TEMPEST attack against high-resolution displays using differences in the transfer function of EM waves

Taiki Kitazawa(1), Yoshiki Kitamura(1), Yougwoo Kim(1), Daisuke Fujimoto(1), Hideaki Sone(2), and Yuichi Hayashi(1)
(1) Graduate School of Science and Technology, Nara Institute of Science and Technology, Nara, Japan
(2) Tohoku University, Sendai, Miyagi, Japan

Abstract

Recent displays are divided into multiple areas to meet the requirement for high-resolution and transmit multiple pixel information simultaneously. Therefore, it is difficult to apply the conventional TEMPEST attack to such high-resolution displays due to the leaked electromagnetic (EM) wave with multiple pixel information. In this paper, we propose a method for reconstructing screen information by separating each pixel information from EM waves in which multiple pixel information is mixed, focusing on the difference in the transfer function of leaking EM waves. In the experiment, the proposed method was applied to a high-resolution display. The screen is divided into left and right by measuring the EM waves at two frequencies with different transmission characteristics. We then demonstrated that the screen could be restored.

1. Introduction

Recently, as information devices become more diverse, indispensable displays are developed with higher resolution. The display is divided into multiple areas to respond to high-resolution and transmits pixel information corresponding to each part on different lines [1].

Considering the TEMPEST attack against such displays, the conventional methods [2]–[8] cannot be applied directly. In the conventional method, attackers can reconstruct the video image by extracting the pixel information directly from the leaked electromagnetic (EM) emanations since target displays are not divided into multiple areas.

However, it becomes difficult to reconstruct information in displays that divide the screen area because multiple pixel information is mixed in the leaked EM emanations.

In this paper, to address the problem, we propose a method for reconstructing the screen information against emanations with multiple pixel information using the difference in the transfer function of the leaked EM emanations from the leakage source inside display to the antenna installed outside the device. Specifically, the image to be displayed on the screen is controlled so that each pixel information transmitted has a different period. The leaked EM emission is amplitude-demodulated to identify the frequency at which each pixel information is most strongly contained, using the period information as an identifier. Moreover, the information extracted from those frequencies are combined to reconstruct the information of the entire screen image.

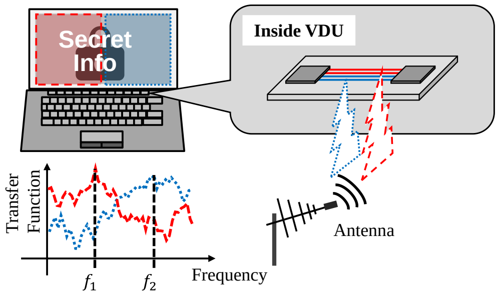


Figure 1. The difference of transfer function in EM emanations between leakage sources and the antenna from adjacent lines transmitting pixel information.

2. Proposed method for reconstructing screen information using the difference in transfer function of multiple emanations

As mentioned in Section 1, the high-resolution display is divided into multiple areas and transmits pixel information corresponding to each part on different lines. Generally, pixel information is transmitted on adjacent lines using the low-voltage differential signaling (LVDS). Therefore, the leaked EM wave emitted from the display contains a mixture of pixel information for each divided screen. Furthermore, since the multiple pixel information transmitted by the LVDS method uses the same clock, the leaked EM waves are synchronized. Even if averaging is performed in the time domain, the effect cannot be removed [9], [10]. As a result, when an attacker reconstructs the screen, the pixel information of each of the divided screens interferes with each other, making it difficult to reconstruct the information.

However, as shown in Figure 1, EM waves emitted from each line transmitting pixel information are received by an antenna through different transfer functions. These differences in transfer function depends on the design of each transmission line, the relative position between these lines, and the receiving position of antenna.

