Progress In Electromagnetics Research B, Vol. 36, 399–419, 2012

NOVEL INFORMATION LEAKAGE THREAT FOR INPUT OPERATIONS ON TOUCH SCREEN MONITORS CAUSED BY ELECTROMAGNETIC NOISE AND ITS COUNTERMEASURE METHOD

H. Sekiguchi*

Osaka University, 565-0871 Osaka, Japan

Abstract—Information leakage of general input operations using button images in graphical user interface on touch screen monitors was experimentally investigated from images reconstructed by receiving the electromagnetic noise. In the experimental investigations for input operations of a personal identification number, it was confirmed that when a button image was touched, the touched button image can be identified from the reconstructed button images. This kind of information leakage has originated the fact that the touched button image has changed the color for informing the operator which button image was touched. From the elucidation of the image reconstruction mechanism, it was found that the information leakage has been caused by the magnitude of the emitted signal that results from the analog voltage differences of the RGB signals between neighboring pixels on the monitor. Therefore, a countermeasure method was proposed from the viewpoint of the combination of the colors of the button images and of the background or of the numerals in the button images. The countermeasure method was then applied to the previous input operations of a personal identification number. From the experimental results for the countermeasure method, it was confirmed that the touched button image cannot be identified from the reconstructed button image. As a result, the proposal countermeasure method can prevent effectively the information leakage of input operations on touch screen monitors due to the electromagnetic noise.

Received 12 October 2011, Accepted 17 November 2011, Scheduled 28 November 2011

* Corresponding author: Hidenori Sekiguchi (sekiguchi@jrl.eng.osaka-u.ac.jp).

1. INTRODUCTION

With the progress of the information society, concerns about information leakage have recently increased from the aspect of information security. A general information security management system (ISMS) standard has been published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) [1]. The Telecommunication standardization sector of the International Telecommunication Union (ITU-T) has also published an ISMS standard for telecommunications [2]. In these ISMSs, information leakage due to electromagnetic noise of electronic and information equipment is treated as a physical security issue. These specifications recommend evaluations and countermeasures for the security risk of information leakage caused by electromagnetic noise of electronic and information equipment. Note that the terms of TEMPEST and emission security or emanations security (EMSEC) have been used generically in the study of this kind of information leakage and countermeasures [3].

On the other hand, it is well known that the electromagnetic emission level of electronic and information equipment has been kept low to prevent electromagnetic interference for each equipment [4–7]. However, in practice all active electronic and information equipments emit slight electromagnetic noise. The electromagnetic noise is generated by the numerous variations in signals that occur in modern electronic circuits. Signals transmitting confidential information are no exception. So equipment dealing with sensitive information may also emit such electromagnetic noise generated by signal variations in that. Thus, a target signal from the information equipment might be reproduced or estimated by receiving and analyzing the low-level electromagnetic noise.

It has already been reported that the display image on a personal computer (PC) that employs either a cathode ray tube (CRT) or a liquid crystal display (LCD) monitor using the raster scan method can be reconstructed by receiving and analyzing the electromagnetic noise [8, 9]. In addition, the key strokes on a PC keyboard can be determined from the electromagnetic noise [10]. These reports show that the information leakage threat of the display image or key strokes might be caused by electromagnetic noise of the information equipment. Additionally, there is an estimation result that the maximum receivable distance of the electromagnetic noise exceeds hundreds of meters from information equipment, taking account of the receivable capacity of used receiver and antenna [11]. Therefore, the information leakage evaluation methods and the

countermeasure techniques to prevent such information leakage are also actively researched [12–17]. These researches are very important for information security, and the investigation of new information leakage threats has become a crucial field for the future.

The present study discusses on a novel information leakage threat caused by electromagnetic noise of information equipment. The focus is input operations on touch screen monitors, which are widely used in commercial information equipment such as automatic teller machines (ATMs), cash dispensers (CDs), door and gate access control terminals, credit-card ticket-vending machines, and so on. On the touch screen monitors, the operator is often required to input a certificate code such as a personal identification number (PIN) and password, which is very important code in information security.

The input operations on the touch screen monitors are generally composed by graphical user interface (GUI), and are usually handled by touching a sequence of button images. When a button image was touched, the touched button image changes the color to inform the operator which button image was touched. This color change upon touching a button image is a general procedure used widely in the sequence of input operations employing the touch screen monitors. However, unfortunately, the display image on the touch screen monitors can be reconstructed by receiving the electromagnetic noise, and the touched button image can be identified from the reconstructed button image [18]. Accordingly, the information of input operations using button images on the touch screen monitors is leaked from the electromagnetic noise. Therefore, the present study has focused on the countermeasure method against this type of information leakage [19].

In this paper, first, it is experimentally demonstrated that a touched button image on a touch screen monitor can be identified from the display images reconstructed by receiving the electromagnetic noise. Next, the mechanism of the information leakage is discussed from the relationships between the color of the button image in the display image, the corresponding analog voltages of the RGB signals, the emitted signal by the analog voltage variations of the RGB signals in the raster scan, the detected component of the emitted signal in the reception signal, and the grayscale shading in the reconstructed display image. In addition, based on these discussions, a countermeasure method is proposed and applied to the input operations on the touch screen monitor. Finally, it is experimentally confirmed that the proposal countermeasure method is effective to prevent this type of information leakage. This paper adds new aspects and examinations to the previous investigations in [18, 19].

2. INFORMATION LEAKAGE OF INPUT OPERATIONS ON TOUCH SCREEN MONITOR DUE TO ELECTROMAGNETIC NOISE

In this section, it is presented that a touched button image on a touch screen monitor can be identified from the display images reconstructed by receiving the electromagnetic noise.

