Progress In Electromagnetics Research C, Vol. 7, 51–64, 2009

MEASUREMENT OF COMPUTER RGB SIGNALS IN CONDUCTED EMISSION ON POWER LEADS

H. Sekiguchi and S. Seto

National Institute of Information and Communications Technology
4-2-1, Nukui-Kitamachi, Koganei-shi, Tokyo 184-8795, Japan

Abstract—leakage of a computer display image that can be reconstructed using the conducted emission on its power leads. The reconstructed images can be generated from the relevant signal that was conducted-emitted by the switching of RGB (Red-Green-Blue) signals in the monitor. The relevant signal was then contained in the frequency region higher than 100 MHz in the conducted emission. From these findings, a measurement system was developed to measure the relevant signal in a conducted emission to 1000 MHz. The relevant signals of three PCs were then measured taking account of the signal-to-noise ratio. The measurement results revealed that the relevant signal level depended on the PC and receiving frequency. In addition, the qualities of the reconstructed images were checked using certain receiving frequencies. The reconstructed image quality and the measured relevant signal level were then compared for the same receiving frequency, and a correlation was found.

1. INTRODUCTION

Concerns about information security have increased with the growth of computer and network use in society. In 2005, a general information security management system (ISMS) standard was published jointly as the ISO/IEC 27001 and 27002 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) [1, 2]. In addition, the Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T) published the ISMS X.1051 for telecommunications in 2004 [3]. The ISMSs are used by organizations as a systematic way of managing sensitive information.

Corresponding author: H. Sekiguchi (hide@nict.go.jp).

In the ISMSs, information leakage due to electromagnetic emission from electrical devices is treated as a physical security issue. The specifications require security risk evaluation and countermeasures. Note that the terms TEMPEST and Emission Security (or Emanations Security; EMSEC) have been used generically in the study of information leakage and countermeasures [3, 4]. As a typical example, it has been reported that the display image on a personal computer (PC) can be reconstructed from electromagnetic radiation [5, 6]. The quality of the reconstructed image depends on the receiving frequency. Since the display image may contain information such as confidential text, the quality evaluation of the reconstructed image is very important.

Thus far, we have proposed and investigated an evaluation method for the relevant signal emitted by the switching of the red, green, and blue (RGB) signals in a PC [7, 8]. Note that the relevant signal is a pulse-like signal with a wide spectrum due to the switching. The relevant signal in the electromagnetic radiation has been measured taking account of the signal-to-noise ratio.

In the present study, we focus on the measurement of the relevant signal in the conducted emission on the power leads of the PC, because the display images can be reconstructed from such a relevant signal in a receiving frequency higher than 100 MHz [9]. We first discuss and develop the measurement system using line impedance stabilization networks (LISNs) that can pick up the conducted emission on the power leads by applying general measurement systems for conducted emission [10–12]. We then investigate the frequency response of LISNs at frequencies higher than 30 MHz to develop the measurement system; a LISN is generally used at frequencies lower than 30 MHz. Next, we develop the measurement system using two receivers and a pair of LISNs suitable for the frequency range from 1 to 1000 MHz on the basis of our previous studies [7–9]. We then measure the relevant signal in the conducted emission on the power leads at a receiving frequency between 50 and 1000 MHz. In addition, we reconstruct display images at some receiving frequencies. Finally, we compare the measured relevant signal level and the reconstructed image quality for the same receiving frequency.

2. DEVELOPMENT OF A SYSTEM FOR MEASURING A RELEVANT SIGNAL IN CONDUCTED EMISSION ON POWER LEADS OF A PC

Generally, the electromagnetic interference radiating and conducting from a PC is emitted over a wide frequency range with various electrical

characteristics. The interference is mostly due to the switching of signals, such as switching by clocks and buses and switching in data transmission in the electronic circuits. The radiated signals can then electromagnetically couple with emissions from nearby lines such as power lines and transmission lines. Thus relevant signal emitted by switching in the RGB signals can be contained in the radiated emission. Moreover the relevant signal in the RGB lines can also combine with the signals in power lines. That is, signals in the lines can combine with each other as crosstalk that is caused by undesired capacitive, inductive, or conductive coupling in a circuit. Thus relevant signal can be also contained in the conducted emission on the power leads. Therefore, a display image can be reconstructed by receiving the conducted emission.

