indicating that it does not contribute further to make the reconstructed image more similar to the original screen. Meanwhile, contrast variation had a negligible impact to the SSIM index, while even slight brightness variations affected the SSIM output drastically up to the brightness level of 130.

4.3 Impact from Image Blending

As the target computer monitor displayed static content throughout the time period of EM signal acquisition, each of the images

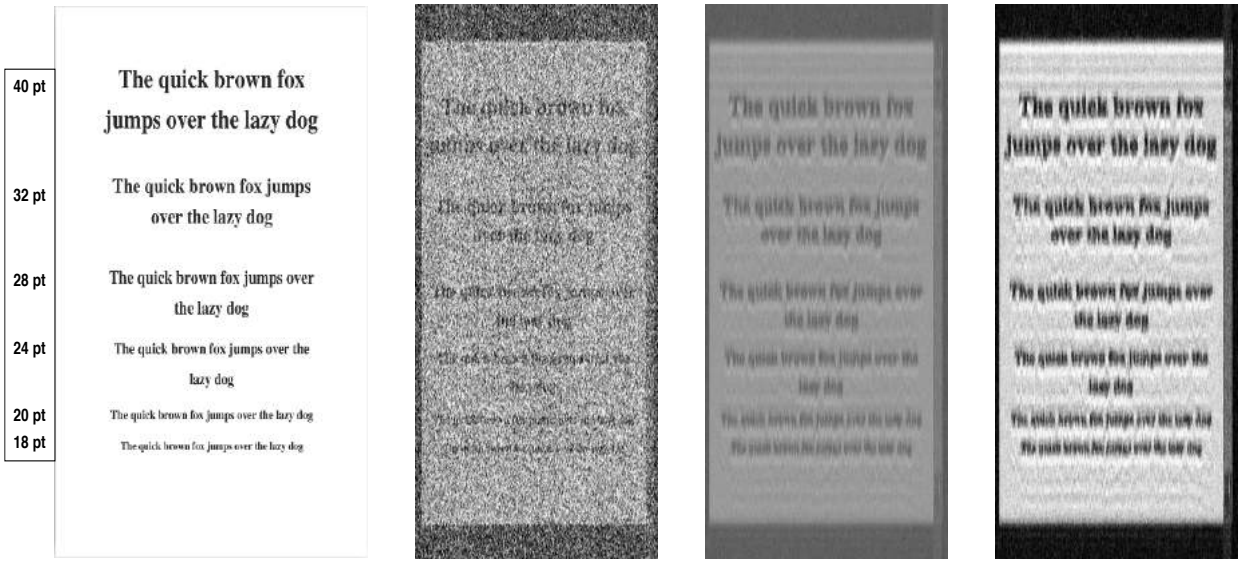

Figure 6: A computer screen captured using the experimental setup with a sample rate of $20MHz$. The images are displayed in the following order: (1) original screen, (2) screen reconstructed with captured signal (SSIM: 0.01), (3) screen reconstructed after a band-pass filter (SSIM: 0.46), (4) blended image of multiple frames constructed after a band-pass filter (0.13).

