Measurement System of Information Signal in Display Image leaking from Conducted Emission on Power leads of a Personal Computer

Hidenori Sekiguchi[#1], Shinji Seto[#2]

[#]*Security Fundamentals Group, Information Security Research Center,*
National Institute of Information and Communications Technology
4-2-1 Nukuikitamachi, Koganei, Tokyo 184-8795, Japan

[1]hide@nict.go.jp

[2]setos@nict.go.jp

***Abstract*—In the present study, we developed a measurement system of the information signal related with the display image in the conducted emission on the power leads of a PC. The information signal has been defined as the signal emitted by the change of the RGB signals that produces the display image, and measured using the signal-to-noise ratio in our previous studies. The measurement system was composed of a pair of line impedance stabilization networks and two receivers. In order to check the validity of the measurement system, test experiments were carried out to measure the information signal. In addition, the reconstructed image was produced from the same conducted emission. The comparison results revealed that the measured S/N level correlated with the quality of the reconstructed images.**

Key words: personal computer, power leads, conducted emission, display image, information leakage, security

I. INTRODUCTION

In information society, information security is a very important issue. An information leakage problem is one of the topics. Before now, it has been reported that the image displayed on a personal computer (PC) can be reconstructed from the reception signal of the radiated and conducted emission from itself [1] - [4]. This means there is a potential security risk of an information leakage due to unintentional electromagnetic emissions from a PC. Therefore, the evaluation of the information leakage becomes an important task.

We have been researching the evaluation method of the information leakage of the display image caused by the electromagnetic noise emitted from a PC [4]. In the present study, we focus the system development for measuring the information signal related with the display image in the conducted emission on the power leads of a PC.

Generally, the conducted emission on power leads of electrical equipments has been measured at frequencies lower than 30 MHz [5], [6]. However, we have found that some of the conducted emission higher than 100 MHz has contained the information signal that can make up the reconstructed image. In addition, the quality of the reconstructed images has depended on the receiving frequency.

Based on these findings, we develop a measurement system of the information signal in the conducted emission at the operation frequencies. As the measurement technique in our previous studies, a specific vertical stripes pattern is used as the test image on a PC. Then, the information signal has a specific frequency component of the stripes pattern [4]. To measure the information signal in the conducted emission, the measurement system is used a pair of line impedance stabilization networks (LISNs) and two receivers. The LISNs can be used to 1000 MHz. The first receiver is used to receive the conducted emission on power leads using a pair of the LISNs. The second receiver, which was connected to the video output of the first receiver, is used to measure the information signal with the specific frequency component contained in the conducted emission. Then, the signal-to-noise ratio (S/N) of the information signal is measured by test measurements. In addition, the reconstructed image is produced from the reception signal of the same conducted emission. Finally, they are compared for checking the validity of the measurement system.

II. INFORMATION SIGNAL MEASUREMENT

A. Measurement method

In our previous studies, the information signal has been defined as the signal emitted by the switching ON/OFF of the RGB signals in the PC monitor. Naturally, the information signal becomes a pulse-like-waveform, because the direct current component is not emitted. Note that ON/OFF represents the change in analogue RGB signals. However, the electromagnetic noise of a PC contains many electromagnetic emission signals. In order to distinguish the information signal from many other electromagnetic emission signals, we give it a specific frequency component 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 as shown in Fig.1. Then, the frequency of the information signal can be calculated from the iteration width, the display resolution, and the refresh rate of the PC monitor.

For example, the display resolution and the refresh rate are set to 1024 × 768 pixels and 60 Hz on the PC, respectively.

Note that the correct total display resolution and refresh rate are 1344×806 pixels and 59.446 Hz, respectively [7]. If the vertical stripes are 16 pixels, the frequency of the information signal is 4.025 MHz [4].

B. Measurement system

Fig.2 shows the measurement system of the information signal in the conducted emission of the power leads of a PC. Note that the setting configuration was based on the conducted emission measurement of the measurement standard [6]. The measurement system was used a pair of LISNs and two receivers. The LISN was placed between the alternating current (AC) adaptor of the PC and the power source. The first receiver (Receiver-1) was used to receive the conducted emission on power leads using the LISNs. The second receiver (Receiver-2) received the baseband signal of the conducted emission from the video output of the Receiver-1. The information signal can be then detected in the baseband signal.

Here, the LISNs were a FCC-LISN-5-50-1-T manufactured by Fischer Custom Communications, Inc, and were covering the wide frequency range from 0.1 to 1000 MHz. Fig.3 shows the frequency response of the LISN when a signal generator injected an input signal level of −10 dBm in the frequency range from 1 to 1000 MHz. The horizontal and vertical axes are the frequency and level, respectively. The dots show the level for each input signal. From the result, it can be confirmed that the LISN has an almost flat frequency response within about 5 dBm to 1000 MHz.

