Synchronization Clock Frequency Modulation Technique for Compromising Emanations Security

Takashi Watanabe[#1], Hiroto Nagayoshi[#2], Hiroshi Sako[#3]

[#]*Central Research Laboratory, Hitachi Ltd.*
1-280 Higashi Koigakubo, Kokubunji-shi, Tokyo, 185-8601 Japan
{[1]takashi.watanabe.dh, [2]hiroto.nagayoshi.wy, [3]hiroshi.sako.ug}@hitachi.com

Toshirou Uemura[*]

[*]*Hitachi-Omron Terminal Solutions, Corp.*
1 Ikegami, Haruoka-cho, Owariasahi-shi, Aichi-ken, 488-8501 Japan
toshirou_uemura@hitachi-omron-ts.com

Abstract— **The security problem of screen image leakage on a display unit through electromagnetic radiation from several meters away has attracted wide interest by security researchers since van Eck wrote about this problem. To solve the problem, techniques for reducing the S/N ratio of emanating information by signal reduction and noise generation have been proposed as countermeasures. Different from them, we investigate a technique that fluctuate frequencies of synchronization signals in display image transmission to reduce correlation between timings of display and transmission. We not only explore the most effective modulation target but also realize a real-time signal modulation unit by a FPGA board, and verified the effectiveness of the technique using a system of a PC and LCD.**

Key words: Compromising Emanation, Side-Channel Analysis, Electromagnetic Radiation, TEMPEST, EMSEC

I. Introduction

After van Eck published his paper [9] in 1985, the risk of information leakage through electromagnetic radiation from a display unit, not only cathode-ray tube (CRT) but also liquid-crystal display (LCD), has been widely known. For preventing information leakage through electromagnetic radiation, constraints and techniques have been investigated under the name of “emanations security (EMSEC)” or “TEMPEST (a nickname of specifications and not recommended to use in standard documents)”. Although little information on guidelines or requirements for TEMPEST has been unveiled, some companies have been selling TEMPEST testing devices.

Intercepting electromagnetic waves from ordinary display units required million-dollar devices a few decades ago. Although such high-end products cost the same today, lower-range products, those costing as little as thousands of dollars, are nearly capable of capturing partial information from a few meters away, which is due to improvements in radio management technologies. Furthermore, with rapid advances in software definition radio (SDR) and field programmable gate array (FPGA), the cost of information retrieval is expected to decrease to less than a thousand dollars in the near future. Because of these changes, development of low-cost countermeasures applicable to ordinary computers is required.

Countermeasures are woven to reduce the S/N ratio of leakage information and are categorized as signal reduction and noise generation. For signal reduction, smoothing functions such as a low-pass filter or Gaussian filter are applied to screen fonts and entire images [1],[4]. For noise generation, an additional noise source is placed near the sources of signal emission, and in addition they are synchronized with a pixel clock to cover the frequency range of information leakage. Techniques of randomizing lower significant bits of images to reduce signal and increases noise concurrently are also proposed [3],[8].

In this paper, we investigate a technique that differentiates timing of standard screen refreshment, that is defined by VESA [10], and data transmission by fluctuating synchronization signals. The technique prevents an attacker from correlating intercepted value to the exact pixel intensity value at each position, thus the screen image cannot be reconstructed. The screen images, however, maintain their quality because a video display unit (VDU) can reconstructs the correct image from modified synchronization signals as long as the signals are in moderate range.

Investigation on how modulation affects the intercepted image was made with a simulation. Detailed strength and leakage model of electromagnetic radiation from a VDU is studied by Dong et.al. [6], and leakage source and mechanism is discussed by Pennesi and Sebastiani [7]. However, we restrict to a simpler model because our investigation requires only qualitative preciseness. On the other hand, effectiveness of the technique is verified with an experimental setup we built for capturing leakage based on [2]. The technique is implemented as a real-time signal modulator device using a FPGA board that is widely available. The device accepts connection to an ordinary computer and VDU system.

