Progress In Electromagnetics Research C, Vol. 7, 1–12, 2009

MEASUREMENT OF RADIATED COMPUTER RGB SIGNALS

H. Sekiguchi and S. Seto

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

Abstract—The present study was conducted to evaluate the information leakage of the display image that can be reconstructed using the electromagnetic interference emitted from a computer. A reconstructed image was generated from the information signal that correlated with the switching of the RGB signals of the computer display. Based on this observation, a measurement method and system for the information signal was developed by displaying an image with vertical stripes. To check the validity of this measurement method and system, test measurements were carried out. The test result revealed that the information signal can be detected in the electromagnetic interference. In addition, the information signal was found to be contained in high volume between 300 and 600 MHz, depending on the receiving frequency band.

1. INTRODUCTION

Concerns about information security have increased with the growth of our computer society. Information leakage from the computers of organizations has become an important issue in security. There is a public demand for organizations to protect personal information. In order to meet this demand, information security management systems (ISMSs) are used by organizations in a systematic approach to manage their sensitive information [1, 2]. ISMS must not only assess security risks but also select appropriate controls and protections.

An electromagnetic information leakage threat exists because the transmission signal in electronic devices can be obtained maliciously from an analysis of its electromagnetic interference [3–5]. For example, it has been reported that the display image on

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

a personal computer (PC) can be reconstructed by receiving the electromagnetic interference [3, 4]. Therefore, this electromagnetic interference represents a crucial information leakage threat, because information such as the texts in the display image can be acquired from the reconstructed image. Some countermeasures to this information leakage threat have also been proposed by using inventive techniques [6–8]. The effect on the visibility of the texts in a reconstructed image has been evaluated objectively for each proposed technique. Fundamentally, the information leakage for an individual PC and the protection effect from the proposed countermeasure should be evaluated quantitatively. However, an evaluation method that can be used by anyone has not been yet developed. Therefore, the development of a quantitative evaluation method for information leakage is needed to implement ISMS.

Thus far, we have investigated a method of evaluating information leakage in relation to a reconstructed image generated from the electromagnetic interference emitted by a PC [9, 10]. In these investigations, since the quality of the reconstructed image varied depending on the receiving frequency band, the signal that could be used to generate text or pictures in a reconstructed image was measured at each receiving frequency in the electromagnetic interference. Here, we termed the signal as the information signal. The present study focuses on the measurement of the information signal by considering the signal-to-noise ratio (S/N). Next, the information signal is investigated at each frequency band in the electromagnetic interference.

2. INFORMATION SIGNAL AND S/N

The electromagnetic interference from a PC is emitted over a wide frequency range with various electrical characteristics. It is mostly generated by ON/OFF signal switching, such as by clocks, buses, data transmission, and other devices in the electronic circuits of a PC. In addition, it contains the information signal that originates from the changes in the RGB (Red, Green, and Blue) signals. Thus the display image can be reconstructed by receiving and processing this electromagnetic interference. Since the information signal is mixed with many other signals, a measurement that considers the S/N is important for its quantitative evaluation. To carry out the measurement using the S/N, the information signal and the concept of the S/N are first defined and described in detail below.

2.1. Definition of Information Signal

First, we can think of the information signal as a pulse-like-signal that is emitted by the ON/OFF switching of the RGB signals, because bigger changes in the RGB signals emit bigger pulse-like-signals [9, 10]. In addition, we have devised an information signal with a specific characteristic that can be identified in the electromagnetic interference.

