Countermeasure Technique for Preventing Information Leakage Caused by Unintentional PC Display Emanations

Yasunao Suzuki[#1], Masao Masugi[#2], Hiroshi Yamane[#3], and Kimihiro Tajima[*4]

[#]*NTT Energy and Environment Systems Laboratories*
9-11, Midori-cho 3-chome Musashino-shi, Tokyo 180-8585 Japan
[1]suzuki.yasunao@lab.ntt.co.jp
[2]m.masugi@lab.ntt.co.jp
[3]yamane.hiroshi@lab.ntt.co.jp

[*]*NTT Research and Development Planning Department*
2-3-1 Ootemachi Chiyoda-ku, Tokyo 100-8116 Japan
[4]k.tajima@hco.ntt.co.jp

***Abstract*— A working personal computer (PC) and/or a PC display monitor usually produce unintentional electromagnetic fields. It has been known that the information from a video display unit could be reconstructed by intercepting such emissions at a distance. Proper measures are needed to prevent information leakage against such eavesdropping, which are often collectively called "TEMPEST". We have studied a countermeasure technique for such a problem and proposed jamming schemes for industrial and home use. We also developed a prototype for protecting devices and evaluated its performance in preventing such emanation eavesdropping.**

Key words: electromagnetic emission, information security, eavesdropping, TEMPEST.

I. Introduction

A. Overview

Working electronic equipment, such as information processing or communication equipment, usually emits and receives unintentional radiated electromagnetic waves. These emissions may cause interference to other equipment and often disrupts their functions. To prevent such problems, unintentional emission levels are regulated by standards in most countries. [1]

On the other hand, some of these emissions often carry significant information processed inside the equipment. This hidden information can often be reconstructed by intercepting such emissions, even if the emission levels are weak enough by those standards. This can be a potential information security threat, especially for the reason that the information can be stolen remotely from a distance with no trace.

Such a threat of information leakage from compromising emanations of a computer cathode-ray tube (CRT) display has been reported by Wim van Eck in 1985 [2]. Before his work, this kind of eavesdropping was considered very difficult, but he pointed out that the screen content of a CRT display can easily be reconstructed using a normal TV receiver and sync pulse generators.

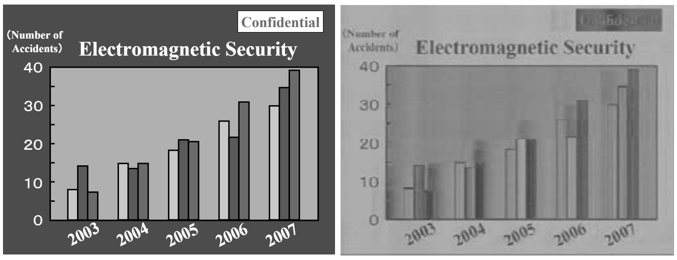
Certain military organizations have researched such emission security since around 1960 [3], but they have not made those results public. However, some US standards have recently been declassified only in excerpts [4] [5] [6] [7], but regulation limits and test methods are kept closed. The US government established a program called "TEMPEST" to study and measure against such eavesdropping on emanations [8]. This codename is now in general use and refers to this type of threat or countermeasure policy.

Recently, the need for information security has increased in military and in industrial fields. We show several conventional countermeasure methods against such eavesdropping and propose a suitable jamming scheme, especially for industrial fields and/or home use for protect information managed in a personal computer (PC). We have also studied radiation properties of a PC to produce reliable jamming signals.

B. Demonstration of leaked video signal reconstruction

Unintentional emanation from a PC contains information that is processed in the equipment. The video signal displayed on a PC monitor is usually radiated intensively compared with that of other information. In many cases, it appears in the frequency range from several tens of megahertz to several gigahertz, and it is often easy to reconstruct the original video signal by receiving and demodulating those emanations.