In the following section, we describe a leakage model, a test setup for eavesdropping, and the preliminary result. In the third section, we describe the modulation technique for preventing information leakage and show test results.

Copyright © 2009 IEICE

II. Leakage Model and Experimental Setup

A. Leakage Model

The upper half of Fig.2 illustrates a conventional computer system, where a personal computer and CRT or LCD connected by a video cable. We call this system a "victim".

An attacker captures electromagnetic wave that is emanated from the victim. Because the format of picture data transmitted through the video cable is standardized by VESA, it is easy to find candidate frequencies for horizontal and vertical synchronization signals. Then, the attacker further searches for accurate frequencies one by one. Once the exact frequencies are found, signal processing techniques are applicable to reduce noise then recover the screen image that was shown on the victim's VDU.

Figure 1 illustrates the data structure of analog RGB and corresponding pattern of electromagnetic wave. In an analog RGB cable, pixel values for three colors, red, green and blue, at each screen position are sequentially transmitted from the left-top of the screen to the right-bottom, what is so called "raster scanning" manner, by three different signal lines. These image pixels are composed of three 8 bit intensity values, and each value is represented by analog voltage. This results in the difference of adjacent pixels stimulating the current on each color signal line, then emits electromagnetic wave.

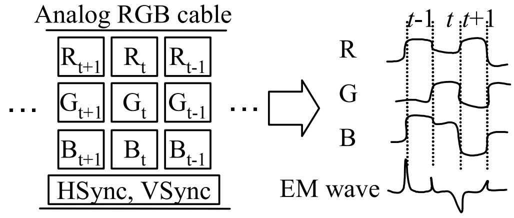


Fig.1 Structure of analog RGB data and electromagnetic wave from the data sequence. (EM: Electro-Magnetic)

The described model leads an estimation of the power of electromagnetic wave P_E for a pixel value p_t at time t and p_{t-1} at time t-1 with a constant positive value c.

$$P_E(t) = c \cdot |p_t - p_{t-1}| \tag{1}$$

The equation is rather simplified compared to that of [6], but it represents leakage qualitatively enough (Table 1 (b)) for the purpose of this paper.

B. Experimental Setup

An experimental setup illustrated in Fig.2 is realized. The victim and the attacker are electronically separated to avoid any connection except for electromagnetic wave.

Table 1 shows a result with the system. The expected leak image (b) was calculated by equation (1). The leaked image (c) was captured at tuning frequency of 134 MHz with a 5 MHz bandwidth receiver, where a pixel clock signal was set to 65.224670 MHz with 1 Hz precision. The horizontal and vertical sync signals were generated based on the values in Table 2. The model generates a qualitatively enough image.

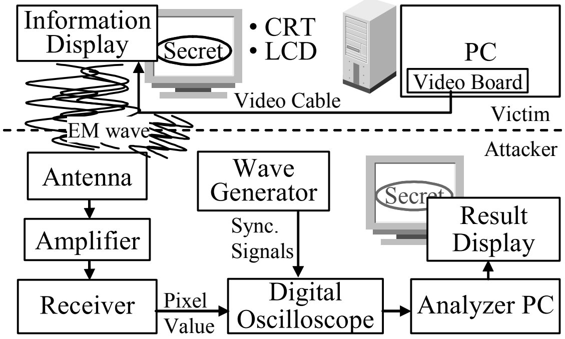
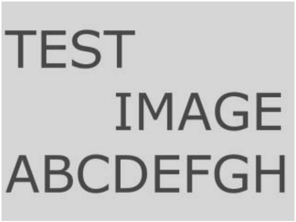
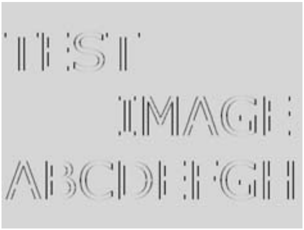
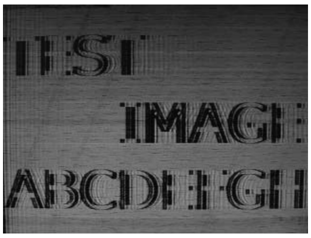