Figures 1(a) and (b) show an image with vertical stripes and a text image along with the corresponding changes in the RGB signals on the red line, respectively. Generally, the RGB signals scan horizontally

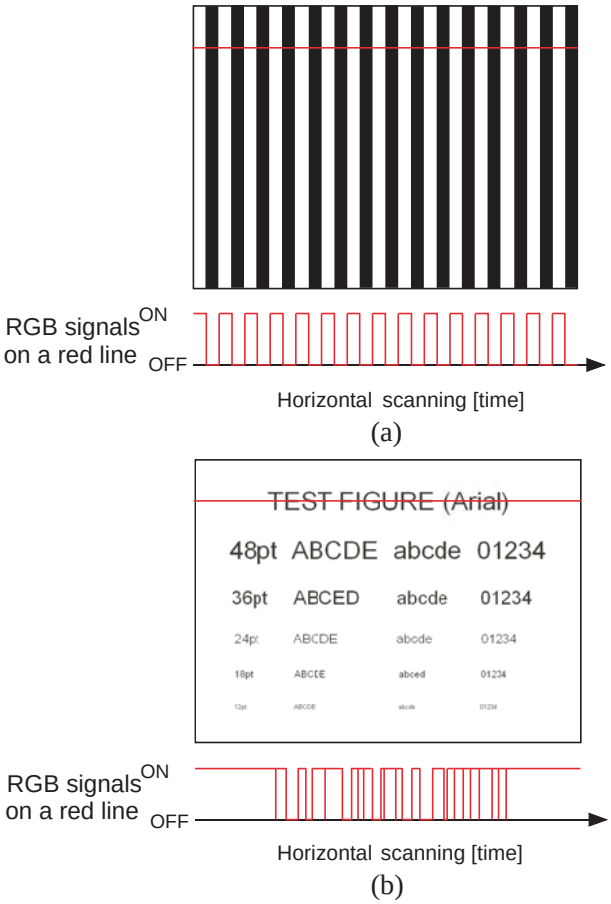

Figure 1. Correlation between display images and RGB signals on the red line, in (a) the case of an image with vertical stripes, and in (b) the case of a text image.

from the left side to the right side and from top to bottom in the computer display. Therefore, when displaying the image with vertical stripes, as shown in Fig. 1(a), the RGB signals switch periodically in the time domain. In contrast, when displaying the text image, as shown in Fig. 1(b), the RGB signals switch with different patterns according to the scanning line. Based on this observation, we displayed an image with periodic white and black vertical stripes on the computer display, as shown in Fig. 1(a). The information signal then takes on the specific frequency component by periodically switching the RGB signals. Thus, it can be identified in the electromagnetic interference.

Now, let us use an image with periodic 8-pixel wide vertical stripes as a test image. The frequency switching of the RGB signals can be calculated from the stripe width of 8 pixels and the display setting parameters of the computer display. It is also the same as the information signal. As an example, the display setting parameters were set to a display resolution of 800×600 pixels and a refresh rate of 60 Hz. Note that the display setting parameters can be selected from the display properties in the case of Microsoft Windows operating systems. The total number of pixels and the exact refresh rate for the computer display were 1056×628 pixels and 60.317 Hz, respectively [11]. Hence, the specific frequency I_s of the information signal can be determined by the following equation using the total pixels and the exact refresh rate:

$$I_s = \frac{\text{total pixel} \times \text{refresh rate}}{\text{width of each stripe}}. \tag{1}$$

Thus, I_s is calculated as follows:

$$I_s = \frac{(1056 \times 628) \times 63.317}{8} \approx 5\,\text{MHz}. \tag{2}$$

2.2. Definition of S/N

The S/N is defined to quantitatively measure the information signal, which is mixed with a lot of other signals. The S is defined as the information signal with the specific frequency I_s, when the RGB signals switch periodically to display an image with periodical vertical stripes. The N is defined as the signal with the same frequency as I_s, that exists when the RGB signals do not switch in the display region of the computer monitor when displaying a black image. Briefly, S and N represent signals with the same frequency in the cases of the image with periodic vertical stripes and the black image, respectively. From this definition of S/N, the information signal S that is emitted by switching the RGB signals can be identified. Therefore, in the next section, the

information signal S in the radiated electromagnetic interference of a PC will be investigated and discussed based on the test measurements.

3. MEASUREMENT OF INFORMATION SIGNAL AND S/N IN RADIATED ELECTROMAGNETIC INTERFERENCE

The information signal S was detected at several frequency bands in the radiated electromagnetic interference of a PC. Figs. 2(a) and (b) show a system block configuration and the actual measurement system used to detect the information signal S.