Figure 1 shows an example of reconstructed video information emanated from a PC at 326 MHz. We used a log-periodic antenna UHALP9107 (Schwarzbeck) and a spectrum analyzer FSET (Rohde & Schwarz) as the radio receiver in this experiment, and the receiver bandwidth was set to 20 MHz. The emanation was measured 3m from the PC in an RF anechoic chamber. A reconstructed image usually contains a large amount of random noise, which can be reduced by averaging stored video frames. In this case, thirty-two video frames were averaged. The original image on the PC monitor, Fig. 1(a), is clearly reconstructed in Fig 1(b).



(a) Original display image on PC monitor (b) Display image reconstructed from PC emanation at 326MHz (32 video frames are averaged)

Fig. 1 Example of eavesdropped display image

II. Countermeasure Schemes

A. Conventional countermeasures

There are conventional countermeasure schemes to protect information from eavesdroppers. Representative measures are listed in Table 1.

The most reliable scheme is shielding devices, rooms, and/or rarely buildings with metallic materials, which prevent radio waves from penetrating. However, this shielding scheme is usually expensive, especially for shielding rooms or buildings. It is not suitable for equipment such as a mobile PC, because it is heavy and expensive.

Inserting filters into interface cables is also effective for suppressing emissions. However, this is effective only if the emissions are radiating mainly from the interface cables.

Soft Tempest is a type of countermeasure software. It has been reported that the strength of emissions can be reduced using specifically designed fonts [9] [10].

Zoning is a policy for maintaining a certain distance from possible eavesdroppers. This enables one to choose a proper countermeasure method according to the protection level defined in each zone, which is classified in several ranks by distance between the equipment and a possible eavesdropping area.

Jamming is another countermeasure technique that intentionally overlays jamming signals, such as random noise or meaningless signals, on the original emanation in order to intercept the leaked information.

A combination of these schemes would be an effective overall countermeasure.

B. Requirement for the jamming signal

Jamming is an effective and low-cost countermeasure scheme. However, for practical use, there are some important points to consider. First, the jamming signal should be carefully chosen because it should overlap the original emanations with sufficient intensity in the entire frequency range.

Fig. 2 shows the frequency dependence of the field strength of an emanation from a PC. The experimental setup and the PC were the same as in Fig. 1. The frequency spectrum of an emanation has many peaks. There are peaks that include components of the PC display information, and they are shown with asterisks in the figure. Most of the other peaks may be generated by other kinds of signals processed in the PC.

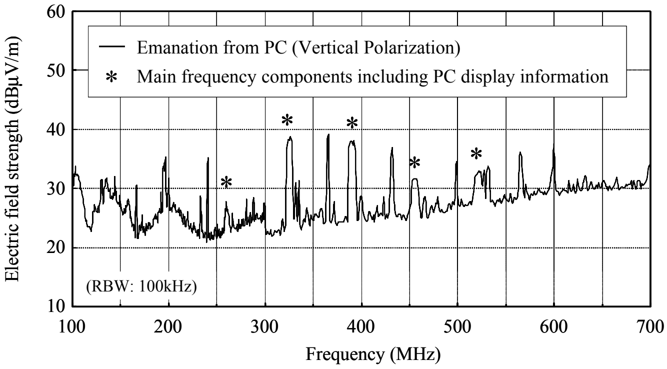


Fig. 2 Field strength of emanation from PC

For conventional analog PC video interfaces [9] [10], the video screen is constructed with pixels, which are displayed on the screen along with the scanning line. A pulse signal for determining the draw timing of the pixels is called a "dot clock" (or "pixel clock") and its frequency is about 30 to 200 MHz. In this case, the dot clock frequency is about 65 MHz with a display resolution of 1024 × 768 (XGA).