In this paper, we reconstruct video images by focusing on the difference of transfer function and observing EM

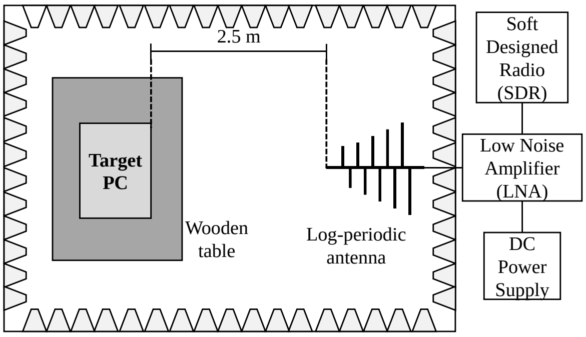


Figure 2. Measurement setup.

Table 1. Measurement equipment.

Equipment	Model
Antenna	Schwarzbeck USLP D-69250
LNA	COSMOWAVE LNA270WS
SDR	National Instruments PXIe-5840

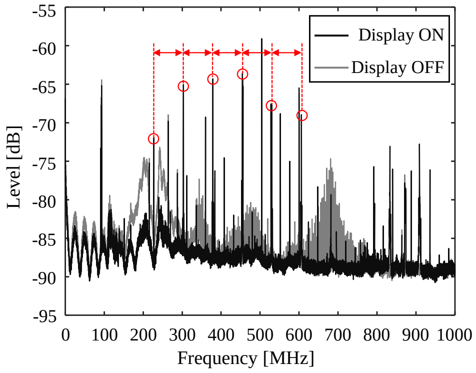


Figure 3. Comparision of leaked frequency spectrum in each state of the display ON/OFF of laptop PC. There are peaks at 277 MHz to 75 MHz intervals.

emanations at frequencies with high transmission efficiency, including the target pixel information.

To facilitate the search for frequencies that satisfy these conditions, we control a video image of the display. Specifically, by displaying an image with period on each area, we make it possible to discriminate which pixel information is leaking; by observing the frequency spectrum after the amplitude demodulation, it is easy to determine which area of the screen contains the relevant pixel information. To further facilitate the measurement, we use image patterns whose leaking signal after demodulation can be recognized as sound information [11]–[13].

3. Image reconstruction from a leaked EM emanation with mixed pixel information

3.1 Identify the leakage frequency corresponding to each screen area using periodic images

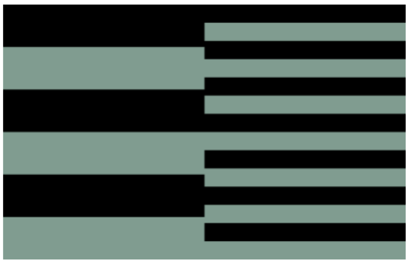


Figure 4. The image displayed on the laptop PC for evaluation.

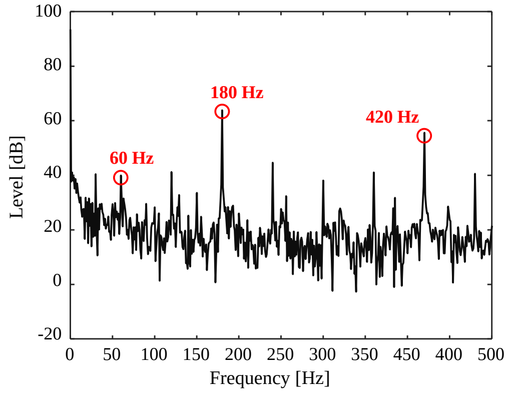


Figure 5. The spectrum of leakage signal after amplitude demodulation at the center frequency of 303 MHz. There are some peaks that corresponds to the displayed image in Figure 4.

Table 2. Peak values at each center frequency.

Center Frequency	180 Hz (Left)	420 Hz (Right)	Difference (180 − 420 Hz)
227 MHz	31.86 dB	34.04 dB	-2.18 dB
303 MHz	63.84 dB	55.61 dB	**+8.23 dB**
378 MHz	36.16 dB	52.96 dB	-16.79 dB
454 MHz	45.92 dB	64.04 dB	**-18.12 dB**
529 MHz	44.03 dB	37.49 dB	+6.54 dB
604 MHz	53.61 dB	52.63 dB	+0.98 dB

Figure 2 and Table 1 show the experimental setup. As an evaluation target, we use a laptop PC that divides the screen into two areas from the center of the vertical direction and draws each screen using pixel information transmitted by different lines. We measure the EM leakage in the chamber, and the distance from the laptop PC to the antenna is 2.5 m. Figure 3 shows the measurement results of the frequency spectrum of the EM leakage. To search for EM waves containing pixel information, we measured the radiation spectrum in each state of the display ON/OFF. During the display operation, peaks were observed at 277 MHz to 75 MHz intervals.