In Fig. 2(a), the radiated electromagnetic interference emitted from a PC is first picked up by an antenna and received by a receiver. The video output port of the receiver outputs the video output signal. Note that the video output signal might be called the base band signal. The video output signal is an amplitude demodulated signal observed in the receiving band width at the receiving frequency. The video output signal is then input to a band-pass filter that passes the information signal S with the frequency I_s. Eventually, the level meter measures only the information signal S contained in the receiving frequency band.

Figure 2(b) shows the measurement system, which used two receivers to actualize the system block configuration shown in Fig. 2(a). The first receiver in Fig. 2(b) became the receiver in Fig. 2(a). The

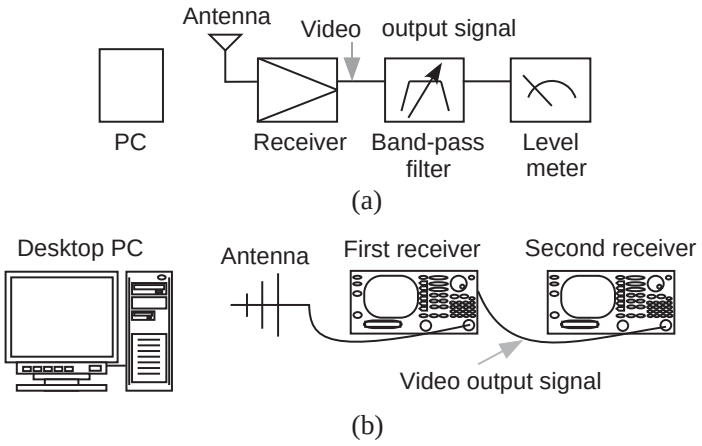

Figure 2. (a) System block configuration and (b) measurement system to detect the information signal in the radiated electromagnetic interference of a PC.

second receiver in Fig. 2(b) substituted for the band-pass filter and level meter in Fig. 2(a). The resolution band width (RBW) of the second receiver served as the band-pass filter. The second receiver performed a frequency sweep and detected the information signal S with the frequency I_s. The value at the frequency I_s on the second receiver served as the level meter. Thus, this measurement system could measure the information signal S in the receiving frequency band that was operated by the receiving frequency and the RBW of the first receiver.

Measurement setups were performed for a standard desktop PC, which was used as the equipment under test (EUT). The display setting parameters and the test image were the same as those discussed in the previous section. Then, the PC radiates the electromagnetic interference. It also contains the pulse-like-signal emitted by the ON/OFF switching of the RGB signals in the computer monitor. Practically, the pulse-like-signal can be observed as a damped sinusoidal waveform with a width as shown in Fig. 3, because a real measurement system has an inductance component. Therefore, if the width of the vertical stripes becomes narrower than that of

the observable pulse-like-signal, the following pulse-like-signal arises before the last pulse-like-signal is steady to zero. In the measurement environment of Fig. 2, when the stripe width is 8 pixels, the pulselike- signal can be detected exactly. Thus, the frequency I_s of the information signal S was about 5 MHz from Eq. (2).

The antenna was a log-periodic antenna that was usable in the frequency range of 80 to 1000 MHz and was located at a distance of 1 m from the front of the EUT in a compact anechoic chamber. The first receiver was the test receiver FSET22 manufactured by ROHDE

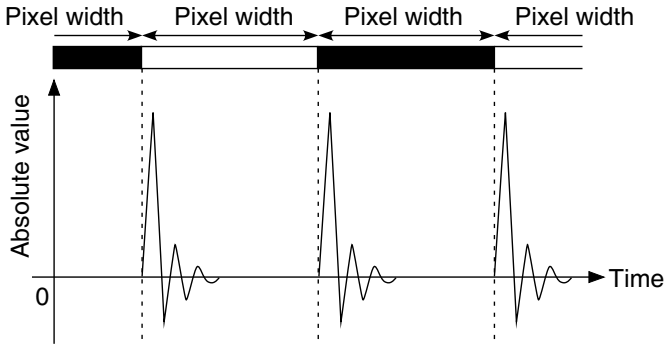

Figure 3. Waveform of observable pulse-like signals.