The Receiver-1 was a FSET 22 manufactured by ROHDE & SCHWARZ. We set up it to the mode: zero-span, resolution-bandwidth (RBW) and video-band-width (VBW): 50 MHz, sweep time: 5 ms, and reference level: -83 dBm, respectively. The wider RBW was usable to detect the information signal with a pulse-like-waveform, which has wider and higher frequency components. Then, the video output was the baseband signal at the receiving frequency with a spectrum band, which can set up by the RBW.

The Receiver-2 was a R3477 manufactured by ADVANTEST. We set up it to the observation frequency range: 3.5-4.5 MHz, RBW=VBW: 10 kHz, attenuator: 0 dB, average number: 256 times, and detector mode: maximum peak, respectively. The Receiver-2 can be stored 1001 points of data in the frequency domain. Thus, the sweep time was set to 20 s, because a measurement point needed a period longer than the refresh rate of 59.446 Hz (16.822 ms).

III. Test Measurement

The information signal of a notebook PC was measured using the measurement system in Fig.2. The display resolution and refresh rate were then set up to 1024×768 and 60 Hz, respectively. When the PC displayed the test image in Fig.1, the information signal of 4.025 MHz would be contained in the conducted emission on the power leads of the PC. However, when the PC displayed the black image, the information signal of 4.025 MHz would not be contained in the conducted emission.

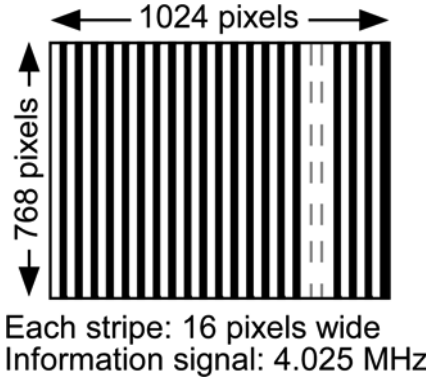

Fig.1 Test image

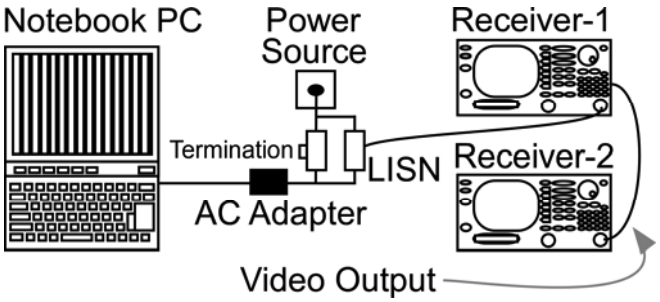

Fig. 2 Measurement system

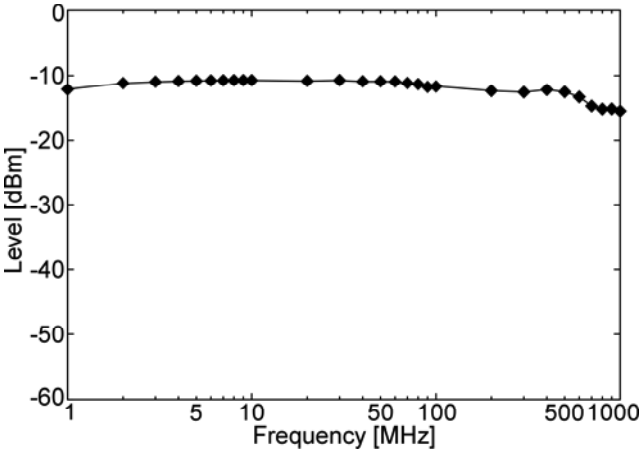

Fig.3 The frequency response of the FCC-LISN-5-50-1-T

Now, test measurements were carried out in our office environment. As the operation frequency was changed on the Receiver-1, the information signal of 4.025 MHz was detected on the Receiver-2. Fig.4 shows the typical observation result of the information signal the operating frequency 350 MHz. The horizontal and vertical axes are the frequency and the signal level detected on the Receiver-2. The solid and dashed lines are observation results when the test image and the black image were displayed, respectively. When the test image was displayed, the observation result has a biggest peak at 4.025

MHz. However, when the black image was displayed, the observation result does not have a biggest peak at 4.025 MHz. Apparently, it is found that the biggest peak is the information signal emitted by the switching ON/OFF of the RGB signals. In addition, the side-lobe signals around 4.025 MHz are thought to be frequency components in the pulse-like-waveform of the information signal.