First of all, the display image on a monitor can be reconstructed using the reception signal of the electromagnetic noise and the vertical and horizontal synchronized signals of the monitor [8, 9, 16, 17]. Note that most monitors adopt the raster scan method, which is a technique for generating a video image by means of a line-by-line sweep. Essentially, the electromagnetic noise that should be ideally observed is the signal emitted by the analog voltage variations of the RGB signals on the raster scan in the monitor, not by the digital image signal transmitted from the graphic device to the monitor. So the emitted signal is a sequential signal according to the raster scan, and is practically contained in the electromagnetic noise. The reception signal of the electromagnetic noise is the video output signal of the receiver. The video output signal might be called the base band signal, which is observed and synchronous-detected (or envelope-detected) in the receiving band width at the receiving frequency of the receiver. The basic principle of the image reconstruction is to arrange the reception signal by using the vertical and horizontal synchronized signals. The vertical and horizontal synchronized signals can be detected from observing the electromagnetic noise [8].

By the way, the vertical and horizontal synchronized signals have a little difference according to the individual graphic device. The little difference is useful to distinguish the target monitor. In other words, the target information equipment with the monitor can be identified from the little difference in information equipments with the monitor of the same model.

2.1. Experimental System and Equipment under Test

Figure 1 shows an experimental system used to receive electromagnetic noise emitted from an equipment under test (EUT), which was composed of a commercial desktop PC and a commercial touch screen LCD monitor. They were used as an example of typical information equipment with touch screen monitor (e.g., ATMs, CDs, credit-card ticket-vending machines, and so on). The EUT was placed in a compact anechoic chamber to receive the electromagnetic noise stably in spite of the ambient electromagnetic noise environment. The use of the

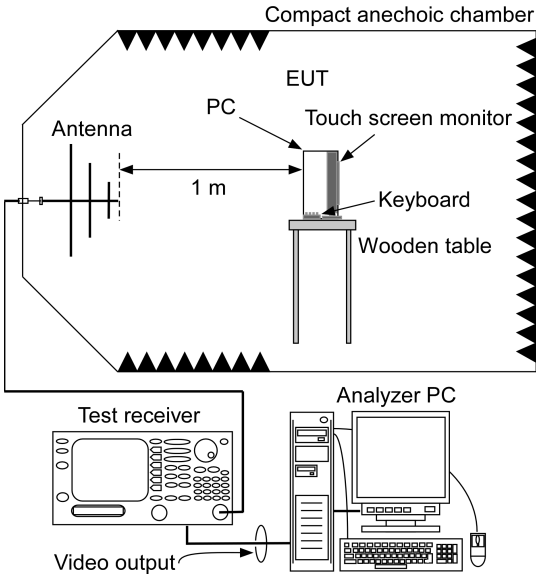

Figure 1. Experimental system used to receive electromagnetic noise emitted from EUT in compact anechoic chamber.

chamber is justified with the need to receive the electromagnetic noise emitted from the EUT with quality and reproducibility.

In Figure 1, the electromagnetic noise emitted from the EUT was received using a log-periodic antenna (SAS-510-2 manufactured by A. H. Systems, Inc.) and a test receiver (FSET22 manufactured by ROHDE & SCHWARZ). The log-periodic antenna inside the chamber was positioned the distance of 1 m from the face of the EUT. The test receiver outside the chamber was set to MODE of zero span, resolution and video bandwidth (RBW and VBW) of 50 MHz, and reference level of -83 dBm. The video output port of the test receiver was connected to an analyzer PC with an image processing board, which was controlled by the special software FrameControl manufactured by SystemWare, Inc..

Note that the above-mentioned receiving band width is the same as the RBW of the test receiver, and the receiving frequency was set to 350 MHz. The receiving band width and frequency affect the quality of the reconstructed display image. The receiving band width is necessary for tens of MHz or more, and the best receiving frequency varies according to the EUT [8, 9, 12, 13].

In the experimental system, the analyzer PC can reconstruct the display image on the touch screen LCD monitor of the EUT using

the reception signal of the electromagnetic noise and the vertical and horizontal synchronized signals. The rough values of the vertical and horizontal synchronized signals obtained from the setting parameters such as the display resolution and the refresh rate of the monitor [20]. Thereafter, those accurate values were adjusted from the correction of the distortion of the reconstructed display image in advance.

2.2. Flow of Display Image in PIN Input Operation

Figure 2 shows an example of the sequence of typical display images involved in a PIN input operation. The display images include button images to input the PIN. The PIN input operation can be performed by touching the button images on a touch screen LCD monitor. The button images and the PIN input operation can be usually constructed by means of GUI tool.

Figure 2(a) shows the display image before the operator touches any button image. Figure 2(b) shows the display image when the operator was touched the button image of the numeral 1. Then, the touched button image changes from the default color to the non-default color. At the same time, the color of the circle image of the left side in the upper row, which shows whether the first digit of the PIN was input, also changes from the default color to the non-default color. The color change of the touched button image informs the operator which button image was touched. The color change of the circle image informs the operator which PIN digit was input. Figure 2(c) shows the display image after the operator released the button image of the numeral 1. Then, the color of the touched button image returns from the non-default color to the default color, whereas the first circle image maintains the non-default color to inform the operator that the first digit of the PIN has been input. These color changes are a general procedure used widely in the sequence of input operations using button images on touch screen monitors.

Here, the color of the objects in the display image is usually managed by the combination of digital 8-bit red-green-blue (RGB) values, which may be generally expressed as $[\mathrm{R}:\mathrm{G}:\mathrm{B}]$ in the GUI tool. As an example, the button images in Figure 2 were given the colors as follows. The default color of the button image was green, for which $[\mathrm{R}:\mathrm{G}:\mathrm{B}] = [0:255:0]$. The non-default color of the touched button image was magenta, for which $[\mathrm{R}:\mathrm{G}:\mathrm{B}] = [255:0:255]$. In addition, the background color outside the button images was black, for which $[\mathrm{R}:\mathrm{G}:\mathrm{B}] = [0:0:0]$. The color of the numerals inside the button images was white, for which $[\mathrm{R}:\mathrm{G}:\mathrm{B}] = [255:255:255]$.