& SCHWARZ. This was set to the zero-span mode, with an RBW and video-band-width (VBW) of 100 MHz. Note that the RBW and VBW were wide to receive the information signal S, which was a pulse-like-signal with wide spectra. The first receiver received the radiated electromagnetic interference of the EUT at a band width of 100 MHz. The second receiver was the signal analyzer R3477, manufactured by ADVANTEST. It was set up with start and stop frequencies of 5.00 MHz and 5.01 MHz, respectively, an RBW and VBW of 10 Hz, ATT (attenuator) of 10 dB, and sweep time of 20 s, with 1001 measurement points. Here, the measurement frequency range was narrowed by a preliminary measurement that specifically searched for the information signal S with the frequency I_s. Note that one measurement point was observed during a longer time than the refresh rate, which was one cycle of the RGB signals. Thus, the second receiver could detect and measure the information signal S with the frequency I_s by performing frequency sweep.

Next, test measurements were carried out to detect the information signal S and the noise signal N, which had a frequency I_s of about 5 MHz, when displaying the test image and the black image on the computer display. Figs. 4(a), (b), and (c) show the detection results for the information signal S and the noise signal N on the second receiver at the receiving frequencies of 100, 300, and 500 MHz on the first receiver, respectively. Note that a shift in the receiving frequency implies a shift in the receiving frequency band. In these figures, the horizontal and vertical axes are the sweeping frequency and the detection level on the second receiver. The red and blue lines show the detection results for the information signal S and the noise signal N with a frequency I_s of about 5 MHz, respectively. The black line shows the system noise on the second receiver. As shown in Fig. 4, when the test image was displayed on the computer display, of all the receiving frequencies, the largest peak detected for the information signal S was at 5.0043 MHz. Its side-lobe signals were then thought to be frequency components of the waveform of the pulse-like-signal. When the black image was displayed, the noise signal N was detected at 5.0043 MHz as a small signal. The small signal was also observed in other frequencies of the second receiver, and became small when the receiving frequency of the first receiver became high. Thus, the small signal was thought to be, not the information signal S, but another signal that existed in the electronic circuit. It may be arise from the harmonics of the vertical and horizontal synchronized signals. Furthermore, the noise signal floor was higher than the system noise floor at all the receiving frequencies, and was larger than 40 dBm at the receiving frequency of 100 MHz. Accordingly, it was found that the measurement method