The PC video signals (red, green, and blue) are modulated periodically and synchronized with dot clock timing, and the dot clock amplitudes correspond to the video signal luminances. As a result of such pulse amplitude modulation, frequency spectra of the video signals appeared at peak harmonic frequencies of the dot clock frequency [8]. In Fig. 2, frequency peak components including PC display information (shown with asterisks) appeared at harmonic frequencies that are multiples of the dot clock frequency of 65 MHz.

Table 1 Countermeasure Schemes and their features

Countermeasure methods	Protection performance	Initial cost	Availability for mobile use	Additional appliance for pre-installed equipment
Shielding structures	High	Very High	Impossible	Hard to apply
Shielding equipment	High	High	Available but not suitable (Heavy weight)	Hard to apply
Filtering	Medium	Low	Available	Applicable
Soft Tempest	Medium	Low-Medium	Available	Applicable
Zoning	(Adaptable for each case)	Low	Difficult to apply	Applicable
Jamming	High	Low-Medium	Available	Applicable

The frequency bandwidths of the peaks that include video signal information are about 6 MHz wide, which corresponds to a frequency bandwidth of the baseband video signal.

From these experimental results, the properties required for jamming signals are clarified as follows;

- The frequency spectrum of the jamming signal should contain frequency harmonic components of dot clock frequency.
- Integrated power of the modulated signal spectrum at these frequency components are sufficiently high compared with original emanations.

Another important point is that the jamming effect of simple random noise is reduced using periodic averaging or other signal-processing techniques. The jamming signals are expected to be effective, even if those techniques are applied by eavesdroppers.

III. DEVELOPMENT OF A PROTOTYPE DEVICE

A. *Principle of proposed jamming schemes*

To countermeasure eavesdropping of PC video signals, we have studied jamming schemes suitable for industrial use or home use. [13].

We propose that a jamming device be attached to every PC. This is because the countermeasures are usually not always necessarily for all PCs used in an office or room, but limited to PCs that require special security need it. Additionally, it makes possible to apply to the PC already used and also to a mobile PCs.

The jamming signal we propose is made from video interface signals processed in a PC. Figure 3 shows a function diagram of the jamming device. First, it regenerates timing pulses of the dot clock signal from the vertical and horizontal video synchronization signals, which are part of the video interface signals. The frequency spectrum of the dot clock timing pulses contains harmonic components of the dot clock frequency, and those components strictly overlap the leaked PC video signals. Accordingly, these timing pulses obstruct eavesdropping by covering up the leakage signal if its level is sufficiently higher than that of the leaked signals.

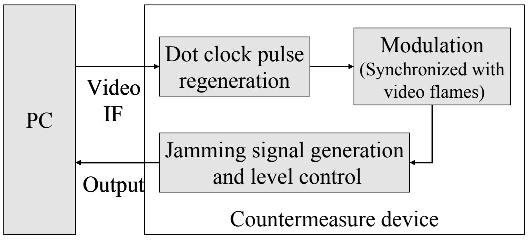

PC
Video IF
Output
Dot clock pulse regeneration
Modulation (Synchronized with video flames)
Jamming signal generation and level control
Countermeasure device

Fig. 3 Function diagram of jamming device

To produce jamming signals, the dot clock timing pulses are modulated to display a fixed pattern on the video screen if it is reconstructed from the intercepted emissions. This modulation measures periodic averaging techniques used by eavesdroppers to improve image quality. If such a modulation is random with time, its jamming effect is degraded by the periodical averaging. However, the jamming effect of the proposed modulation is effective because a fixed pattern on the video frames remains, even if they are averaged.

The power level of the jamming signal generated is controlled to comply with radio regulations, and the signal is fed into a PC as a common-mode voltage. Then the jamming signal is emitted from the PC by the same radiation mechanism as the original video signal, and the PC plays the role of an antenna in both cases.

We have developed a prototype countermeasure device to prevent information leakage from PCs. The outward appearance of the device is shown in Fig. 4. The device is connected to the video display connector on a PC to pick up video signals and to feed the jamming signal into the PC. It is powered externally from a PC USB port or a commercial AC power supply.