2.3. Reconstructed Button Images from Electromagnetic Noise

The display images shown in Figures 2(a), 2(b), and 2(c) were reconstructed by receiving the electromagnetic noise emitted from the EUT, as depicted in Figure 1. Here, the reconstructed button image of the numeral 1 was focused to investigate the correspondence with the color change of the button image of the numeral 1 on the display images in Figures 2(a), 2(b), and 2(c). Figures 3(a), 3(b), and 3(c) show the reconstructed button images of the numeral 1, which are corresponding to the button image of the numeral 1 on the display images in Figures 2(a), 2(b), and 2(c), respectively. The reconstructed button images are then represented in grayscale.

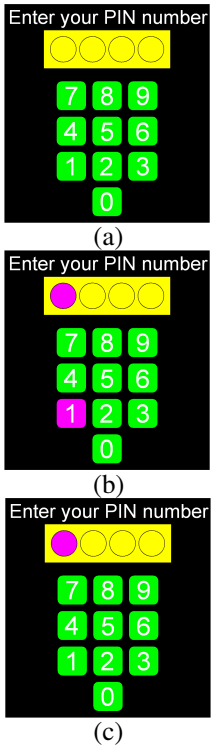

Figure 2. Typical sequence of display images in PIN input operation. (a), (b), and (c) show display images before, when, and after the button image of numeral 1 is touched, respectively.

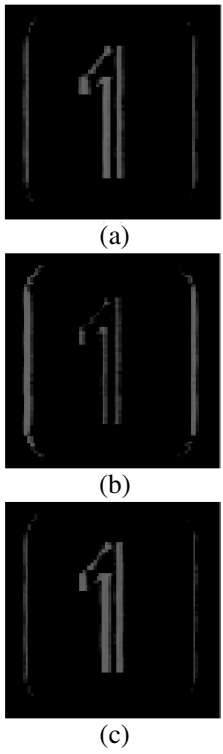

Figure 3. Reconstructed button images of numeral 1. (a), (b), and (c) correspond to the button images of numeral 1 in Figures 2(a), (b), and (c), respectively.

Note that the signals emitted by each analog voltage variations of the RGB sub-pixels in the raster-scanned pixels on the touch screen LCD monitor are electromagnetically coupling within space, and become a part of the electromagnetic noise. Thus, the reception signal of the electromagnetic noise cannot separate to the RGB components. So, the grayscale shading in the reconstructed image depends on the magnitude of the reception signal.

From Figure 3, firstly, it is confirmed that the button images of the numeral 1 in the display images in Figure 2 can be clearly reconstructed by receiving the electromagnetic noise emitted from the EUT. Secondly, by comparing with Figures 3(a), 3(b), and 3(c), it is found that the vertical frame of the reconstructed button image in Figure 3(b) is significantly thicker than that in Figures 3(a) and 3(c). In contrast, the vertical frame of the numeral 1 in the reconstructed button image in Figure 3(b) is thinner than that in Figures 3(a) and 3(c). The difference of the thickness of those vertical frames resulted from the difference of the color of the button images in Figure 2. In addition, there is no difference in the vertical frames of the reconstructed button images and of the numeral 1 in the reconstructed button images between Figures 3(a) and 3(c), because the color of the button images in the display images in Figures 2(a) and 2(c) is the same. Moreover, there was also no difference in the vertical frames of the reconstructed button images and of the other numerals in the reconstructed button images. Thus, from the correspondence with Figures 2 and 3, it can be confirmed that when the color of the button image in the display image is green, the vertical frame of the reconstructed button image is thin and the vertical frame of the numeral 1 in the reconstructed button image is thick. In contrast, when the color of the button image in the display image is magenta, the vertical frame of the reconstructed button image is thick and the vertical frame of the numeral 1 in the reconstructed button image is thin.

From the experimental results in Figure 3, it was revealed that the input operations using button images on the touch screen LCD monitor can be understood from the comparison with the button images reconstructed by receiving the electromagnetic noise.

Incidentally, if the reconstructed display image has been observed in real-time, only the vertical frames of the reconstructed button image corresponding to the touched button image appear to flash clearly. It is because the thickness of the vertical frame of the reconstructed button image and of the numeral in the reconstructed button image changes for a moment, nevertheless the rests keep static. As a result, it was confirmed that the information of the input operation using

button images on the touch screen monitor was leaked from the electromagnetic noise.

Note that the horizontal frames of the reconstructed button image and of the numeral 1 in the reconstructed button images are not drawn in Figure 3. This aspect is discussed in detail in the following section.

3. INFORMATION LEAKAGE MECHANISM

In this section, the mechanism of the information leakage of the input operations using button images on touch screen monitor was discussed based on the relationships between the color of the button image in the display image, the corresponding analog voltages of the RGB signals, the emitted signal by the analog voltage variations of the RGB signals in the raster scan, the detected component of the emitted signal in the reception signal, and the grayscale shading in the reconstructed display image.

Firstly, the color of the objects in the display image is managed by a combination of digital 8-bit RGB values [R : G : B] in the GUI tool, as mentioned in the previous section. However, each digital 8-bit RGB values also control the analog voltages for each RGB light-emitting elements of the RGB sub-pixels in raster-scanned pixels on the touch screen LCD monitor. Namely, the color of the objects is physically controlled and emitted light by the combination of the analog voltages of the RGB signals. In addition, a color change between neighboring pixels in the display image generates analog voltage variations of the RGB signals in the raster scan on the monitor.