Fig.2 Experimental Setup

TABLE 1 Image displayed on VDU, image calculated and image captured through electromagnetic wave

Source	Image
(a) Displayed Image (on the VDU, 1024×768 pixels)	
(b) Expected Leak Image (Calculated by equation (1))	
(c) Leaked Image (from Actual Device)	

III. Pixel Clock Frequency Modulation

We investigate modulation of frequency of synchronization signals to prevent the attacker from recovering correspondence between the captured electromagnetic wave's power and the pixel intensity at each position. In other words, the attacker cannot reconstruct the original image although he might have captured valid pixel information, because he cannot locate the pixel intensity value at correct positions.

A. Possible Modulation Targets

In the victim system of Fig.1, pixel values of a screen image are transmitted in parallel with synchronization signals such as: pixel clock, data enable, horizontal synchronization

Copyright © 2009 IEICE

and vertical synchronization signals. Transmission of every pixel value is synchronized with the pixel clock. Therefore, to reconstruct the screen image, we need exact synchronization signals. It means that the attacker cannot reconstruct the image without recovering exact synchronization signals. However it is almost impossible to find them from a captured electromagnetic wave because of mixture of the power from pixel transition and synchronization pulses with considerably lower ratio of the latter. Figure 3 shows a screen image and corresponding synchronization signals. Although it is not explicitly illustrated, every signal is synchronized with the pixel clock.

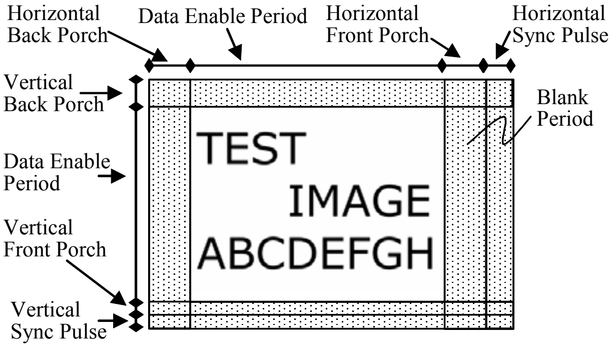


Fig.3 Relation between screen image and horizontal, vertical and data enable synchronization signals. Every signal is synchronized with pixel clock.

An example timing set of synchronization signals that is mostly used in a LCD system is shown in Table 2. Although they are not shown here, XGA (1024×768 pixels) mode has at least four different timing sets.

TABLE 2 TIMING OF SYNCHRONIZATION SIGNALS FOR XGA MODE

Pixel CLK [MHz]	Horizontal Sync. [clock]			
	Data Enable Period	Front Porch	Sync. Pulse	Back Porch
65	1024	24	136	160
	Vertical Sync. [clock]			
	Data Enable Period	Front Porch	Sync. Pulse	Back Porch
	768	3	6	29

There are four candidates for frequency modulation: horizontal sync, vertical sync, data enable and pixel clock signals. We examine those below. Shown images are calculated by equation (1) and corresponding amount of positional shift.

1) Modulation of Horizontal Synchronization Signal

When the frequency of horizontal synchronization signal is modulated by the rate of 1, 5, 10, 100, 1000 and 1344 pixels per line, resulting eavesdropped images become ones in Fig.4. Special care has to be taken for the rate to not being the multiple of the number of pixels per line because the leaked image suddenly becomes a tile of the original image such as the one shown in Fig.4 (f).

2) Modulation of Vertical Synchronization Signal

When the frequency of vertical synchronization signal is modulated by the rate of 10, 1000 and 100000 pixels per screen, resulting eavesdropped images become ones in Fig.5.

3) Modulation of Data Enable Signal

Because data enable signal has to be in the period of horizontal back porch and front porch, possible modulation range is strongly limited. Thus, it is not appropriate for jamming synchronization. However, when the frequency of data enable signal is modulated by the rate of randomly between ±5, ±10 and ±20 pixels at each line, resulting eavesdropped images become ones in Fig.6.