Next, a system for measuring the relevant signal in the conducted emission is discussed in the following subsection.

2.1. Fundamental Investigation of a LISN

The conducted emission on the power leads of electrical equipment has been generally measured using a pair of LISNs. The LISNs can be used to stably measure the conducted emission, blocking off external noise from the power source. However, the measurement frequency region is commonly lower than 30 MHz for compliance testing in accordance with international standards such as those of the IEC and the Comité International Spécial des Perturbations Radioélectriques (CISPR). Our measurement system requires the LISNs to operate in a frequency region higher than 30 MHz because the present study aims to measure the relevant signal in conducted emission at frequencies higher than 30 MHz.

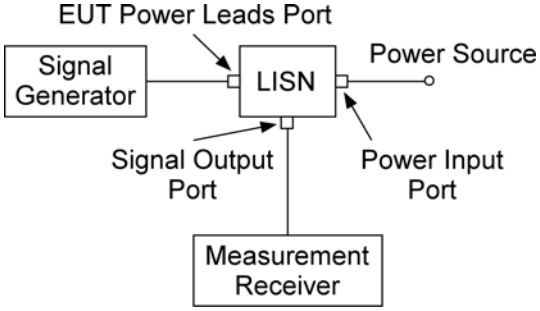

Figure 1. System block configuration for measuring the frequency response of an LISN.

We first investigated the frequency response of three LISNs to 1000 MHz. The first and second LISNs are the KNW-242C and KNW-407 manufactured by Kyoritsu Corporation. They are designed to measure the general electromagnetic interference on the power leads and are specified as having a usable frequency range between 9 kHz and 30 MHz and between 450 kHz and 30 MHz, respectively. The third is the FCC-LISN-5-50-1-T manufactured by Fischer Custom Communications, Inc. It is designed to be used in the frequency range between 100 kHz and 1000 MHz. Figure 1 shows the system block configuration for measuring the frequency responses of the LISNs [10]. A signal generator was connected to the equipment under test (EUT) power lead port of the LISN. A measurement receiver was connected to the signal output port of the LISN. The power input port of the LISN was opened. The signal generator injected an input signal level of −10 dBm in the frequency range from 1 to 1000 MHz, and the measurement receiver measured the level of the injection signal. Note that the connection line between the LISN and the measurement receiver was made as short as possible to reduce its influence.

The measurement results for each LISN are shown in Figure 2. In the figure, the horizontal and vertical axes indicate the received frequency and level, respectively. White rectangles, white triangles, and black diamonds represent the measurement levels for the KNW-242C, KNW-407, and FCC-LISN-5-50-1-T, respectively. The measurement levels show the capacitor coupling level in the LISN for the input signal level of −10 dBm. Although the KNW-242C and KNW-407 had almost flat frequency responses to about 60 MHz, the responses tended to fluctuate and decline overall above 60 MHz. These tendencies are attributed to the impedance matching for frequencies

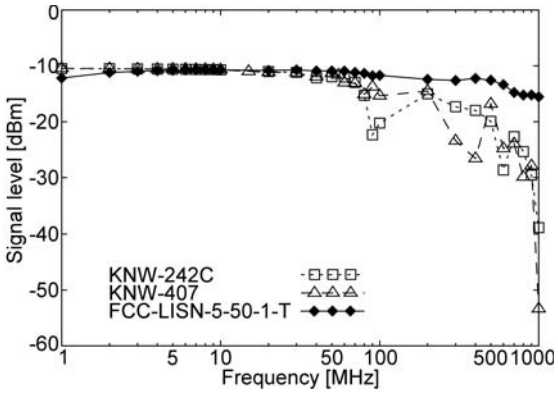

Figure 2. Measurement results of the frequency response of each LISN for the input signal.

lower than 30 MHz, and the impedance resonance for frequencies higher than 30 MHz. In comparison, the FCC-LISN-5-50-1-T had an almost flat frequency response to 1000 MHz, with the response tending to fall slightly by about 5 dBm. The tendency is attributed to impedance matching for frequencies higher than 30 MHz; for such impedance, a 5 μH inductor was used rather than a commonly-used 50 μH inductor. Therefore, the FCC-LISN-5-50-1-T can be used in our measurement system for conducted emission to 1000 MHz. A measurement system is now presented for investigating the relevant signal in the conducted emission on the power leads of a PC using the FCC-LISN-5-50-1-T.

