URSI GASS 2020, Rome, Italy, 29 August - 5 September 2020

The Source Estimation of Electromagnetic Information Leakage from Information Devices

Ryota Birukawa(1), Daiya Nagata* (1), Yu-ichi Hayashi(2), Takaaki Mizuki(3), Hideaki Sone(3)
(1) Graduate School of Information Sciences, Tohoku University, Sendai, Miyagi, Japan, 980-8579, https://www.is.tohoku.ac.jp/
(2) Graduate School of Science and Technology, Nara Institute of Science and Technology, Nara, Japan
(3) Cyberscience Center, Tohoku University, Sendai, Miyagi, Japan

Abstract

A risk of eavesdropping the screen image of a device by exploiting unintended electromagnetic (EM) emanation is reported. Estimating the source of EM emanation from the device is an efficient method to protect the device from eavesdropping by use of EM shield to reduce unintended EM emanation. The authors estimated, multiple EM emanation sources by observing the EM distribution at leakage frequencies of a tablet and a display monitor. The mersurement, showed estimation of the EM emanation sources such as a cable that connects LCD panel to the integrated circuit in the tablet, HDMI cable, and the edge of the screen.

1 Introduction

Eavesdropping the screen image of a device by exploiting EM emanation has been shown as a serious threat[1]. EM information leakage occurs because there is a correlation between the transmission data of the displayed screen image and the AM-modulated EM emanation at the leakage frequency[2]. EM shielding the device is known as a countermeasure of the EM information leakage[3]. However, EM emanation sources should be located to use the EM shield. The authors developed a new method of source estimation of EM emanation by measuring the distribution of electromagnetic field at specific frequencies which are determined by estimating leakage frequencies of a tablet and a display monitor.

2 The leakage frequency estimation

The authors have developed a method to detect the leakage frequencies by displaying a specific image ("control image") on a device[4]. The control image on the device is designed so that, AM-demodulated EM emanation at the leakage frequency can be detected as an audible range frequency signal. By detecting the audio signal, the leakage frequencies are detected without screen reconstruction[4]. We used this method to estimate leakage frequency. In the following measurement, two devices are used: (1) a tablet that transmits the data with low voltage differential signaling (LVDS), and (2) a display monitor that transmits the data with TMDS (Transition Minimized Differential Signaling) which is data transmission protocol used in HDMI. The control images shown in Fig. 1 are designed by considering the mechanism of EM emanation in each transmission method and the leakage frequencies. When the control images are displayed on the device, the audible range frequency signal is determined to be 240 Hz. We estimated EM emanation sources at the estimated leakage frequencies with this method.

(a) Control image in LVDS (b) Control image in TMDS

Figure 1. Control image in each transmission method

2.1 Estimating the leakage frequency in the tablet

Figure 2 shows the detected 240 Hz signal intensity of the AM demodulated EM emanation of the tablet.
Information leakage likely occurred at frequencies where steep peaks were observed. As indicated in Figure 2, we estimated 653 MHz and 932 MHz as leakage frequencies and we observed audio signal in this frequency.
The images in Fig. 3 are (a) displayed image in the tablet and reconstructed images (b, c) from detected EM emanation at these two frequencies. The images are well reconstructed in both cases.

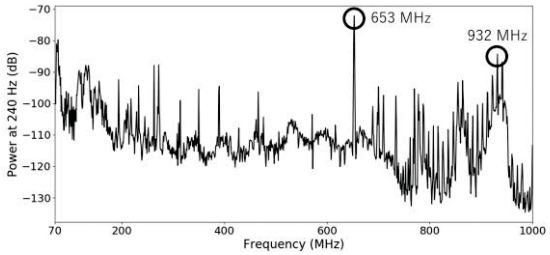
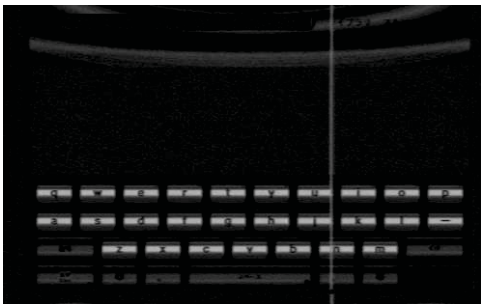


Figure 2. Detected 240 Hz signal of the AM demodulated EM emanation of the tablet

(a) Displayed image on the tablet



(b) 653MHz

(c) 932MHz

Figure 3. Reconstruction results of the tablet

2.2 Estimating the leakage frequency in the display monitor

Figure 4 shows detected 240 Hz signal in the display monitor. As indicated in Figure 4, we estimated 462 MHz and 522 MHz are leakage frequencies because steep peaks were observed and we also observed audio signal.

We confirmed that unintended EM emanation likely leaks strongly at higher harmonics of the HDMI clock signal (154 MHz) in Figure 4. Therefore, we estimated 462 MHz is generated from HDMI cable and 522 MHz is generated from another EM emanation source. The images in Fig. 5 are (a) displayed image on the display monitor and reconstructed images (b, c) for these two frequencies.