Next, we identify frequencies containing pixel information for each drawing area from the EM emanations. Figure 4 shows the image with periodic displayed on the laptop PC created based on previous studies [11]–[13].

While displaying the image, the amplitude demodulated leaked signal contains a period corresponds to 180 Hz on the left side and a period corresponds to 420 Hz on the right side. We distinguish which period in the left or right is a dominant at the center frequency that observed some peaks in Figure 3.

Figure 5 shows the frequency spectrum after applying the amplitude demodulation to leaked EM wave at the center frequency of 303 MHz. We can observe some peaks, 60 Hz of refresh rate and 180 Hz and 420 Hz, including pixel information of the left and right sides, respectively.

Table 2 lists the frequency components and their intensities obtained after the amplitude demodulation at the peak frequencies shown in Figure 3. The difference between 180 Hz and 420 Hz is also shown. The 303 MHz contains a strong component of 180 Hz, and 454 MHz contains a strong component of 420 Hz, predicting that 303 MHz and 454 MHz contain the information left and right screen, respectively. At other frequencies, the intensity difference between 180Hz and 420Hz is slight, so the pixel information of the right and left screens are mixed with the same intensity, indicating that it is difficult to reconstruct the screen when these frequencies are used.

3.2 Screen reconstruction using multiple leak frequencies

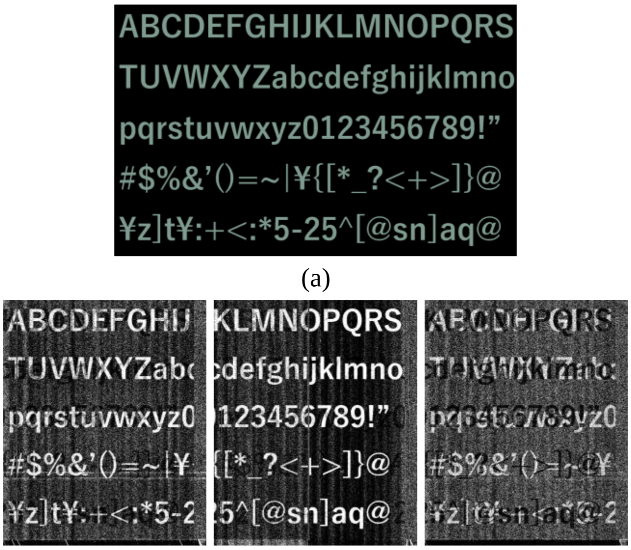
Based on the results of the previous section, in this section, the verification of restoring screen information for an image with characters displayed on the laptop PC is conducted by minimizing the overlap between the left and right screen information. Figure 6 shows the screen displayed on the laptop and the reconstructed video image when the center frequency is set to 303 MHz and 454 MHz. The reconstructed images are applied to averaging sufficiently. As results obtained in the previous section, the image left and right sides were reconstructed at 303 MHz and 454 MHz, respectively.

We then reconstruct the video image at a center frequency of 604 MHz where the intensity difference between 180 Hz and 420 Hz is small, as shown in Table 2; expected that pixel information are contained at the same level in the emanation. As shown, unlike the case focusing on 303 MHz and 454 MHz, both left and right screens are mixed.

From the above results, although the overall leakage intensity is strong at 604 MHz, the difference in transmission characteristics is small, which makes it difficult to recognize the screen information due to overlapping characters. However, at 303 MHz and 454 MHz, the characters can be recognized without overlapping.

4. Conclusion

In this paper, we proposed the method for reconstructing screen information against EM emanations with multiple pixel information. The proposed method focused on the difference of transfer function in leaked EM emanations as varying the observed frequency. First, we experimented to verify the difference of transfer function by displaying the image with a certain period on the high-resolution display that divides the screen area. Next, we verified the proposed method by varying the frequency of observation of EM emanation from high-resolution displays, it was possible to separate the pixel information transmitted in each drawing area and reconstruct the screen information.



