Design of Suitable Controlled Image for Evaluation of EM Information Leakage

Daiya Nagata, Ryota Birukawa, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone

Abstract – There is a risk of eavesdropping the screen image of an information device by exploiting unintended electromagnetic (EM) emanation. Leakage frequencies may be detected by displaying a specific image ("control image") on the device. The control image is effective to estimate the source of EM emanation from the device. In this article, to design a more effective control image for estimating the leakage frequency, we compared several control images considering EM emanation in transition-minimized differential signaling.

1. Introduction

There is a threat of EM information leakage from the display of tablet devices [1]. Electromagnetic (EM) eavesdropping from high-definition multimedia interface (HDMI) has been reported [2]. There is a method to estimate the source of EM emanation from the device by displaying a specific image ("control image") on the display and estimating the leakage frequency [3]. In this article, we discuss the design of the control image that is more effective in estimating the leakage frequency in transition-minimized differential signaling (TMDS), which is the transmission method used for HDMI cables.

2. Estimating the Leakage Frequency by Using the Control Image

The control image displayed on the information 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]. This method is used to estimate the leakage frequency by designing the control the control image considering the EM emanation in TMDS.

Manuscript received 29 August 2020.

Daiya Nagata and Ryota Birukawa are with the Graduate School of Information Sciences, Tohoku University, 6-3-09 aza Aoba Aramaki Aoba-ku, Sendai, Miyagi, 980-8579 Japan; e-mail: daiya.nagata.r6@dc.tohoku.ac.jp.

Yu-ichi Hayashi is with the Nara Institute of Science and Technology, 8916-5 Takayma-cho, Ikoma, Nara, 630-0192 Japan; e-mail: yu-ichi@is.naist.jp.

Takaaki Mizuki and Hideaki Sone are with the Cyberscience Center, Tohoku University, 6-3 aza Aoba Aramaki Aoba-ku, Sendai, Miyagi, 980-8578 Japan; e-mail: mizuki+ursi@tohoku.ac.jp, sone@cc.tohoku.ac.jp.

This work was supported by JSPS KAKENHI grants 17H01751 and 19H01104.

Figure 1 shows an example of image reconstruction. The amplitude of an AM demodulation signal 240 Hz from radiation 0 MHz to 1000 MHz was measured while the control image was displayed. The result shown in Figure 1a indicates that leakage frequencies 462 MHz and 522 MHz are estimated. Figure 1b is displayed image on the display monitor, and Figures 1c and 1d are images obtained by EM radiation at the frequencies. The reconstructed images in Figures 1c and 1d have degraded contrast, and contrast in Figure 1d is inverted, but the information displayed can be read. By using the control image, the leakage frequency was estimated effectively.

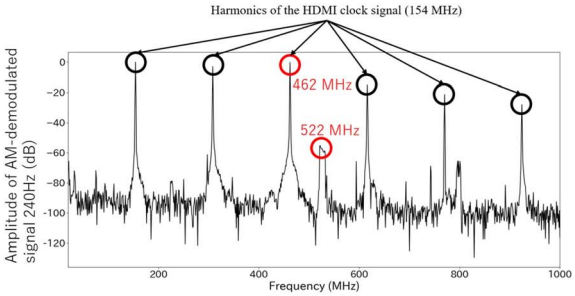
A low-voltage differential signaling (LVDS) transmission method is used in laptop PCs and tablets. The control image using a display color with more bit inversions in transmission data is more suitable for estimating a leakage frequency for LVDS [4]. The control image that makes the intended frequency large is more effective to estimate the leakage frequency. To design a more effective control image for estimating the leakage frequency in TMDS, we compared multiple control images considering EM emanation in TMDS.

3. Design and Evaluation of Control images

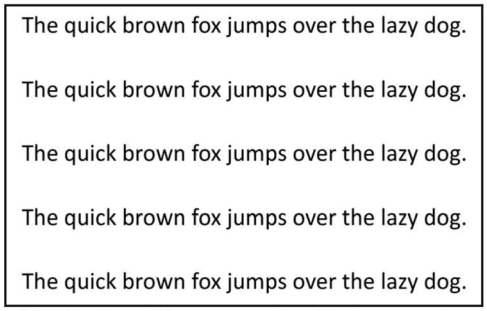
The control image derived from a previous study [4] is "striped black and white" and has black and white stripes, shown in Figure 2a; this is used as a reference for proposed control images. TMDS and LVDS are digital signal transmission methods, which differ by the encoding format. The encoding process of TMDS has two stages. Each RGB 8 bit code is converted to a transition-minimized 9 bit code word and then into a 10 bit code word that manages the overall dc balance of the transmitted stream [5]. The overall appearance numbers of "0" and "1" in the output stream become equal. Even if the input RGB values are the same, the output may be different, depending on past transmission data. Effective control image for evaluating EM information leakage should have no fluctuation in the number of bit inversions in each encoding.