Secondly, the analog voltage variations of the RGB signals between the neighboring pixels emit signals, the magnitude of which corresponds with the analog voltage differences of the RGB signals between the neighboring pixels. The emitted signals are electromagnetically coupling within space, and become a part of the electromagnetic noise.

Finally, the electromagnetic noise is received by the receiver with antenna. Then, the proportion of the emitted signal in the electromagnetic noise depends on the magnitude of the other emitted signals in the electromagnetic noise. Moreover, since each of the emitted signals has a characteristic in the frequency components, the reception signal used for the reconstructed display image depends on the receiving frequency and the receiving band width of the receiver. In the receiving frequency where the display image can be reconstructed, the proportion of the emitted signal in the received electromagnetic noise is high. Then, the reconstructed display image can be represented clearly in grayscale. Additionally, when the reception signal is the

largest in the time series of the raster scan, white is drawn in the reconstructed display image. Conversely, when the reception signal is the smallest, black is drawn.

Taking into account the physical aspects, Figure 4 shows the relationships between the color of the button image in the background (top row), the corresponding analog voltages of the RGB signals on the

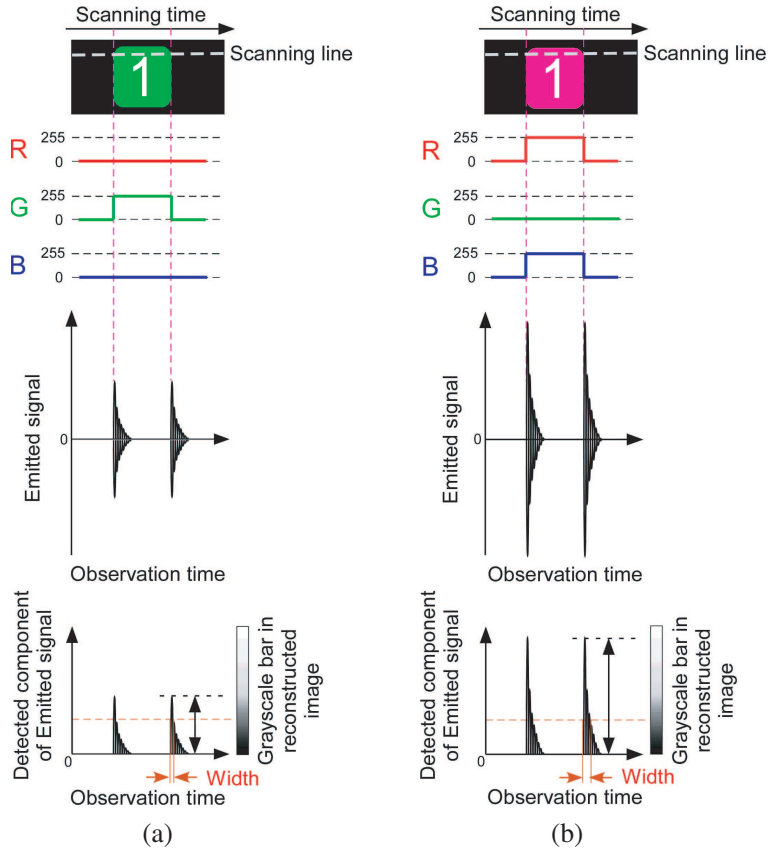

Figure 4. Relationships between the color of button image in background (top row), the corresponding analog voltages of RGB signals on scanning line of top row (second row), the emitted signal by analog voltage variations of RGB signals in raster scan (third row), the detected component of emitted signal in reception signal (left side in bottom row), and the grayscale bar used in reconstructed display image (right side in bottom row). (a) and (b) show for each button image of green and magenta, respectively.

scanning line of the top row (second row), the emitted signal by the analog voltage variations of the RGB signals in the raster scan (third row), the detected component of the emitted signal in the reception signal (left side in bottom row), and the grayscale bar used in the reconstructed display image (right side in bottom row). The top row in Figure 4(a) shows the button image of the numeral 1 that corresponds with Figures 2(a) and 2(c). The color of the button image is green, for which $[\mathrm{R}:\mathrm{G}:\mathrm{B}] = [0:255:0]$. The top row in Figure 4(b) shows the button image of the numeral 1 that corresponds with Figure 2(b). The color of the button image is magenta, for which $[\mathrm{R}:\mathrm{G}:\mathrm{B}] = [255:0:255]$. The background color outside those button images is black, for which $[\mathrm{R}:\mathrm{G}:\mathrm{B}] = [0:0:0]$.

The white dashed lines superimposed onto the button images in Figures 4(a) and 4(b) show an example of a scanning line in the raster scan on the touch screen LCD monitor. The horizontal axis in the top and second rows gives the scanning time in the raster scan, which is the same as the observation time of the emitted signal in the third and bottom rows. Each column in Figures 4(a) and 4(b) is corresponding at the time.

In Figure 4(a), it is now focused on the first color change along the scanning line on the button image. The color changes from black ($[\mathrm{R}:\mathrm{G}:\mathrm{B}] = [0:0:0]$) to green ($[\mathrm{R}:\mathrm{G}:\mathrm{B}] = [0:255:0]$) at the vertical frame of the button image, as shown in the top row. So, the analog voltage variations of the RGB signals are generated at neighboring pixels on the vertical frame, as shown in the second row. In this case, only G (green) signal is changed. Thus, the analog voltage variation of G (green) signal emits a signal into space. The emitted signal is naturally the dumped oscillation signal in space as shown in the third row, because the radiation part of the emitted signal acts as the differentiators. The magnitude of the emitted signal depends on the analog voltage differences of the RGB signals between neighboring pixels. So, the magnitude of the emitted signal gives a relative analog voltage difference of 255 from black ($[\mathrm{R}:\mathrm{G}:\mathrm{B}] = [0:0:0]$) to green ($[\mathrm{R}:\mathrm{G}:\mathrm{B}] = [0:255:0]$). Then, the polarity of the dumped oscillation shape depends on the polarity of the analog voltage variation. The emitted signal in the reception signal has the detected component by the detector in the receiver, as shown the left side in the bottom row. In the reconstructed display image, the shading corresponding to the magnitude of the detected component in the emitted signal becomes then the middle color in the grayscale, as shown in the right side in the bottom row. In brief, the vertical frame of the button image of green in the display image is drawn by the middle color in the grayscale on the reconstructed button image.