2.2. Development of Measurement System

Figures 3(a) and (b) show the system block configuration and the setup configuration of the measurement system for the relevant signal in the conducted emission on the power leads of a PC, respectively. They are based on general electromagnetic interference measurement systems [10–12] and our previous studies [7–9]. Note that a pair of FCC-LISN-5-50-1-T LISNs is used.

The power leads of a target PC were connected to a power source through each LISN. One LISN was then terminated to 50 Ω and the other was connected to measurement receiver 1. Measurement receiver 1 was a FSET22 test receiver manufactured by Rohde & Schwarz. The receiver was set to the zero-span mode and had a resolution bandwidth (RBW) and a video bandwidth (VBW) of 50 MHz. Note that the RBW and VBW were set wide to receive the relevant signal because the signal is pulse-like with a wide spectrum. Measurement receiver 1 can receive the conducted emission of the PC at a receiving frequency with a bandwidth of 50 MHz. The video output signal of measurement receiver 1 was input to measurement receiver 2. Note that the video output port outputs the baseband signal of the conducted emission observed at the receiving frequency for the bandwidth. Measurement receiver 2 was a R3477 signal analyzer manufactured by Advantest. The receiver was set to the frequency of the relevant signal with a span of 1 MHz, an RBW and VBW of 10 kHz, an attenuation of 0 dB, a sweep time of 20 s for 1001 measurement points, an average number of sweeps of 256, and positive peak detection. Here, the span was set to detect the relevant signal. Note that at a certain receiving frequency, a measurement point should be observed for a period longer than the refresh rate of the PC monitor, which is one period of the cycle of the RGB signals. Thus, measurement receiver 2 can detect and measure the relevant signal in the conducted emission, which was received at the receiving frequency with the bandwidth of 50 MHz by measurement receiver 1. Note that the frequency of the relevant signal is briefly

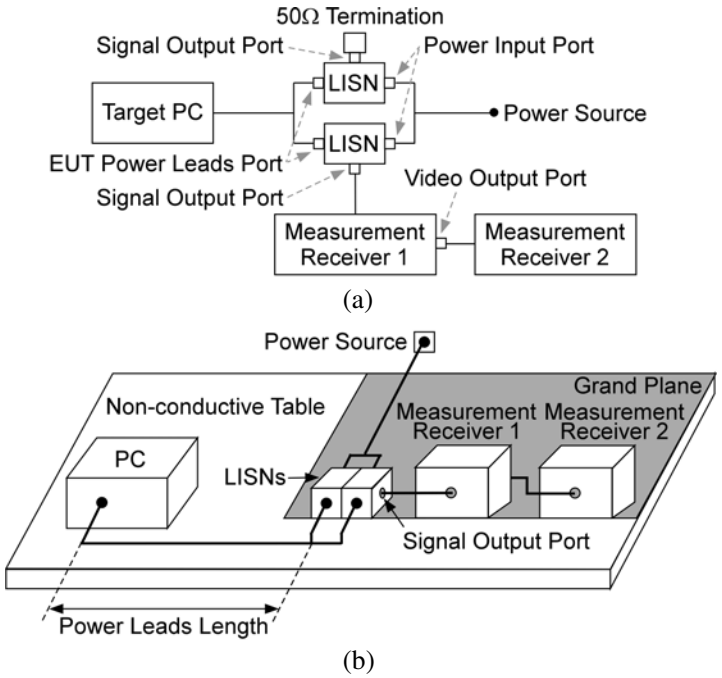

Figure 3. System for the measurement of the relevant signal in the conducted emission on the power leads of a PC, (a) system block configuration, (b) setup configuration.

reviewed in the Appendix. In the next section, the relevant signal in the conducted emission will be investigated in detail on the basis of test experiments.

3. MEASUREMENT OF RELEVANT SIGNAL

Test experiments were carried out to measure the relevant signal in the conducted emission on the power leads of three PCs using the measurement system shown in Figure 3(b). The PCs were standard notebook PCs. Their display resolutions and refresh rates were all set to 1024×768 pixels and 60 Hz, respectively. The PCs displayed vertical white and black stripes with widths of 16 pixels. Thus, the frequency of the relevant signal was calculated as 4.025 MHz (see the appendix).