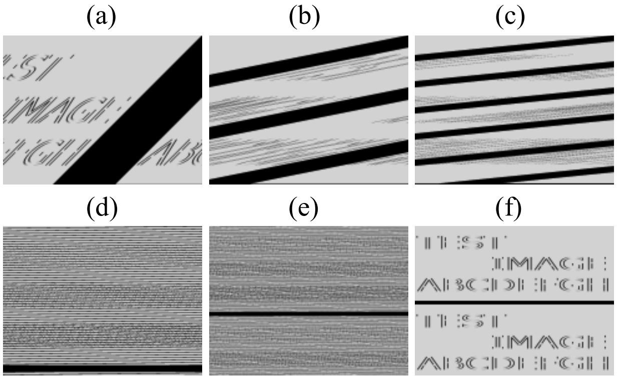


Fig.4 Resulting images by horizontal sync frequency modulation. Modulation rates are (a) 1 pixel, (b) 5 pixels, (c) 10 pixels, (d) 100 pixels, (e) 1000 pixels, (f) 1344 pixels per line.

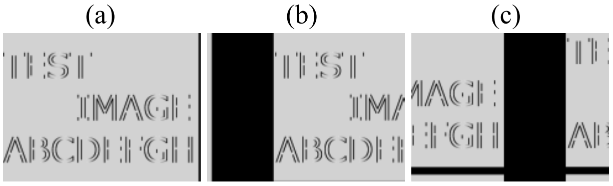


Fig.5 Resulting images by vertical sync frequency modulation. Modulation rates are (a) 10 pixels, (b) 1000 pixels, (c) 100000 pixels per screen.

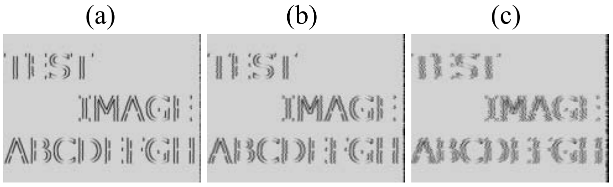


Fig.6 Resulting images by data enable signal frequency modulation. Modulation rates are randomly selected between (a) ±5 pixels, (b) ±10 pixels, (c) ±20 pixels at each line.

4) Modulation of Pixel Clock

If the pixel clock frequency is modulated, all of the horizontal synchronization signal, vertical synchronization signal and data enable signal are also modulated because those signals are synchronized with the pixel clock. It means that all

Copyright © 2009 IEICE

effects shown above can be accomplished merely by modulating the pixel clock frequency.

The above examination indicates that modulation of vertical synchronization signal or data enable signal alone does not give effective jamming property. As a consequence, we conclude that the most effective modulation target is the pixel clock. In the following section, we consider implementation of the pixel clock frequency modulation.

B. *Pixel Clock Frequency Modulation*

To accomplish real-time processing and installation to existing systems, we developed a pixel clock modulation unit.

The processing system is illustrated in Fig.7. Incoming pixel data are buffered in a FIFO buffer then the buffer is read at the modulated clock frequency.

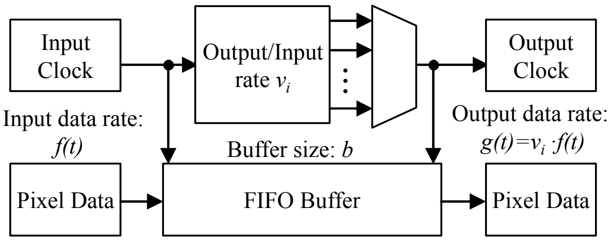


Fig.7 Real-time pixel clock frequency modulation system

C. *Experimental Result*

We implemented the proposed technique on a FPGA board: Altera Cyclone III starter kit with Bitec DVI daughter board. The board is placed between a computer and a VDU so that it modulates output data from the computer in real time (Fig. 8). To analyze effectiveness of the technique, we coupled the attacker's antenna with the output of the board.