Similarly, in Figure 4(b), the color along the scanning line on the button image changes firstly from black ([R : G : B] = [0 : 0 : 0]) to magenta ([R : G : B] = [255 : 0 : 255]) at neighboring pixels on the vertical frame. In this case, R (red) and B (blue) signals change. Thus, the analog voltage variations of R (red) and B (blue) signals emit signals into space. The emitted signals are electromagnetically coupled to one emitted signal in space. So, the magnitude of the coupling emitted signal gives a relative analog voltage difference of 510 (= 255 × 2) from black ([R : G : B] = [0 : 0 : 0]) to magenta ([R : G : B] = [255 : 0 : 255]). The coupling emitted signal in the reception signal has the detected component by the detector in the receiver. In the reconstructed display image, the shading corresponding to the magnitude of the detected component in the coupling emitted signal becomes then the high color (i.e., white) in the grayscale. In brief, the vertical frame of the button image of magenta in the display image is drawn by the high color in the grayscale on the reconstructed button image. Note that since the receiver with antenna receives the coupling emitted signal, the reconstructed display image is represented by one color shading.

By comparing with Figures 4(a) and 4(b), it is found that the magnitude of the emitted signal in Figure 4(b) is twice as large as that in Figure 4(a) in principle, because the relative analog voltage difference in the RGB signals in Figure 4(b) is twice as large as that in Figure 4(a). In addition, since those emitted signals from the dumped oscillation shapes, the width of the emitted signal in Figure 4(b) is wider than that in Figure 4(a) at the same magnitude, from the comparison of the left sides in the bottom row of Figures 4(a) and 4(b). Also, those emitted signals do not have the direct current component. Thus, all the horizontal portions on the vertical frame and on the numerals in the button image are not drawn in the reconstructed display image.

These physical aspects in the image reconstruction have revealed the mechanism of the information leakage of input operations using button images on touch screen monitors. The experimental results in Figure 3 have also proven the mechanism of the image reconstruction due to the electromagnetic noise of the touch screen monitor.

By the way, from this information leakage mechanism, it can be explained that why the vertical frame of the numeral 1 in the reconstructed button image in Figure 3(b) is thicker than that in Figures 3(a) and 3(c). It is because the color of the numeral 1 is white ([R : G : B] = [255 : 255 : 255]). Figure 5 shows briefly the relationships between the button image of the numeral 1 (top row), the corresponding analog voltages of the RGB signals on the scanning

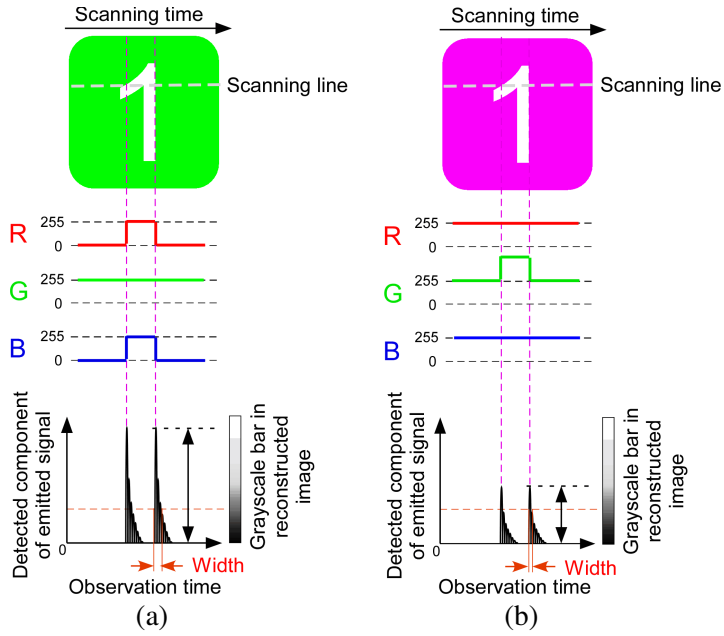

Figure 5. Relationships between the button image of numeral 1 (top row), the corresponding analog voltages of RGB signals on scanning line of top row (middle row), the detected component of emitted signal in reception signal (left side in bottom row), and the grayscale bar used in reconstructed display image (right side in bottom row). (a) and (b) show for each button image of green and magenta, respectively.

line of the top row (middle row), the detected component of the emitted signal in the reception signal (left side in bottom row), and the grayscale bar used in the reconstructed display image (right side in bottom row). At the vertical frame of the numeral 1 in the button image, when the color changes from green ($[R:G:B] = [0:255:0]$) to white ($[R:G:B] = [255:255:255]$) as shown in Figure 5(a), the relative analog voltage difference of the RGB signals is 510 ($= 255 \times 2$). In contrast, when the color changes from magenta ($[R:G:B] = [255:0:255]$) to white ($[R:G:B] = [255:255:255]$) as shown in Figure 5(b), the relative analog voltage difference of the RGB signals is 255. Therefore, the magnitude of the emitted signal in Figure 5(a) is twice as large as that in Figure 5(b). In the reconstructed button images in Figure 3, the vertical frames of the numeral 1 in Figures 3(a) and 3(c) are whiter and thicker than that in Figure 3(b).