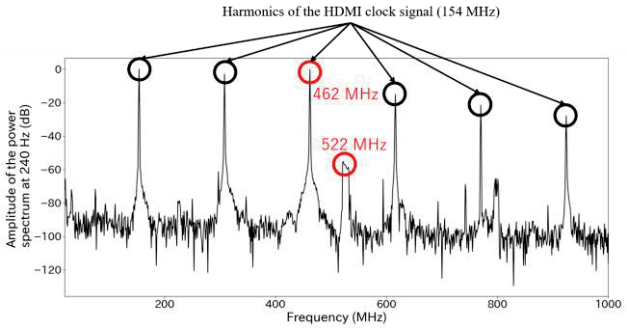
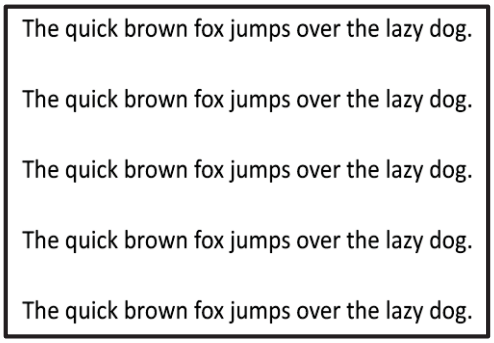
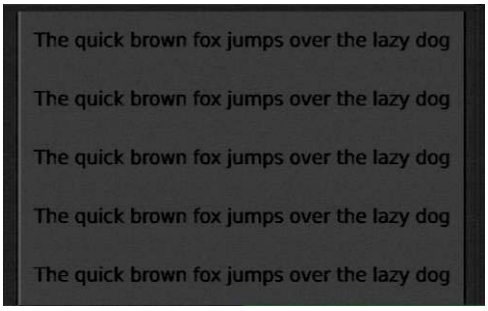


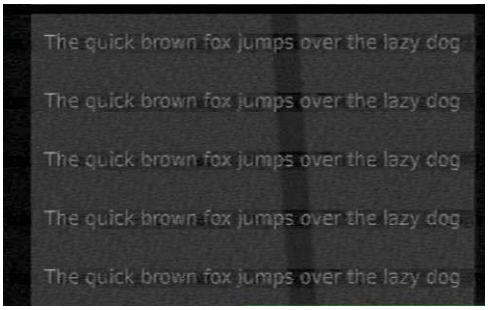
Figure 4. Detected 240 Hz signal of the AM demodulated EM emanation in the display monitor



(a) Displayed image on the display monitor



(b) 462MHz



(c) 522MHz

Figure 5. Reconstruction results of the display monitor

3 Measuring the distribution of electromagnetic field

This section discusses on measured the distribution of the electromagnetic field of the tablet and the display monitor at leakage frequencies.

3.1 Estimating EM emanation sources of the tablet

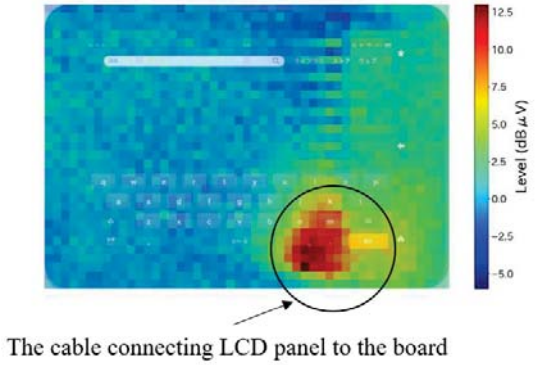
Figure 6 shows the distribution of the electromagnetic field of the tablet at 653 MHz and 932 MHz.
We confirmed that the EM emanation source of 653MHz is from the cable which connects LCD panel to the board of the tablet, and the source of 932MHz is from the edge of the screen in Figure 6. The authors speculated that the reason why the edge of the screen generates EM emanation is they act as antennas. Therefore, we confirmed multiple EM emanation sources in the tablet.

3.2 Estimating EM emanation sources in the display monitor

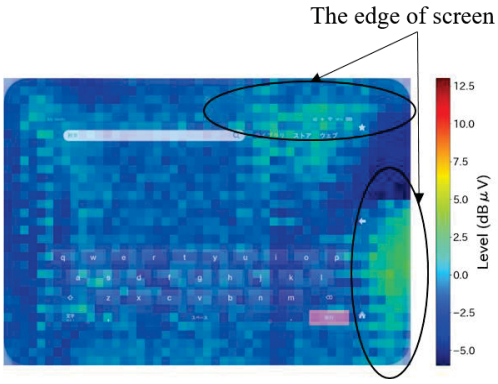
Figure 7 shows the distribution of the electromagnetic field of the front and back surfaces of the display monitor at 462 MHz and 522 MHz. We estimated EM emanation sources are HDMI cable, power supply wiring, and the edge of the screen.
Figure 8 shows reconstruction results at displaying the display setting window in the display monitor. As indicated in Figure 8, we confirmed that 522MHz is concerned with the EM emanation sources of the display monitor. The display setting window image is overwritten on the original screen image signal transmitted in HDMI cable. Different reconstruction image means their leakage frequency have different sources which are before and after the setting screen is overwritten. Therefore, we found that 462 MHz and 522 MHz have different EM emanation sources.