3.1. Detection Results of Relevant Signal

First, we investigated the relevant signal of PC (a) to check the validity of the measurement system outlined in Figure 3(b). Measurement receiver 2 was then set to the center frequency of 4 MHz with a span of 1 MHz. The test image shown in Figure A1 and an all black image were used to confirm the detection of the relevant signal. When PC (a) displayed the test image, the relevant signal of 4.025 MHz might be contained in the conducted emission. However, when PC (a) displayed the black image, the relevant signal of 4.025 MHz is not contained in the conducted emission.

Figures 4(a), (b), and (c) show results for the relevant signal measured by measurement receiver 1 at receiving frequencies of 300, 350, and 700 MHz, respectively as typical results. Note that a shift in the receiving frequency resulted in a shift in the receiving frequency band of 50 MHz. In the figures, the horizontal and vertical axes are the detection frequency and level for measurement receiver 2, respectively. The solid and dashed lines show the results when displaying the test image and the black image, respectively.

As shown by the solid lines in Figure 4, for all receiving frequencies when the test image was displayed, the largest peak was detected at 4.025 MHz. This peak was largest for the receiving frequency of 350 MHz. The experimental results presented in Figure 4 reveal that the relevant signal level in the conducted emission depended on the receiving frequency. In addition, regarding Figure 4(b), the sidelobe signals around 4.025 MHz are thought to be frequency components in the pulse-like waveform of the relevant signal. Sidelobe signals around 4.025 MHz at the receiving frequencies of 300 MHz and 700 MHz in Figures 4(a) and (c) were not observed because the peak at 4.025 MHz was small.

On the other hand, as shown by the dashed lines in Figure 4 for the display of the black image, there was no distinct peak at 4.025 MHz for any of the receiving frequencies. Since some peaks are common with those for the solid lines, they are attributed to signals other than the signal emitted by the switching of the RGB signals in the display region.

The results presented in Figure 4 confirm that the developed measurement system can detect the relevant signal in the conducted emission at the receiving frequency. Moreover, it is revealed the relevant signal can combine with the power lead signal by complex electromagnetic coupling in the circuits of the PC.

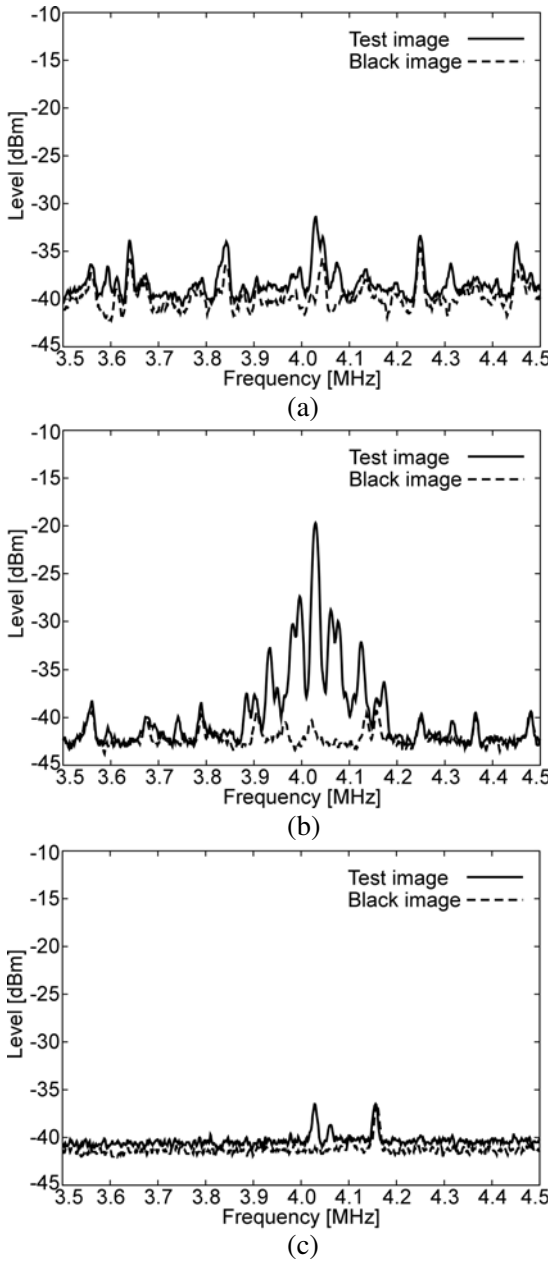

Figure 4. Detection results for the relevant signal at three receiving frequencies of (a) 300 MHz, (b) 350 MHz, and (c) 700 MHz.