As a consequence, it was revealed that the information leakage of input operations using button images on touch screen monitors

is caused by the magnitude of the emitted signal that results from the analog voltage differences of the RGB signals between neighboring pixels at all of before/after and when the button image was touched. The emitted signal is contained in the electromagnetic noise. In brief, the information leakage is caused by the analog voltage differences of the RGB signals between the neighboring pixels, which are generated from the color change by touching the button image.

4. COUNTERMEASURE METHOD

From the previous discussion, it can be considered that the information leakage of input operations using button images on touch screen monitors can be prevented by remaining constant the analog voltage difference in the RGB signals between neighboring pixels, at all of before/after and when the operator touches a button image. In this section, the principle of this approach was described in details as a countermeasure method against this type of information leakage. Additionally, it was applied to the previous PIN input operations, and the validity was verified experimentally. Moreover, the applicable condition of the countermeasure method was discussed.

4.1. Principle of Countermeasure Method

The proposal countermeasure method was applied to the default colors of green shown in Figure 2. As an example, the default color of the button image was modified from green ($[\mathrm{R}:\mathrm{G}:\mathrm{B}] = [0:255:0]$) to cyan ($[\mathrm{R}:\mathrm{G}:\mathrm{B}] = [0:255:255]$). In short, the default color of the button image is cyan ($[\mathrm{R}:\mathrm{G}:\mathrm{B}] = [0:255:255]$), and the non-default color of the touched button image is magenta ($[\mathrm{R}:\mathrm{G}:\mathrm{B}] = [255:0:255]$).

Figure 6 shows the relationships between the color of the button image in the background (top row), the corresponding analog voltages of the RGB signals on the scanning line of the top row (second row), the emitted signal by the analog voltage variations of the RGB signals in the raster scan (third row), the detected component of the emitted signal in the reception signal (left side in bottom row), and the grayscale bar used in the reconstructed display image (right side in bottom row), as well as Figure 4.

Now, the color along the scanning line in the button image changes firstly from black ($[\mathrm{R}:\mathrm{G}:\mathrm{B}] = [0:0:0]$) to cyan ($[\mathrm{R}:\mathrm{G}:\mathrm{B}] = [0:255:255]$) at the vertical frame of the button image, as shown in the top row. So, the analog voltage variations of the RGB signals are generated at neighboring pixels on the vertical frame, as shown in the second row. In this case, G (green) and B (blue) signals change.

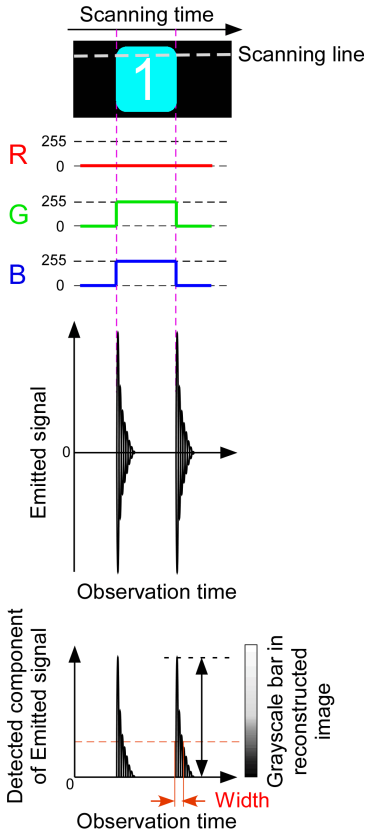

Figure 6. Relationships between the color of button image in background (top row), the corresponding analog voltages of RGB signals on scanning line of top row (second row), the emitted signal by analog voltage variations of RGB signals in raster scan (third row), the detected component of emitted signal in reception signal (left side in bottom row), and the grayscale bar used in reconstructed display image (right side in bottom row), for button image of cyan.

Thus, the analog voltage variations of G (green) and B (blue) signals emit signals into space. The emitted signals are electromagnetically coupled to one emitted signal in space, as shown in the third row. The magnitude of the coupling emitted signal gives a relative analog voltage difference of 510 ($= 255 \times 2$) from black ($[\mathrm{R}:\mathrm{G}:\mathrm{B}] = [0:0:0]$) to cyan ($[\mathrm{R}:\mathrm{G}:\mathrm{B}] = [0:255:255]$). The coupling emitted signal in the reception signal has the detected component by the detector in the receiver. In the reconstructed display image, the shading corresponding

to the magnitude of the detected component in the coupling emitted signal becomes then the high color (i.e., white) in the grayscale.

Again, the button image in Figure 6 shows the default button image, and the button image in Figure 4(b) shows the touched button image. From the comparison of Figures 6 and 4(b), it is found that the magnitude of the emitted signal is the same, and thus the level of the grayscale shading is also the same, in principle. In other words, although the button image changes the color to inform the operator which touched button image, there is no difference in the reconstructed button images in principle. Consequently, the proposal countermeasure method can prevent the information leakage of input operations performed using button images on touch screen monitors without spoiling the functionality and usability of this type of input operation.

4.2. Application and Verification of Countermeasure Method

Here, the proposal countermeasure method was applied to the PIN input operations in the previous section, and the validity was verified experimentally. The experimental system was the same as Figure 1.

Figure 7 shows the sequence of the display images for a PIN input operation, as well as Figure 2. Then, the proposal countermeasure method has been applied to the color of the button images. Figure 7(a) shows the display image before the operator touches any button images. The default color of the button images is cyan ([R : G : B] = [0 : 255 : 255]). Figure 7(b) shows the display image when the operator touched the button image of the numeral 1, which changed the color from cyan ([R : G : B] = [0 : 255 : 255]) to magenta ([R : G : B] = [255 : 0 : 255]). Figure 7(c) shows the display image after the operator has released the button image of the numeral 1, which returned the color from magenta ([R : G : B] = [255 : 0 : 255]) to cyan ([R : G : B] = [0 : 255 : 255]).