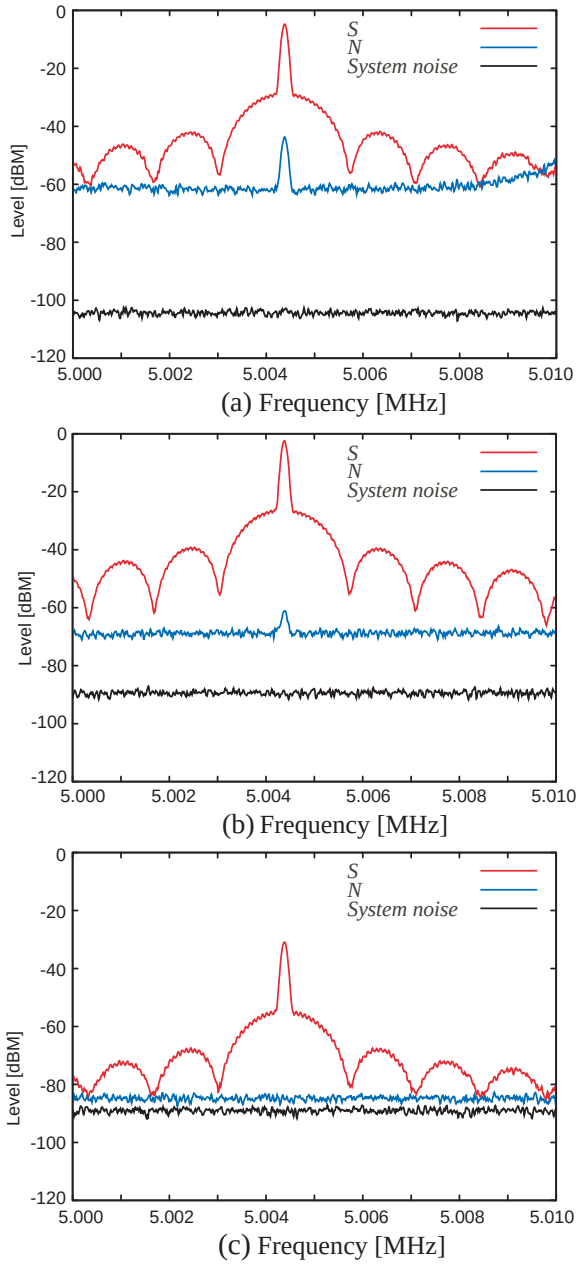

Figure 4. Detection results for the information signal S and the noise signal N for the frequency I_s of about 5 MHz on the second receiver at the receiving frequencies of (a) 100 MHz, (b) 300 MHz, and (c) 500 MHz on the first receiver, respectively.

and system could detect and measure the information signal S at the receiving frequency band in the radiated electromagnetic interference of the EUT. It was also determined that the noise signal N should be taken into account when measuring the information signal S.

Next, the information signal S and the noise signal N were measured at each receiving frequency to investigate the receiving frequency dependence. Fig. 5 shows these measurement results. The horizontal and vertical axes are the receiving frequency on the first receiver and the measurement level at 5.0043 MHz on the second receiver, respectively. The red and blue points show the measurement results for the information signal S and the noise signal N, respectively. Their levels became smaller when the receiving frequency was higher, while the difference between them varied. On the other hand, this result revealed that the information signal S was observed at all the receiving frequencies. Consequently, the S/N was investigated from Fig. 5. Fig. 6 shows the measurement results of the S/N at each receiving frequency band in the radiated electromagnetic interference. The horizontal and vertical axes present the receiving frequency and measurement level, respectively. The black points show the measurement results of the S/N. As shown in Fig. 6, the level of the S/N depended on the receiving frequency band, with the difference being about 40 dB between the receiving frequencies of 400 and 1000 MHz. As a result, in the radiated electromagnetic

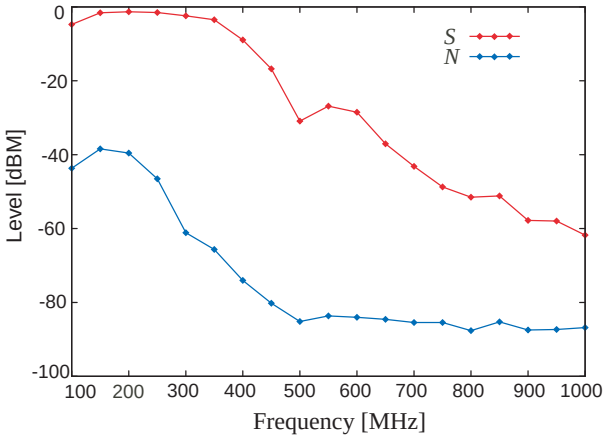

Figure 5. Measurement results for the information signal S and the noise signal N at each receiving frequency band in the radiated electromagnetic interference.