Such conversion cases are 52 among 256 values of 8-bit data. The number of bit inversions in 10 bits is at least two times and at most five times. In this article, the control image was designed from 52 cases, using display color cases that have bit inversion for two, three, and five times. A display color (RGB value: 16, 16, 16) that has bit inversion for two times was selected as a display color in the region of small emanation.

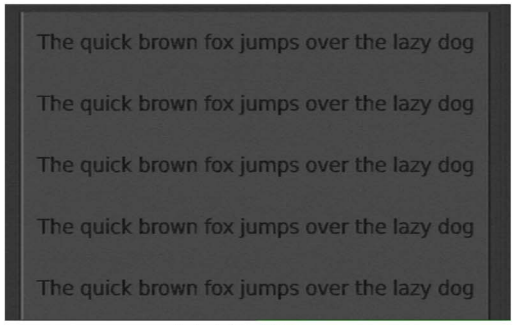
Figures 2b–2d show control images that have different bit inversion numbers. Table 1 shows the display colors used in the control images. The case



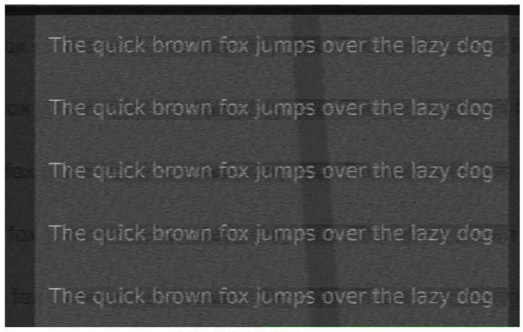
(a) Amplitude of AM-demodulated signal 240Hz



(b) Displayed image on the display monitor



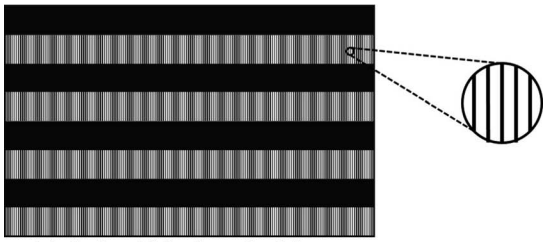
(c) 462 MHz



(d) 522 MHz

Figure 1. Reconstruction results of the display monitor.

(Figure 2d) of bit inversion for five times, which is a maximum number, has the largest emanation. When the control images are displayed on the device at a refresh rate of 60 fps (≒59.95), the audible range frequency signal is determined to be 240 Hz, which is a product of the number of striped patterns control images which has



(a) Striped black and white

(b) Bit inversion for 2 times

(c) Bit inversion for 3 times

(d) Bit inversion for 5 times

Figure 2. Control images in TMDS.

Table 1. Colors used for designing control images in TMDS

Displayed color	RBG Value	TMDS data	EM emanation
Bit inversion for 2 times	16 16 16	CH1: 0111110000 CH2: 0111110000 CH3: 0111110000	Small
(b) Bit inversion for 2 times	238 238 238	CH1: 1000001111 CH2: 1000001111 CH3: 1000001111	Small
(c) Bit inversion for 3 times	137 137 137	CH1: 0110000111 CH2: 0110000111 CH3: 0110000111	Medium
(d) Bit inversion for 5 times	85 85 85	CH1: 0100110011 CH2: 0100110011 CH3: 0100110011	Large

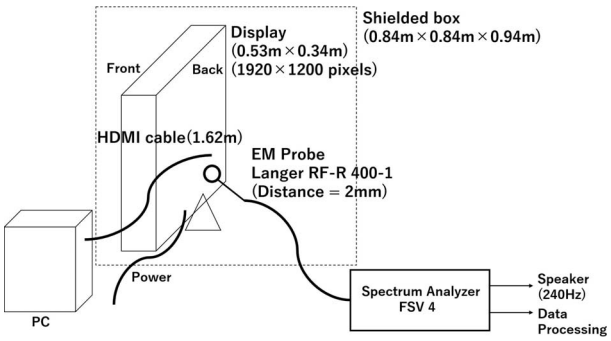


Figure 3. Experimental setup.

Table 2. Specifications of the target device[a]

Number of pixels	1920 × 1200 (WUXGA)
Refresh rate	59.95 Hz
Horizontal scan frequency	74.04 kHz

[a] WUXGA Wide Ultra Extended Graphics Array.