3.2. Measurement Results for the Relevant Signal

The signal-to-noise ratio is taken into account to evaluate the relevant signal in the conducted emission quantitatively [8]. The "signal" is the relevant signal at 4.025 MHz when the test image is displayed. The "noise" is the signal at 4.025 MHz when the black image is displayed.

For experimental measurements, three notebook PCs manufactured by different companies were tested. Here the receiving frequency of measurement receiver 1 was changed from 50 MHz to 1000 MHz in 50 MHz steps because the RBW was set to 50 MHz. Figure 5 shows the measurement results. The horizontal and vertical axes indicate the receiving frequency and the level of the relevant signal taking account of the signal-to-noise ratio. The solid line with white diamonds, the short-dash line with white rectangles, and the long-dash line with black triangles show the measurement results for PCs (a), (b), and (c), respectively.

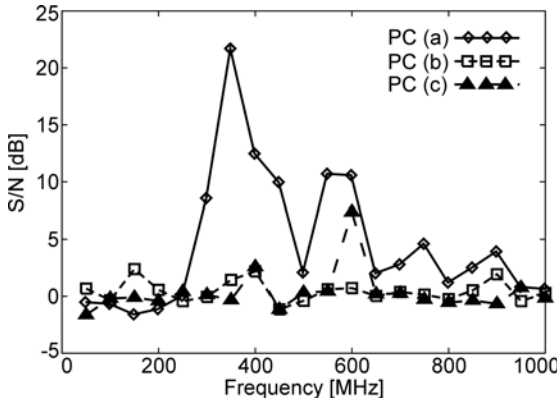

Figure 5. Measurement results for the relevant signal using the signal-to-noise ratio.

As shown in Figure 5, the relevant signal level for PC (a) varied greatly according to the receiving frequency, with the difference being about 20 dB. The peak level was 21.77 dB at the receiving frequency of 350 MHz. The relevant signal level for PC (b) was weaker than that for PC (a), although the peak was detected at the receiving frequency of 600 MHz. In comparison, the relevant signal level for PC (c) was almost flat within ± 2.5 dB. Since the relevant signal level is found to depend on the receiving frequency and the PC used, it is thought the difference can be used in evaluating information leakage of the display image due to conducted emission. Our measurement system can evaluate quantitatively the information leakage threat due to the

conducted emission on the power leads of the PC.

Additionally, the possible ways to protect the information leakage would be expected from Figures 4 and 5. For examples, a low-pass or band elimination filter mounted on the power leads will be valid. Further, an emitter that can inject the anti-phase signal with the relevant signal or the noise signal into the power leads will be also valid. These protection methods need to discuss on the effectiveness.

In the next section, sample images are reconstructed from the conducted emission and compared with the measured relevant signal levels. Finally, a suitable PC for the security issue would be able to be chosen from the evaluation result.

4. RELEVANT SIGNAL LEVELS AND RECONSTRUCTED IMAGES

The quality of reconstructed images due to the conducted emission on the power leads was evaluated using a sample image on PC (a). Measurement receiver 2 in Figure 3 was then substituted with a PC with an image processing board for analysis [7–9]. The PC used a Framecontrol image processing software developed by SystemWare, Inc.

Figure 6(a) shows a mixed image of text and picture displayed on PC (a) that was used in determining the clarity of the reconstructed image. Figures 6(b), (c), and (d) show the reconstructed images at receiving frequencies of 300, 350, and 750 MHz, respectively. The reconstructed image was then processed by averaging of 256 times. The figures suggest the display image might be successfully reconstructed by receiving the conducted emission on the power leads of PC (a). The quality also depends on the receiving frequency. The text and picture can be vaguely seen for a receiving frequency of 300 MHz (Figure 6(b)), can be clearly recognized for a receiving frequency of 350 MHz (Figure 6(c)), and are unrecognizable for a receiving frequency of 700 MHz (Figure 6(d)). The quality of reconstructed images is thought to depend on the level of the relevant signal in the conducted emission.