The display images shown in Figures 7(a), 7(b), and 7(c) were reconstructed by receiving the electromagnetic noise emitted from the EUT in Figure 1. Now, the reconstructed button images of the numeral 1 was focused to confirm the correspondence with the color change of the button image of the numeral 1 on the display images in Figures 7(a), 7(b), and 7(c). Figures 8(a), 8(b), and 8(c) show the reconstructed button images of the numeral 1 corresponding to the display images in Figures 7(a), 7(b), and 7(c), respectively.

From the reconstructed button images in Figure 8, it can be confirmed that the button image of the numeral 1 in Figure 7 can be reconstructed by receiving the electromagnetic noise emitted from

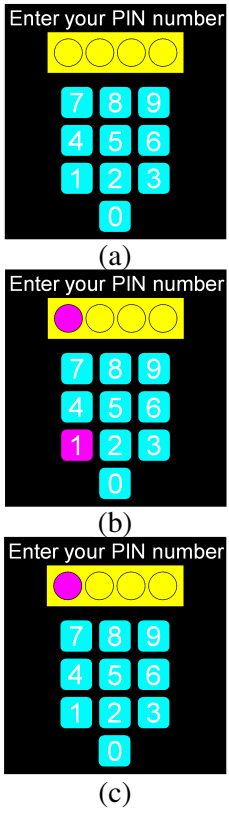

Figure 7. Proposed sequence of display images in PIN input operation. (a), (b), and (c) show the display image before, when, and after the button image of numeral 1 is touched, respectively.

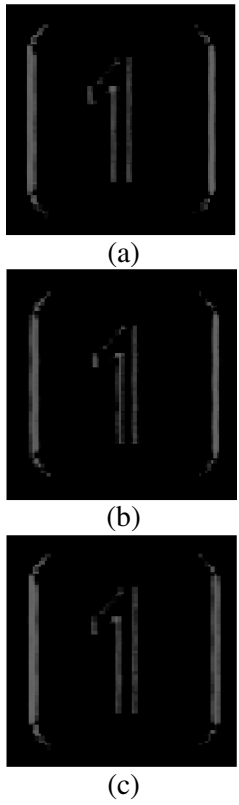

Figure 8. Reconstructed button images of numeral 1. (a), (b), and (c) correspond to Figures 7(a), (b), and (c), respectively.

the EUT. However, in contrast to the reconstructed button images in Figure 3, all the vertical frames in the reconstructed button images in Figure 8 were the same thickness. In addition, all the vertical frames of the numeral 1 in the button images were also the same thickness.

In conclusion, there was no difference in the reconstructed button images in Figure 8, despite the fact that the touched button image changed the color. These results verified that the proposal countermeasure method can prevent effectively this type of information leakage caused by the electromagnetic noise.

4.3. Applicable Conditions of Countermeasure Method

The key point of the proposal countermeasure method is that the relative analog voltage difference of the RGB signals between neighboring pixels remains constant at all of before/after and when the button image was touched, as shown in Figures 4(b) and 6. So, the applicable condition for the proposal countermeasure method was discussed from the RGB color difference between the button images and the background or the numerals. Under the key point, there are a lot of possible combinations for those colors.

Now, the colors of the background and the numerals are $[\mathrm{R_{BG}} : \mathrm{G_{BG}} : \mathrm{B_{BG}}]$ and $[\mathrm{R_{NUM}} : \mathrm{G_{NUM}} : \mathrm{B_{NUM}}]$, respectively. The default color before/after touching the button image and the non-default color when touching the button image are $[\mathrm{R_{DEF}} : \mathrm{G_{DEF}} : \mathrm{B_{DEF}}]$ and $[\mathrm{R_{NDEF}} : \mathrm{G_{NDEF}} : \mathrm{B_{NDEF}}]$, respectively. Then, the applicable condition for the RGB color difference between the background and the button images is given by the following equation:

$$\begin{aligned} &|\mathrm{R_{BG}} - \mathrm{R_{DEF}}| + |\mathrm{G_{BG}} - \mathrm{G_{DEF}}| + |\mathrm{B_{BG}} - \mathrm{B_{DEF}}| \\ = \ &|\mathrm{R_{BG}} - \mathrm{R_{NDEF}}| + |\mathrm{G_{BG}} - \mathrm{G_{NDEF}}| + |\mathrm{B_{BG}} - \mathrm{B_{NDEF}}| \end{aligned} \quad (1)$$

Also, the applicable condition for the RGB color difference between the numerals and the button images is given by the following equation:

$$\begin{aligned} &|\mathrm{R_{NUM}} - \mathrm{R_{DEF}}| + |\mathrm{G_{NUM}} - \mathrm{G_{DEF}}| + |\mathrm{B_{NUM}} - \mathrm{B_{DEF}}| \\ = \ &|\mathrm{R_{NUM}} - \mathrm{R_{NDEF}}| + |\mathrm{G_{NUM}} - \mathrm{G_{NDEF}}| + |\mathrm{B_{NUM}} - \mathrm{B_{NDEF}}| \end{aligned} \quad (2)$$

In (1) and (2), the symbol $|X|$ denotes the absolute value of X. Note that since the detected component in the emitted signal has the positive value by the detector of the receiver, the symbol is necessary.