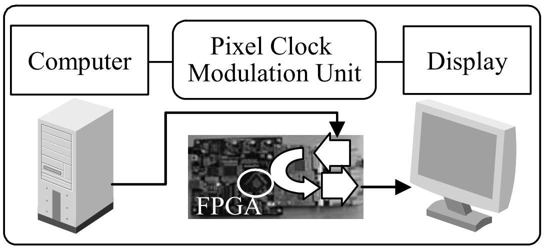
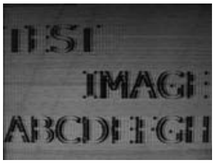
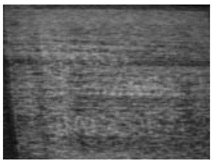


Fig.8 Computer system with pixel clock frequency modulation unit

Table 3 shows sets of a display image and corresponding leak image, those represent the experimental results without any countermeasure and with the proposed technique. Settings of capturing devices are same to those of section II B. The technique jammed emanating signals enough with no visual penalty on the VDU. Patents on this technique are pending.

TABLE 3 DISPLAY AND LEAK IMAGES WITH OR WITHOUT COUNTERMEASURE

	No countermeasure	Proposed method
Display Image		
Leak Image		

IV. CONCLUSION

In this paper, we investigated a technique that fluctuate timing of image data transmission to differentiate those of information displayed on a screen and actual transmission. By the loss of timing information, an attacker cannot locate the exact pixel intensity value at each screen position, thus he cannot recover the screen image from captured information.

We verified effectiveness of the technique on a system of a computer and LCD connected by an analog RGB cable with the pixel clock modulation unit which we realized using a FPGA board.

As countermeasures for electromagnetic security, Kuhn suggested techniques those cut higher frequency information and randomizes lower significant bits of pixel value that do not significantly affect the quality of a screen image. However, these techniques themselves are not fully protective. Since the synchronization signal modulation technique can be implemented independently from these image processing countermeasures, the technique combined with them is expected to improve security. We will investigate integration of existing countermeasures for the secure system in the future research.

REFERENCES

[1] H. Tanaka, O. Takizawa and A. Yamamura, "Evaluation and Improvement of TEMPEST fonts", Information Security Applications (WISA2004), LNCS 3325, pp.457-469, 2004

[2] Markus Kuhn, "Compromising emanations: eavesdropping risks of computer displays", University of Cambridge Technical Report Number 577, December 2003

[3] Markus Kuhn, "Electromagnetic Eavesdropping Risks of Flat-Panel Displays", 4th Workshop on Privacy Enhancing Technologies, pp.1-20, 2004

[4] Markus Kuhn and Ross Anderson, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations", Information Hiding 1998, pp.124-142, 1998

[5] S. Dong, J. Xu and C. Guo, "Bit error rate of a digital radio eavesdropper on computer CRT monitors", IEEE International Symposium on Communications and Information Technology (ISCIT), vol.2, pp.1093-1099, 2004

[6] S. Dong, J. Xu, H. Zhang and C. Wu, "On compromising emanations from computer VDU and its interception", 3rd International Symposium on Electromagnetic Compatibility, pp.692-695, 2002

[7] S. Pennesi and S. Sebastiani, "Information security and emissions control", International Symposium on Electromagnetic Compatibility (EMC2005), pp.777-781, 2005

[8] T. Watanabe, H. Nagayoshi and H. Sako, "A Display Technique for Preventing Electromagnetic Eavesdropping Using Color Mixture Characteristic of Human Eyes", Information Hiding (IH2008), LNCS 5284, pp.1-14, 2008.

[9] Wim van Eck, "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?", Computers and Security, No.4, pp.269-286, 1985

[10] Monitor Timing Specifications, Version 1.0, Revision 0.8, Video Electronics Standards Association (VESA), San Jose, California, 1998.

Copyright © 2009 IEICE