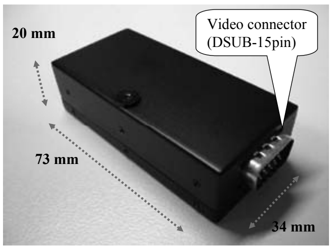


Fig. 4 Image of countermeasure device

B. *Performance evaluation*

We have experimentally confirmed the effectiveness and availability of the proposed jamming scheme using this prototype device.

The experimental results confirming the effectiveness of the jamming signal is shown in Fig. 5. It shows the intercepted and reconstructed image of the original image (Fig. 1(a)) when the countermeasure device is active. The experimental setup and conditions were the same as the case shown in Fig. 1, and 32 video frames were averaged.

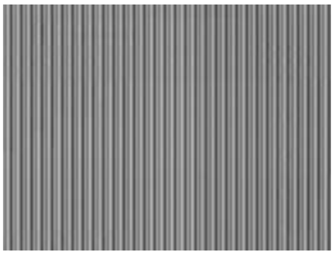


Fig. 5 Reproduced display image from PC with countermeasure device

For this prototype, we planned to display fixed vertical stripes on the eavesdropping display monitor to counteract video-frame averaging. Comparing this result with Fig. 1(b), the information of the original image disappears completely in high-contrast vertical stripe image.

An example of the frequency spectrum of an emanation from a PC, when the countermeasure device is active, is shown in Fig. 6 with the light-colored solid line. In contrast, the field strength of the original emanation from the PC is represented with the dark-colored solid line.

Note that the electric field strength of the emanation with the jamming signal from the countermeasure device is much higher than the original signal, especially at the peak frequency including the video signal information. This means that the jamming protection is effective at a wide frequency region for any PC in accordance with its video interface settings.

In addition, the regulation limit of CISPR22 classes A and B is shown in this figure. The output level of our device can be manually limited to comply with such radio regulations.

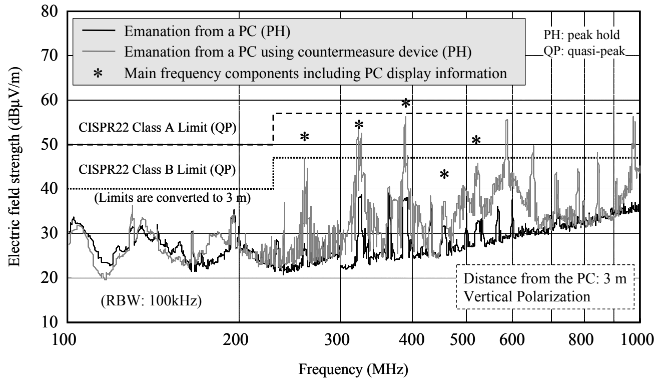
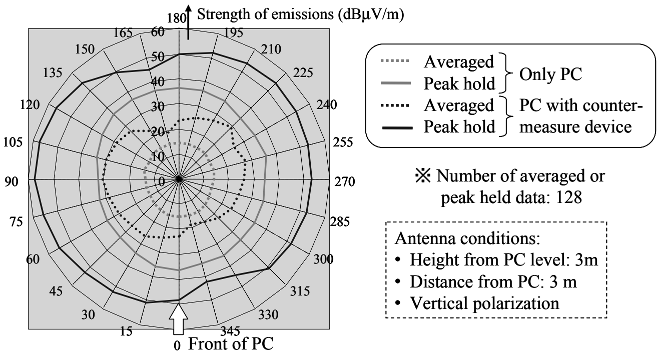


Fig. 6 Electric field strength of emanations from PC



Antenna conditions:

- Height from PC level: 3m
- Distance from PC: 3 m
- Vertical polarization

Fig. 7 Directional dependence of electromagnetic field strength

An example of a radiation pattern of the countermeasure device is shown in Fig. 7. It shows the directional dependence of the electromagnetic field strength at a 390-MHz peak.