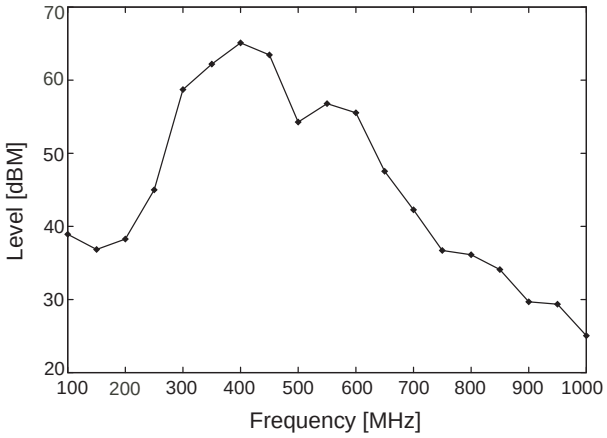

Figure 6. Measurement results for the S/N at each receiving frequency band in the radiated electromagnetic interference.

interference, the information signal S was contained in high volume in the frequency region between 300 and 600 MHz. This tendency may depend on the EUT, which contains an inherent antenna that effectively radiates the frequency band signal.

4. CONCLUSION

We experimentally investigated the information signal in detail, which can be used to reconstruct the display image from the radiated electromagnetic interference of a PC. We first confirmed that the measurement method and system could detect the information signal that was emitted by switching the RGB signals. The information signal was then measured at each frequency band of 100 MHz in the radiated electromagnetic interference. It was found to be contained in the wide frequency region between 100 and 1000 MHz. Next, the signal-to-noise ratio (S/N) of the information signal was measured at each receiving frequency band. The level of the S/N depended on the receiving frequency band. It was then shown quantitatively that the information signal was contained in high volume in the frequency region between 300 and 600 MHz of the radiated electromagnetic interference of the PC.

This measurement method and system worked well for the quantitative measurement of the information signal emitted by the switching of the RGB signal in the radiated electromagnetic

interference of a PC. Therefore, this measurement method and system can become a valid approach to quantitatively evaluate the information leakage of the display image caused by the electromagnetic interference of a PC.

ACKNOWLEDGMENT

This work was supported in part by a Grant-in-Aid for Young Scientists (B) (18760292, 2006) from the Ministry of Education, Culture, Sports, Science and Technology, Japan.

REFERENCES

1. "ISO/IEC 27002: Information technology — Security techniques — Code of practice for information security management," International Organization for Standardization (ISO) and INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC), 2005.
2. "X.1051: Information Security Management System — Requirements for Telecommunications (ISMS-T)," International Telecommunication Union — Telecommunication Standardization Sector (ITU-T), 2004.
3. Van Eck, W., "Electromagnetic radiation from video display units: An eavesdropping risk?" *Computers and Security*, Vol. 4, No. 4, 269–286, 1985.
4. Kuhn, M. G. and R. J. Anderson, "Soft tempest: Hidden data transmission using electromagnetic emanations," *Proceedings of the Second International Workshop on Information Hiding*, Portland, USA, April 1998.
5. Zhuang, L., F. Zhou, and J. D. Tygar, "Keyboard acoustic emanations revisited," *Proceeding of the 12th ACM Conference on Computer and Communications Security*, New York, USA, November 2005.
6. Kuhn, M. G., Filtered-tempest fonts, Available: http://www.c1.cam.ac.uk/mgk25/st-font.zip.
7. Beyond IT Co., Ltd., CrypType, Available: http://CrypType .com.
8. Suzuki, Y., R. Kobayashi, M. Masugi, K. Tajima, and H. Yamane, "Development of countermeasure device to prevent leakage of information caused by unintentional PC display emanations," *Proceeding of the EUROEM 2008 European Electromagnetics*, Lausanne, Switzerland, July 2008.

9. Sekiguchi, H. and S. Seto, "Proposal of information signal measurement method in display image contained in electromagnetic noise emanated from a personal computer," *Proceeding of the 2008 IEEE International Instrummentation & Measurement Technology Conference*, Victoria, Canada, May 2008.
10. Sekiguchi, H., "A measurement and evaluation method of a display image signal contained in electromagnetic emanation from a personal computer," *Transaction of IEICE*, Vol. J91–B, No. 11, 1478–1483, 2008 (in Japanese).
11. "Monitor Timing Specifications, Version 1.0, Revision 0.8," Video Electronics Standards Association (VESA), 1998.