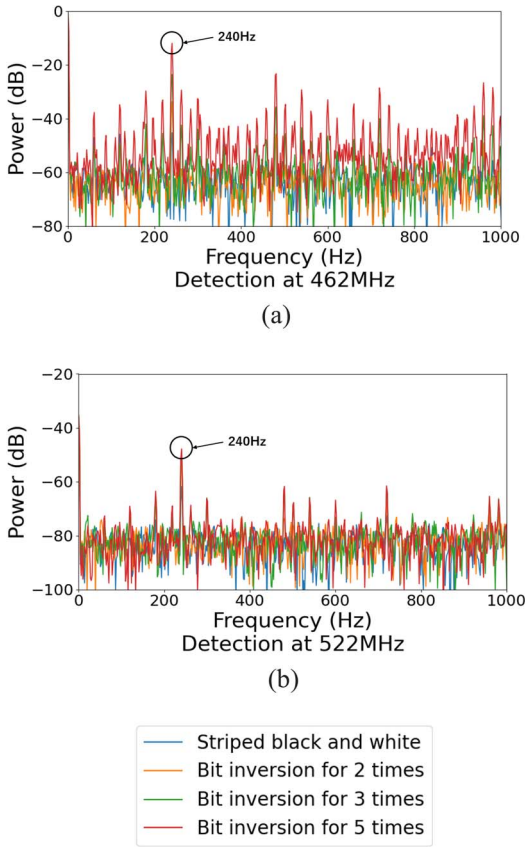


Figure 4. Spectrum of AM-demodulated signal.

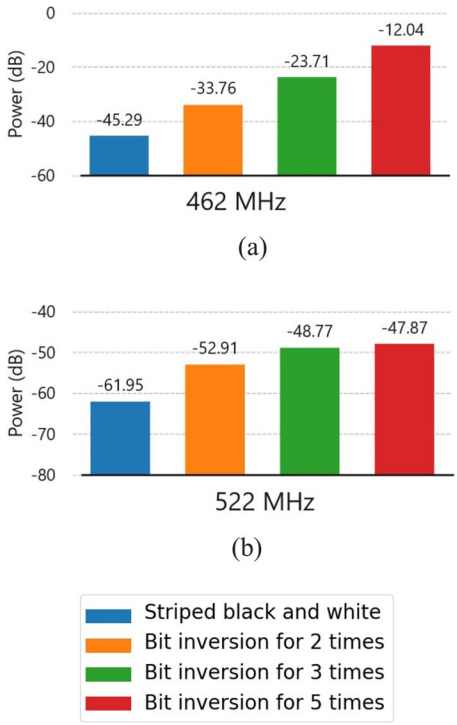


Figure 5. Peak value at 240 Hz of each control image.

four stripes and the refresh rate (240 Hz). We designed control images with the same size as the screen resolution 1920 × 1200. Figure 3 shows the experimental setup, and Table 2 shows specifications of the target device.

Figure 4 shows spectrum of AM-demodulated signal at the leakage frequencies, and Figure 5 shows the peak value of 240 Hz at the leakage frequency of each control image. We confirmed that the larger the number of bit inversions becomes in the transmitted signal at the leakage frequencies of both 462 MHz and 522 MHz, the larger the peak value of 240 Hz becomes. The control image of "case d" (five times) in Table 1 and Figure 2d has the highest sensitivity to evaluate EM information leakage frequency.

4. Conclusion

To design a more effective control image for estimating the leakage frequency, we compared several control images considering EM emanation in TMDS. We designed control images by selecting the display color considered the number of bit inversion of transmission signal. We confirmed that the larger the number of bit inversion of the transmission signal of display color becomes, the larger the peak value of 240 Hz becomes. We considered that it would be effective to consider the choice of display color when estimating the leakage frequency using the control image that contained the intended frequency.

5. References

1. 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," CCS ′14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, November 3–7, 2014, pp. 954-965.
2. I. Kubiak and A. Przybysz, "DVI (HDMI) and DisplayPort Digital Video Interfaces in Electromagnetic Eavesdropping Process," IEEE International Symposium on Electromagnetic Compatibility, Barcelona, Spain, September 2–6, 2019, pp. 388-393.
3. R. Birukawa, D. Nagata, Y. Hayashi, T. Mizuki, and H. Sone, "The Source Estimation of Electromagnetic Information Leakage from Information Devices," Thirty-Third General Assembly and Scientific Symposium of the International Union of Radio Science, Rome, Italy, August 29–September 5, 2020, pp. 1-4.
4. R. Birukawa, Y. Hayashi, T. Mizuki, and H. Sone, "A Study on an Effective Evaluation Method for EM Information Leakage without Reconstructing Screen," IEEE International Symposium on Electromagnetic Compatibility, Barcelona, Spain, September 2–6, 2019, pp. 383-387.
5. Digital Display Working Group, Digital Visual Interface DVI, Revision 1.0, (02 April 1999), Online, Retrieved from http://www.cs.unc.edu/Research/stc/FAQs/Video/dvi_spec-V1_0.pdf