On the other hand, the signal of 4.025 MHz detected slightly when the black image was displayed. The signal is not the information signal, but another emission signal. Therefore, the detection level of the information signal needs to be evaluated using the S/N, because many other emissions are contained in the conducted emission. In the S/N, the "Signal" is defined as the detection signal of 4.025 MHz when the test image displayed. The "Noise" is also defined as one when the black image displayed.

Next, the S/N was measured in the operation frequency from 50 MHz to 1000 MHz in steps of 50 MHz. Fig.6 shows the measurement result. The horizontal and vertical axes are the operation frequency and the level of the S/N. The dots show the measurement level for each operation frequency point. It is found that the S/N level varied greatly according to the operation frequency, with the difference being about 25 dB.

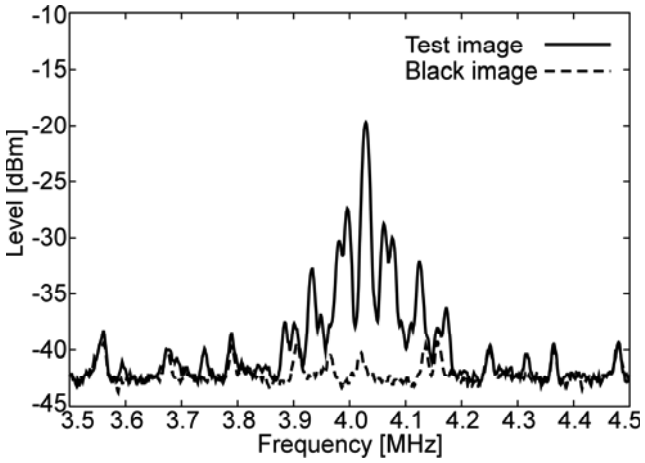

Fig.4 Detection result of the information signal at the operation frequency of 350 MHz.

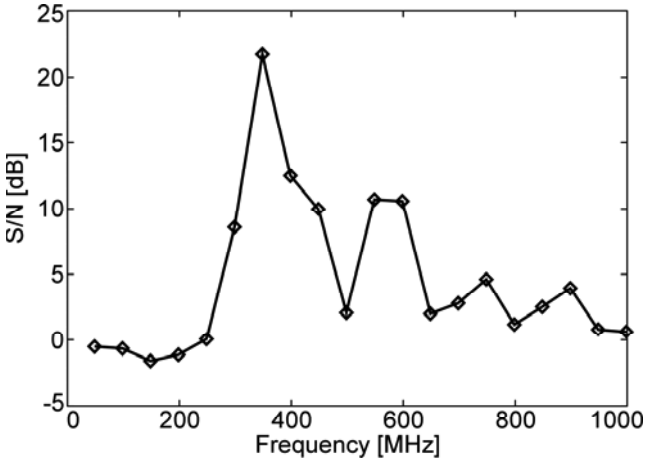

Fig.5 Measurement result of the information signal using the S/N

From the results, our measurement system seems to work well in measuring the information signal contained in the conducted emission on the power leads of a PC.

IV. Discussion on the Information Leakage

We investigated the correlation between the measurement level of the S/N and the quality of the reconstructed image. To produce the reconstructed image from the reception signal of the conducted emission on the power leads of the PC, the Receiver-2 was replaced with an analyzer PC with an image processing board in Fig.2 [4]. The video output of the Receiver-1 was then connected to the image processing board. An image processing software in the analyzer PC can produce the reconstructed image. The software was a Framecontrol manufactured by SystemWare Inc.

Fig.6 (a) shows a sample image with text and picture on the PC. Fig.6 (b), (c), and (d) show the reconstructed images at the operation frequency of 300, 350, 750 MHz, respectively. Fig.6 (b) displays slightly recognizable glyphs. Fig.6 (c) reconstructs clearly Fig.6 (a). Fig.6 (d) does not display recognizable glyphs. From these results, it can be confirmed that the display image leaks through the conducted emission on its power leads of the PC. Additionally, the clearness or visibility of the reconstructed image, which might be expressed as quality, is different depending on the operation frequency.

These reconstructed images were compared with the measurement level of the S/N for each operation frequency. The S/N levels were 8.64, 21.77, and 2.87 dB at the operation frequencies of 300, 350, 750 MHz from Fig.5, respectively. As compared with them, the quality of the reconstructed image seems to correlate with the S/N level, although the quality can not be quantitatively evaluated in a visual manner.