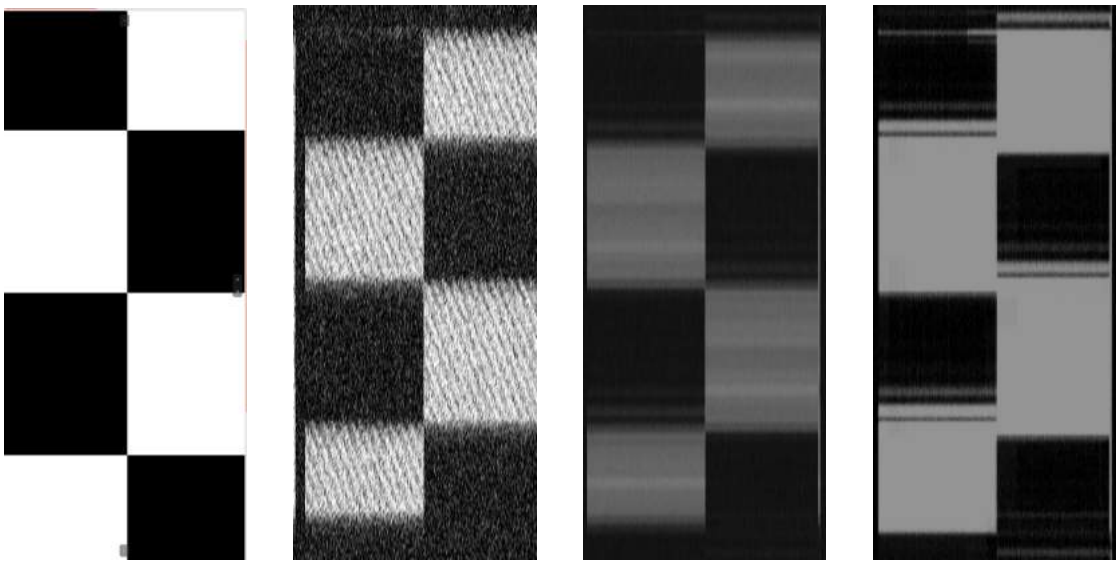

Figure 7: A checkerboard pattern displayed on a computer screen is captured using the experimental setup with a sample rate of $10MHz$. The images are displayed in the following order: (1) original screen, (2) screen reconstructed with captured signal (SSIM: 0.0305), (3) screen reconstructed after a band-pass filter (SSIM: 0.2443), (4) blended image of multiple frames constructed after a band-pass filter (SSIM: 0.4096).

in a data set should contain the same information with different distortions due to noise interference. This is due to the fact that the external noise sources were unlikely to affect multiple frames in the precise same manner. Therefore, while one reconstructed image may contain a distorted detail in one specific location, another reconstructed image may have that detail intact from noise. Therefore, blending multiple consecutive images together should result in the preserved details across different images to fall into right place in the end.

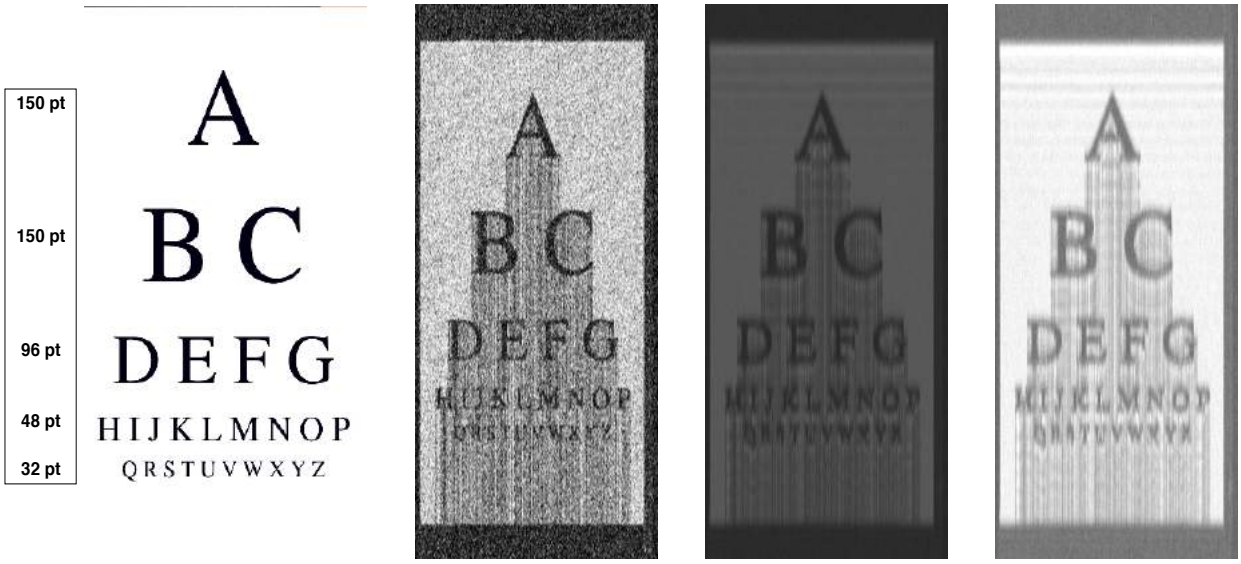

Figure 8: An eye chart displayed on a computer screen is captured using the experimental setup with a sample rate of $20MHz$. The images are displayed in the following order: (1) original screen, (2) screen reconstructed with captured signal (SSIM: 0.0198), (3) screen reconstructed after a band-pass filter (SSIM: 0.3628), (4) blended image of multiple frames constructed after a band-pass filter (SSIM: 0.3625).