According to the applicable conditions of (1) and (2), the RGB color differences between the button images and the background or the numerals becomes relatively the same, and the relative analog voltage difference of the RGB signals between neighboring pixels remains constant at all of before/after and when the button image was touched, too. Thus, the magnitude of the emitted signal by the relative analog voltage difference becomes also the same, and all the vertical frames in the reconstructed button images have the same thickness. Conclusively, the touched button image cannot be identified from the reconstructed button image, when it change the color under the applicable conditions of (1) and (2). A choice of the colors of the background, the button images, and the numeral in the button images, that meets the applicable conditions of (1) and (2), can prevent the information leakage of input operations using button images on the touch screen monitor caused by the electromagnetic noise, without spoiling the functionality and usability that informs the operator the touched button image.

5. CONCLUSION

In this paper, the information leakage of input operations performed using button images on touch screen monitors was experimentally investigated from the display images reconstructed by receiving the electromagnetic noise. First, it was experimentally demonstrated that a touched button image on the touch screen LCD monitor can be identified from the reconstructed button images, and the information of the input operations using button images can be leaked from the electromagnetic noise. This type of information leakage has been also experimentally confirmed in the combinations of a lot of PCs and monitors, although those results have not been presented in this paper. Next, the mechanism of this type of information leakage was investigated from the relationships between the color of the button image in the display image, the corresponding analog voltages of the RGB signals, the emitted signal by the analog voltage variations of the RGB signals in the raster scan, the detected component of the emitted signal in the reception signal, and the grayscale shading in the reconstructed display image. From the investigations, it was revealed that this type of information leakage was caused by the magnitude of the emitted signal that results from the analog voltage differences in the RGB signals between neighboring pixels at all of before/after and when the button image was touched. In addition, a countermeasure method was proposed to prevent to this type of information leakage. The countermeasure method was that the relative analog voltage differences of the RGB signals between neighboring pixels remains constant at all of before/after and when the button image is touched. Then, it was applied to the previous input operations, and the validity was verified experimentally. From the experimental results, it was confirmed that the proposal countermeasure method can prevent effectively this type of information leakage. An advantage of the countermeasure method is that it can prevent this type of information leakage caused by the electromagnetic noise, but it is not the electromagnetic noise suppression method by using hardware such as shielding or filtering. The further suppression of the electromagnetic noise of electronic and information equipment needs considerable efforts or costs. However, the proposal countermeasure method can be applied by the software technique. Moreover, it did not also spoil the functionality and usability of the touch screen monitor system with man-machine interface operations.

ACKNOWLEDGMENT

The author gratefully expresses his gratitude to his colleague Mr. Shinji Seto, who provided constructive comments and encouragement.

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. RFC2828, "Internet security glossary," Internet Engineering Task Force, 2000.
4. CISPR 22, "Information technology equipment — Radio disturbance characteristics — Limits and methods of measurement," International Electrotechnical Commission (IEC), 2008.
5. IEC 61000-6-3, "Electromagnetic Compatibility (EMC) — Part 6-3: Generic Standards — Emission Standard for Residential," Commercial and Light-Industrial Environments International Electrotechnical Commission (IEC), 2006.
6. K.48, "EMC requirements for telecommunication equipment — Product family Recommendation," International Telecommunication Union — Telecommunication Standardization Sector (ITU-T), 2006.
7. MIL-STD-461F, "Requirements for the control of electromagnetic interference characteristics of subsystems and equipment," Department of Defense Interface Standard (United State of America), 2007.
8. Van Eck, W., "Electromagnetic radiation from video display units: An eavesdropping risk?" *Computers and Security*, Vol. 4, No. 4, 269–286, 1985.
9. Kuhn, M. G., "Compromising emanations: Eavesdropping risks of computer displays," Tech. Rep. UCAM-CL-TR-577, University of Cambridge Computer Laboratory, 2003.
10. Vuagnoux, M. and S. Pasini, "An improved technique to discover compromising electromagnetic emanations," *Proc. 2010 IEEE Int. Symp. EMC*, Florida, USA, Jul. 2010.

11. Sekiguchi, H. and S. Seto, "Estimation of receivable distance for radiated disturbance containing information signal from information technology equipment," *Proc. 2011 IEEE Int. Symp. EMC*, California, USA, Aug. 2011.
12. Sekiguchi, H., "Measurement of radiated computer RGB signals," *Progress In Electromagnetics Research C*, Vol. 7, 1–12, 2009.
13. Sekiguchi, H. and S. Seto, "Measurement of computer RGB signals in conducted emission on power leads," *Progress In Electromagnetics Research C*, Vol. 7, 51–64, 2009.
14. Kuhn, M. G., "Filtered-tempest fonts," available: http://www.cl.cam.ac.uk/~mgk25/emsec/softtempest-faq.html.
15. Beyond IT Co., Ltd., CrypType, available: http://CrypType.com.
16. Suzuki, Y. and Y. Akiyama, "Jamming technique to prevent information leakage caused by unintentional emissions of PC video signals," *Proc. 2010 IEEE Int. Symp. EMC*, Florida, USA, Jul. 2010.
17. Watanabe, T., H. Nagayoshi, T. Urano, T. Uemura, and H. Sako, "Countermeasure for electromagnetic screen image leakage based on color mixing in human brain," *Proc. 2010 IEEE Int. Symp. EMC*, Florida, USA, Jul. 2010.
18. Sekiguchi, H., "Information leakage of input operation on touch screen monitors caused by electromagnetic noise," *Proc. 2010 IEEE Int. Symp. EMC*, Florida, USA, Jul. 2010.
19. Sekiguchi, H., "Software countermeasure technique against information leakage threat of button input operations in display image caused by radiated electromagnetic noise from information equipments," *IEICE Trans.*, Vol. J92-B, No. 7, 1113–1120, 2009, in Japanese.
20. "Monitor Timing Specifications, Version 1.0, Revision 0.8," Video Electronics Standards Association (VESA), 1998.