The field strength of the emanation with jamming signal was almost isotropic and much higher than that of the emanations from a single PC in any direction from the PC's position. This means that the device effectively interfered with eavesdropping from all directions.

IV. CONCLUSION

We have proposed jamming schemes to countermeasure eavesdropping of information displayed on a PC from intercepted unintentional emanations. We also have developed a portable countermeasure device using a jamming scheme, and experimentally evaluated its performance.

The jamming signal of the countermeasure device synchronizes to the original video signal, so it is suitable for individual PCs. It is also effective on emissions of any frequency and in any direction. Moreover, it is effective even when the video-frame averaging technique is used by the eavesdroppers.

Establishing an objective index for evaluating the ability of preventing information leakage is the aim for future work.

REFERENCES

[1] CISPR22, "Information technology equipment – Radio disturbance characteristics – Limits and methods of measurement," Mar. 2006.

[2] Wim van Eck: Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? Computers & Security, Vol. 4, pp. 269–286, 1985.

[3] Rick Lehtinen, Deborah Russell, G. T. Gangemi Sr.: Computer security basics. 2nd Edition, Appendix B: TEMPEST. O'Reilly, 2006, ISBN 0-596-00669-1

[4] National Security Telecommunications and Information Systems Security Advisory Memorandum NSTISSAM TEMPEST/1-92: Compromising Emanations Laboratory Test Requirements, Electromagnetics. National Security Agency, Fort George G. Meade, Maryland, 15 December 1992. Partially declassified transcript: http://cryptome.org/nsa-tempest.htm

[5] NACSIM 5000: Tempest Fundamentals. National Security Agency, Fort George G. Meade, Maryland, February 1982. Partially declassified transcript: http://cryptome.org/nacsim-5000.htm

[6] National Security Telecommunications and Information Systems Security Advisory Memorandum NSTISSAM TEMPEST/2-95: RED/BLACK Installation Guidance. National Security Agency, Fort George G. Meade, Maryland, 12 December 1995. Transcript: http://cryptome.org/tempest-2-95.htm

[7] National Security Telecommunications and Information Systems Security Instruction NSTISSI No. 7000: TEMPEST Countermeasures for Facilities. National Security Agency, Fort George G. Meade, Maryland, 29 November 1993. Partially declassified transcript: http://cryptome.org/nstissi-7000.htm

[8] Markus G. Kuhn: Compromising emanations: eavesdropping risks of computer displays, University of Cambridge (Computer Laboratory) Technical Report Number 577, UCAM-CL-TR-577, ISSN 1476-2986, 2003: http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.html

[9] Markus G. Kuhn, Ross J. Anderson: Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations. Information Hiding, IH'98, Portland, Oregon, 15–17 April 1998, Proceedings, LNCS 1525, Springer-Verlag, pp. 124–1

[10] H. Tanaka, O. Takizawa, and A. Yamamura, "Evaluation and Improvement of the Tempest Fonts," Information Security Applications, 5th International Workshop (WISA 2004), Lecture Notes in Computer Science, Vol. 3325, Springer- Verlag, Aug. 2005.

[11] VESA Standard DMT 1.0; "Industry Standards and Guidelines for Computer Display Monitor Timing (DMT) Standard," Version 1.0, Revision 11, May 2007.

[12] VESA GTF 1.0; "Generalized Timing Formula (GTF)," Version 1.1, Revision 11, Sep. 1999.

[13] Yasunao Suzuki, Ryuichi Kobayashi, Masao Masugi, Kimihiro Tajima, and Hiroshi Yamane, "Development of Countermeasure Device to Prevent Leakage of Information Caused by Unintentional PC Display Emanations," Proc. of European Electromagnetics 2008 (EuroEM2008), Lausanne, Switzerland, 2008