(a)

(b) (c) (d)

Figure 6. (a) The image displayed on the laptop PC. Reconstruct video images at the center frequency of (b) 303 MHz, (c) 454 MHz, (d) 604 MHz.

5. Acknowledgements

This work was supported by JSPS KAKENHI Grant Numbers JP 21K19772, JP 21K03995 and JST FOREST Program, Grant Number JPMJFR206L.

References

[1] L. Semiconductor, “Open LDI/FPD-LINK/LVDS Transmitter Interface IP User Guide,” 2019.

[2] W. van Eck, “Electromagnetic radiation from video display units: An eavesdropping risk?,” *Computers and Security*, vol. 4, no. 4, pp. 269–286, 1985.

[3] M. G. Kuhn, “Compromising emanations: eavesdropping risks of computer displays,” *Citeseer*, 2002

[4] Y. Hayashi, N. Homma, M. Miura, T. Aoki, and H. Sone, “A Threat for Tablet PCs in Public Space: Remote Visualization of Screen Images Using EM Emanation,” in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, Scottsdale, Arizona, USA, Nov. 2014, pp. 954–965.

[5] D. Nagata, Y.-I. Hayashi, T. Mizuki, and H. Sone, “QR Bar-Code Designed Resistant against EM Information Leakage,” in *2021 XXXIVth General Assembly and Scientific Symposium of the International Union of Radio Science (URSI GASS)*, Aug. 2021, pp. 1–4.

[6] Y.-I. Hayashi, “Electromagnetic Information Security Threats to Hardware and Their Countermeasures,” *IEICE ESS Fundamentals Review*, vol. 13, p. 28, Jul. 2019.

[7] V. Yli-Mäyry, D. Miyata, N. Homma, Y. Hayashi, and T. Aoki, “Statistical Test Methodology for Evaluating Electromagnetic Information Leakage

From Mobile Touchscreen Devices," *IEEE Trans. Electromagn. Compat.*, vol. 61, no. 4, pp. 1107–1114, Aug. 2019.

[8] Y.-I. Hayashi, N. Homma, Y. Toriumi, K. Takaya, and T. Aoki, "Remote Visualization of Screen Images Using a Pseudo-Antenna That Blends Into the Mobile Environment," *IEEE Trans. Electromagn. Compat.*, vol. 59, no. 1, pp. 24–33, Feb. 2017.

[9] P. De Meulemeester, B. Scheers, and G. A. E. Vandenbosch, "Differential Signaling Compromises Video Information Security through AM and FM Leakage Emissions," *IEEE Trans. Electromagn. Compat.*, vol. 62, no. 6, pp. 2376–2385, 2020.

[10] P. De Meulemeester and B. Scheers, "A quantitative approach to eavesdrop video display systems exploiting multiple electromagnetic leakage channels," *IEEE Transactions on*, 2019

[11] R. Birukawa, Y.-I. Hayashi, T. Mizuki, and H. Sone, "A study on an Effective Evaluation Method for EM Information Leakage without Reconstructing Screen," in *2019 International Symposium on Electromagnetic Compatibility - EMC EUROPE*, Sep. 2019, pp. 383–387.

[12] R. Birukawa, D. Nagata, Y.-I. Hayashi, T. Mizuki, and H. Sone, "The Source Estimation of Electromagnetic Information Leakage from Information Devices," in *2020 XXXIIIrd General Assembly and Scientific Symposium of the International Union of Radio Science*, Aug. 2020, pp. 1–4.

[13] R. Birukawa, T. Mizuki, H. Sone, and Y.-I. Hayashi, "A Practical Evaluation Method for EM Information Leakage by Using Audible Signal," in *2019 Joint International Symposium on Electromagnetic Compatibility, Sapporo and Asia-Pacific International Symposium on Electromagnetic Compatibility (EMC Sapporo/APEMC)*, Jun. 2019, pp. 250–253.