Next, the reconstructed images are compared with the relevant signal levels in Figure 5. It is found that the reconstructed images at 300, 350, and 700 MHz have relevant signal levels of 8.64 dB, 21.77 dB, and 2.87 dB, respectively. As compared with them, the relevant signal level seems to correlate with the quality of the reconstructed image, although the quality of a reconstructed image cannot be quantitatively evaluated in a visual manner.

In consequence, the visibility or legibility of a reconstructed image,

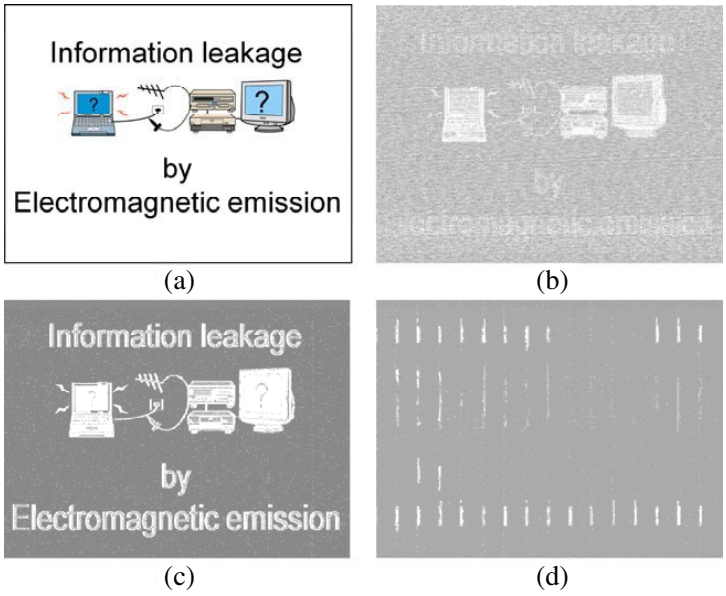

Figure 6. Comparisons between the display image and reconstructed images at three receiving frequencies; (a) display image, (b) reconstructed image at 300 MHz, (c) reconstructed image at 350 MHz, and (d) reconstructed image at 700 MHz.

which might be expressed as the quality, is shown to depend on the receiving frequency. In addition, our measurement level of the relevant signal is also shown to depend on the receiving frequency. From the comparison, our measurement system seems to work well in evaluating the quality of a reconstructed image. Thus the measurement system can be used in evaluating information leakage of a display image on a PC due to conducted emission on the power leads.

5. CONCLUSION

We developed a system for the measurement of an relevant signal emitted by the switching of RGB signals and contained in the conducted emission. The relevant signal can be used to reconstruct the display image from the conducted emission on the power leads of a PC using frequencies higher than 100 MHz. The measurement system comprises a pair of LISNs that can be used in a wide frequency range between 1 and 1000 MHz, and is based on general measurement systems for conducted emission. Relevant signals in conducted emissions were

experimentally investigated for three PCs at receiving frequencies between 50 MHz and 1000 MHz, taking account of the signal-to-noise ratio. The results showed that the measurement level depended on the PC and receiving frequency. It is thought that the differences can be used to evaluate the information leakage of a display image due to conducted emission. Therefore, display images were reconstructed from the conducted emission at different receiving frequencies. The measured relevant signal levels were compared with the quality of the reconstructed images at the same receiving frequency, and a correspondence was found.

In summary, the measurement system works well for the quantitative measurement of the relevant signal in the conducted emission on the power leads of a PC. The measurement system can be used in evaluating the information leakage of a display image because the measured relevant signal level correlates with the quality of the reconstructed images, which depends on the individual PC and the receiving frequency.

ACKNOWLEDGMENT

The authors would like to thank members of the Electromagnetic Research Center of the National Institute of Information and Communications Technology for the use of equipment. This research was partially supported by a Grant-in-Aid for Young Scientists (B) (18760292, 2006) from the Ministry of Education, Culture, Sports, Science and Technology, Japan.

APPENDIX A. FREQUENCY OF THE RELEVANT SIGNAL

In our previous studies, the relevant signal has been defined as the signal due to the switching ON/OFF of the RGB signals in the PC monitor. The relevant signal is also emitted by conduction, radiation, or both [7–9]. Note that ON/OFF represents the change in analogue RGB signals. To distinguish the relevant signal from many other electromagnetic emission signals, we have devised a way to give it a specific frequency characteristic by periodically iterating the ON/OFF of the RGB signals. The iteration then displays an image of white and black vertical stripes on the PC monitor. That is, the display image of the vertical stripes gives the relevant signal the iteration frequency component.