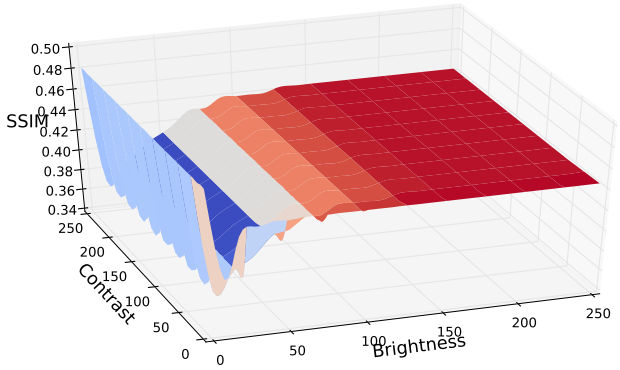

Figure 9: Variation of the SSIM index with brightness and contrast of the captured images before blending to create a resulting image. A brightness threshold of 130 is evident in this graph.

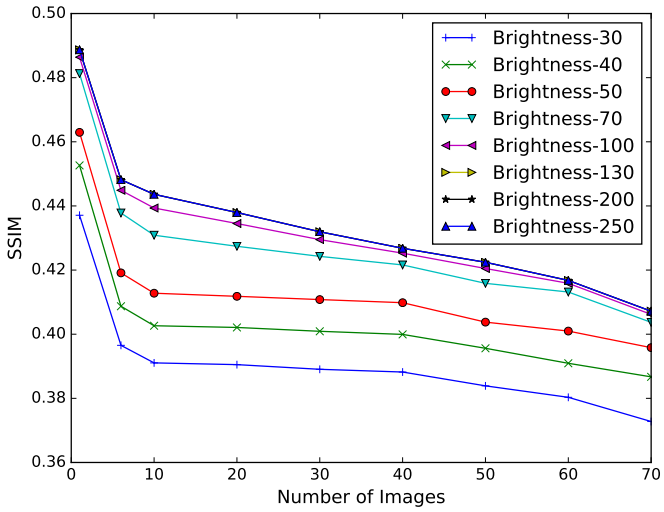

Figure 10: Variation of the SSIM with the number of images blended together. The accuracy of the captured image does not improve beyond the the brightness level of 130 in 8-bit greyscale images.

The image blending was performed by averaging the values of pixels which are present in the same location across a group of consecutive images. Figure 10 illustrates the the variation of SSIM values against the number of consecutive images blended together to produce the final output. The impact of brightness adjustments to the SSIM value of the reconstructed image, which was identified in the previous Figure 9, is also evident in this graph. The SSIM variation does not improve beyond the brightness value of 130. Meanwhile, the SSIM value of the resulting image decreases with the number of consecutive images blended together increases.

The reason for getting increasingly distorted images by blending a higher number of images together is attributable to the slight misalignments of the frames. Even though the misaligned frames are removed by manual inspection, there seems to be frames remaining that are not identifiable visually by human perception. This situation demands a technique for automatically aligning the image

frames that are misaligned. Automatically aligning images will require the identification of similar features across multiple images while the images are distorted differently. The alignment algorithm must be very precise – otherwise, the image reconstruction phase from the earlier stages should be improved further to minimise these misalignments imperceptible to the naked eye. The limiting factor of the sampling rate is the reason image reconstruction cannot lock into the frame rate precisely causing misalignments in the reconstructed frames.

Figure 7 and 8 compare and contrast the impact of enhancement techniques to reconstructed images. In the former, a checkerboard pattern was used as the screen target, while the latter uses an eye chart. It is evident that the preprocessing of EM data before image reconstruction and brightness adjustments after the image reconstruction has contributed to the clarity and readability. However, the contribution of blending adjacent images has mixed impacts. In Figure 7, image blending has caused the end result to improve the sharpness and the similarity to the original screen as identifiable from the SSIM index. However, in Figure 8, image blending seems not provided any improvement, while the SSIM index has decreased slightly. These results indicate that adjacent image blending can only be an effective method to improve EM side-channel based screen eavesdropping if it is possible to minimise frame misalignments. Even a marginal misalignment in an image dataset can lead to unpredictable results in the output.

5 CONCLUSION AND FUTURE WORK

This work focused on the issue of achieving successful EM side-channel eavesdropping attacks on computer monitors using SDR hardware. Previous work has shown that the sample rate of EM signal acquisition is the largest contributing factor to the clarity of the reconstructed images. However, the unavailability of sophisticated hardware with extremely fast sample rates such as $500MHz$ limits the capability of successful image reconstruction. This work explored some of the available workarounds to make successful EM side-channel eavesdropping attacks to monitors with hardware capable of sampling at as lower rates as $20MHz$.