V. Conclusion

In this paper, we developed a measurement system of the information signal in the display image contained in the conducted emission on the power leads of a PC. From the results of test measurements taking account of the S/N of the information signal, it was shown quantitatively that the S/N level was different depending on the operation frequency. In addition, the S/N level was compared with the reconstructed image at some operation frequencies. In consequence, the S/N level seems to correlate with the quality of the reconstructed image. Therefore, our measurement system works well to evaluate the information leakage of the display image due to the conducted emission on the power leads of a PC.

Acknowledgments

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.

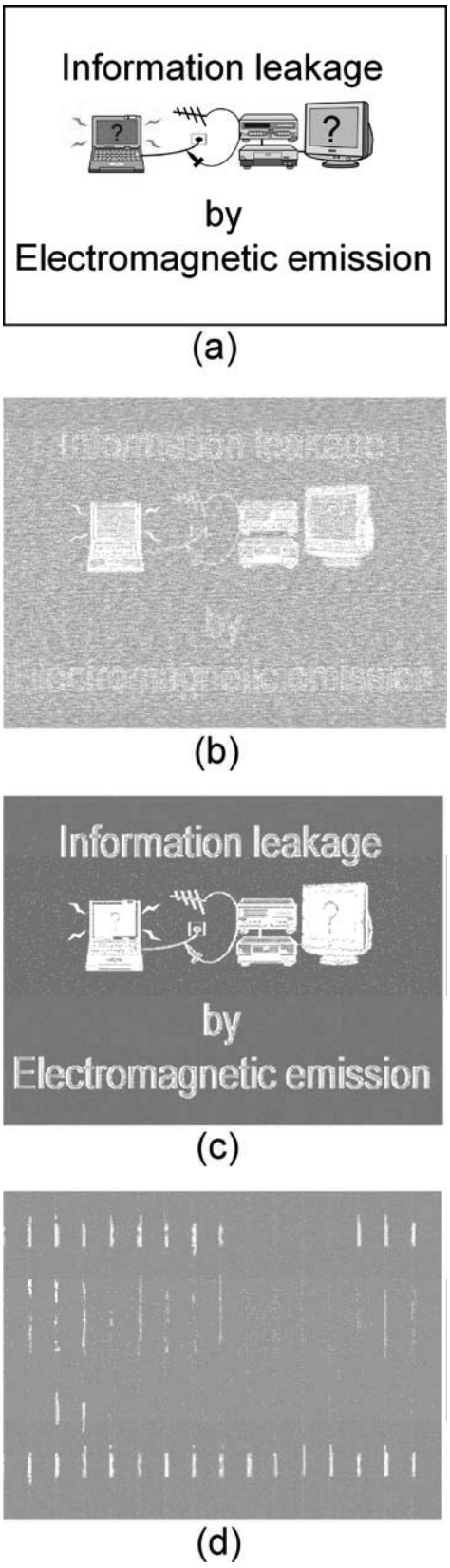

Fig.6 A sample image and reconstructed images at the differential operation frequencies, (a) sample image, (b) reconstructed image at 300 MHz, (c) reconstructed image at 350 MHz, (d) reconstructed image at 750 MHz

REFERENCES

[1] W. van Eck, "Electromagnetic radiation from video display units: An eavesdropping risk?," Computers and Security, vol. 4, pp. 269-286, 1985.

[2] M.G. Kuhn, and R.J. Anderson, "Soft tempest: Hidden data transmission using electromagnetic emanations," Springer-Verlag, Lecture Notes in Computer Science, vol. 1525, pp. 124-142, 1998.

[3] H Tanaka, O Takizawa, and A Yamamura, "A trial of the interception of display image using emanation of electromagnetic wave," Journal of the National Institute of Information and Communications Technology, Vol.52, pp. 213-223, 2005.

[4] H. Sekiguchi, and S. Seto, "Proposal of an information signal measurement method in display image contained in electromagnetic noise emanated from a personal computer," in Proc. of IEEE Conf. on Instrumentation and Measurement Technology, CD-ROM, pp. 1859-1863, May 2008.

[5] CISPR 22: Information technology equipment - Radio disturbance characteristics - Limit s and methods of measurement, INTERNATIONAL ELECTROTECHNICAL COMMISSION, 1997.

[6] MIL-STD-461E: Requirements for the control of electromagnetic interference characteristics of subsystems and equipment, DEPARTMENT OF DEFENSE, INTERFACE STANDARD, 1999.

[7] Monitor Timing Specifications, Version 1.0, Revision 0.8, Video Electronics Standards Association (VESA), 1998.