The frequency of the relevant signal generated from the iteration can be calculated from the width of the vertical stripes and the display

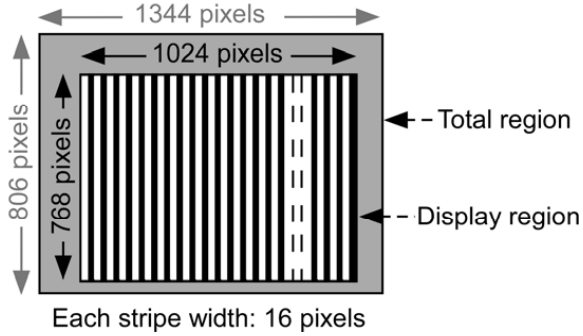

Figure A1. Test image.

resolution and refresh rate of the PC monitor. As an example, the display resolution and refresh rate are set to 1024×768 pixels and 60 Hz, respectively. Note that the correct total display resolution and refresh rate are 1344×806 pixels and 59.446 Hz, respectively [13]. The vertical stripes have widths of 16 pixels as shown in Figure A1 as a test image. There are then 64 ON/OFF switchings of the RGB signals on a horizontal line. Thus the frequency of the relevant signal can be calculated for 4.025 MHz using

$$\begin{aligned} Is &= \frac{(1344 \times 806)\ [\text{pixels}] \times 59.446\,[\text{Hz}]}{16\,[\text{pixels}]} \\ &\approx 4.025\,[\text{MHz}]. \end{aligned}$$

Accordingly, the relevant signal for 4.025 MHz can be detected in the electromagnetic emission. Note that the actual frequency may be shifted slightly, depending on the real specifications of elements such as resistors and capacitors in the electrical circuit.

REFERENCES

1. ISO/IEC 27001, "Information technology-security techniques-information security management systems-requirements," International Organization for Standardization and International Electrotechnical Commission, International Standard, 2005.
2. ISO/IEC 27002, "Information technology — security techniques — code of practice for information security management," International Organization for Standardization and International Electrotechnical Commission, International Standard, 2005.

3. X.1051, "Information security management system — Requirements for telecommunications (ISMS-T)," Telecommunication Standardization Sector of the International Telecommunication Union, International Standard, 2004.
4. RFC2828, "Internet security glossary," Internet Engineering Task Force, 2000.
5. Van Eck, W., "Electromagnetic radiation from video display units: An eavesdropping risk?," *Computers and Security*, Vol. 4, No. 4, 269–286, 1985.
6. Kuhn, M .G. and R. J. Anderson, "Soft tempest: Hidden data transmission using electromagnetic emanations," *Proc. of the Second International Workshop on Information Hiding*, Portland, USA, April 1998.
7. Sekiguchi, H. and S. Seto, "Proposal of an information signal measurement method in display image contained in electromagnetic noise emanated from a personal computer," *Proc. of IEEE Conf. on Instrumentation and Measurement Technology*, Victoria, Canada, May 2008.
8. Sekiguchi, H. and S. Seto, "Measurement of radiated computer RGB signals," *Progress In Electromagnetics Research C*, Vol. 7, 1–12, 2009.
9. Sekiguchi, H. and S. Seto, "Evaluation method of information leakage for display image reconstructed from electromagnetic noise of personal computer," *Proc. of 2008 IEEJ Symposium*, No. 1-S2-9, 25–28, 2008 (in Japanese).
10. MIL-STD-461E, "Requirements for the control of electromagnetic interference characteristics of subsystems and equipment," Department of Defense, Interface Standard, 1999.
11. IEC 61000-6-3, "Electromagnetic compatibility (EMC) — Part 6-3: Generic standards — Emission standard for residential, commercial and light-industrial environments," International Electrotechnical Commission, 1996.
12. CISPR 22, "Information technology equipment — radio disturbance characteristics — limits and methods of measurement," International Electrotechnical Commission, 1997.
13. *Monitor Timing Specifications*, Version 1.0, Revision 0.8, Video Electronics Standards Association, 1998.