Through empirical studies, it was revealed that when using SDR devices with wide bandwidths to acquire EM emissions from computer displays, it is necessary to extract the narrow band of frequencies emitted from the target carefully avoiding external noise sources including other computer monitors. A precisely designed band-pass filter can improve the image reconstruction significantly. Furthermore, proper adjustments to the reconstructed image quality have improved the recognisability of screen contents, such as text and shapes, as revealed through the SSIM index-based comparisons. It was revealed that even though blending similar images together is a well known method to increase the clarity of an image, the slight misalignments in the EM side-channel based eavesdropped images causes the technique to fail unless the maligned image frames are manually removed from the image data set. Algorithms to automatically detect and fix such issues are required in order to go further on that direction.

5.1 Future Work

As identified from the results of this work, multiple avenues remain to be explored in order to make EM side-channel based eavesdropping attacks on computer monitors more robust and viability in a broader range of real-world scenarios.

- When generating a stream of images based on EM emissions of a monitor, it would be advantageous to categorise sets of images that contains the same screen content. This is due to the fact that the current assumption of static content in the target monitor throughout the attack may not be realistic in real-world scenarios.
- The identification of badly reconstructed frames, such as those resulting from sudden noise interference, as outliers and remove them automatically from the output.
- Methods are required to align eavesdropped frames that are showing the same original screen content before they are blended together. Such a technique has to oversee the noise distortions applied differently to the images.
- When screen content is reconstructed, the automatic detection of the text shown on screen using optical character recognition (OCR) without human intervention improves the viability of the attack.

REFERENCES

[1] Stephen Butterworth. 1930. On the Theory of Filter Amplifiers. *Wireless Engineer* 7, 6 (1930), 536–541.

[2] Fürkan Elibol, Uğur Sarac, and Işin Erer. 2012. Realistic Eavesdropping Attacks on Computer Displays with Low-cost and Mobile Receiver System. In *Signal Processing Conference (EUSIPCO), 2012 Proceedings of the 20th European*. IEEE, 1767–1771.

[3] Daniel Genkin, Adi Shamir, and Eran Tromer. 2014. RSA Key Extraction via Low-bandwidth Acoustic Cryptanalysis. In *International Cryptology Conference*. Springer, 444–461.

[4] Robin Getz and Bob Moeckel. 1996. Understanding and eliminating EMI in Microcontroller Applications. *National Semiconductor* (1996).

[5] Yu-ichi Hayashi. 2016. State-of-the-art Research on Electromagnetic Information Security. *Radio Science* 51, 7 (2016), 1213–1219.

[6] Arie Kouwen, Mark Scanlon, Kim-Kwang Raymond Choo, and Nhien-An Le-Khac. 2018. Digital Forensic Investigation of Two-Way Radio Communication Equipment and Services. *Digital Investigation* 26S, 1 (07 2018).

[7] Markus Guenther Kuhn. 2002. *Compromising Emanations: Eavesdropping Risks of Computer Displays*. Ph.D. Dissertation. University of Cambridge.

[8] Martin Marinov. 2018. TempestSDR Remote Video Eavesdropping using a Software-defined Radio Platform. (2018). https://github.com/martinmarinov/TempestSDR, Last accessed on 2018-02-01.

[9] Samuel Joseph O'Malley and Kim-Kwang Raymond Choo. 2014. Bridging the Air Gap: Inaudible Data Exfiltration by Insiders. In *20th Americas Conference on Information Systems (AMCIS)*. Association for Information Systems.

[10] Michael Ossmann. 2016. Software Defined Radio with HackRF. *Great Scott Gadgets, https://greatscottgadgets. com/sdr* (2016).

[11] Henry W Ott. 2011. *Electromagnetic Compatibility Engineering*. John Wiley & Sons.

[12] Asanka Sayakkara, Nhien-An Le-Khac, and Mark Scanlon. 2018. Electromagnetic Side-Channel Attacks: Potential for Progressing Hindered Digital Forensic Analysis. In *Proceedings of the International Workshop on Speculative Side Channel Analysis (WoSSCA 2018)*. ACM, Amsterdam, Netherlands.

[13] Wim Van Eck. 1985. Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? *Computers & Security* 4, 4 (1985), 269–286.

[14] Zhou Wang, Alan C Bovik, Hamid R Sheikh, and Eero P Simoncelli. 2004. Image Quality Assessment: From Error Visibility to Structural Similarity. *IEEE transactions on image processing* 13, 4 (2004), 600–612.

[15] Alenka Zajic and Milos Prvulovic. 2014. Experimental Demonstration of Electromagnetic Information Leakage from Modern Processor-memory Systems. *IEEE Transactions on Electromagnetic Compatibility* 56, 4 (2014), 885–893.