4 Conclusion

In this paper, multiple EM emanation sources are estimated at each leakage frequency of the tablet and the display monitor. The measurement, showed EM emanation sources are the cable connecting LCD panel to the board of the tablet, the edge of the screen, HDMI cable and power supply wiring used in display monitors. Therefore, we have to take multiple EM emanation sources into account to prevent EM information leakage from devices.

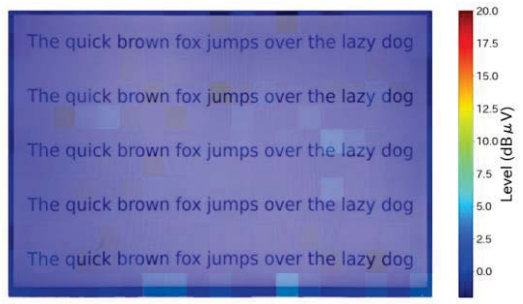


(a) 653MHz

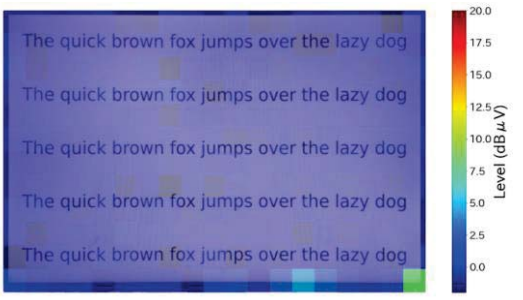


(b) 932MHz

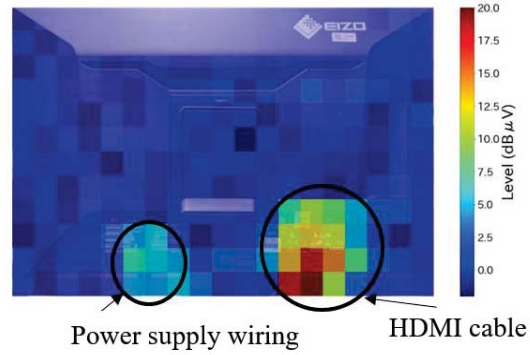
Figure 6. Distribution of electromagnetic field of the tablet



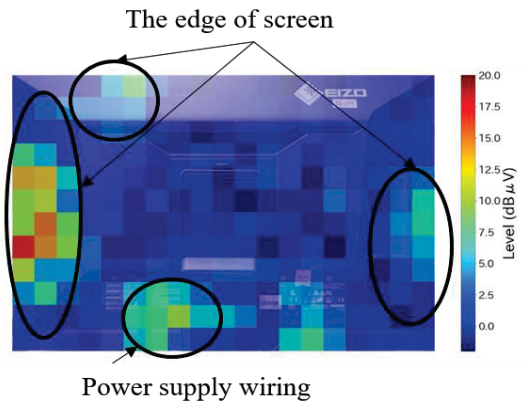
(a) 462 MHz (Front)



(c) 522 MHz (Front)

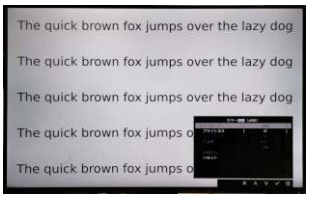


(b) 462 MHz (Back)

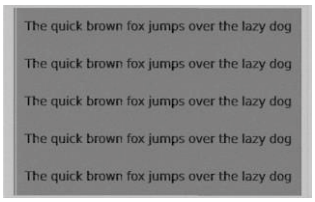


(d) 522 MHz (Back)

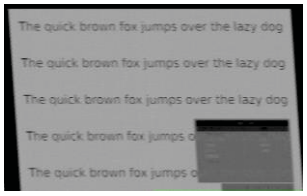
Figure 7. Distribution of electromagnetic field of the display



(a) Displayed image on the display monitor



(b) 462MHz



(c) 522MHz

Figure 8. Reconstruction results at displaying the display setting screen

5 References

1. M.G. Kuhn, “Compromising emanations: eavesdropping risks of computer displays”, Technical Report UCAM-CL-TR-577, University of Cambridge, Computer Laboratory, December 2003.
2. M.G. Kuhn, “Electromagnetic Eavesdropping Risks of Flat-Panel Displays,” 4th Workshop on Privacy Enhancing Technologies, Proceedings, LNCS 3424, pp. 88-105, 2004.
3. Y. Hayashi, N. Homma, M. Miura, T. Aoki, H. Sone, “A Threat for Tablet PCs in Public Space: Remote Visualization of Screen Images Using EM Emanation," 21st ACM Conference on Computer and Communications Security (CCS'14), pp. 954-965, 2014.
4. R. Birukawa, Y. Hayashi, T. Mizuki and H. Sone, “A study on an Effective Evaluation Method for EM Information Leakage without Reconstructing Screen,” 2019 International Symposium on Electromagnetic Compatibility - EMC EUROPE, Barcelona, Spain, 2019, pp. 383-387.