URSI AP-RASC 2019, New Delhi, India, 09 - 15 March 2019

Information leakage and simplified recovery from monitor

First A. Author(1), Second B. Author* (1), and Third C. Author(2)
(1) The ABC Company, Wash., DC, 20031, http://xxx.xxxx.xxx
(2) The Next Company, Neverland, USA

Abstract

TEMPEST studies how to recover screen information using electromagnetic fields leakaged by the monitor. Since the monitor is a screen for displaying the output of the peripheral device to the user, it is fatal to the user when the information is leaked. In the case of TEMPEST using autocorrelation function, the problem of inclination of the screen occurs, and improvement is needed. In this paper, a method is proposed that recovers the leakage signal of a monitor without using an autocorrelation function.

1. Introduction

Over the years, the use of various smart devices has increased. Because smart devices require monitor displays for human convenience, the demand for monitor displays increases. Because of the various uses of monitors, the security of screen information was essential and various studies are underway.[1,2]

The name of the study to recover the leak signal from the monitor is called TEMPEST. Information leakage by the electromagnetic imanations began with the van eck phreaking in 1985 [3]. The leakage electromagnetic waves generated by the monitor include screen information. This is because leakage information is instantaneously generated when the screen information, which is a form of digital signal, changes with time.

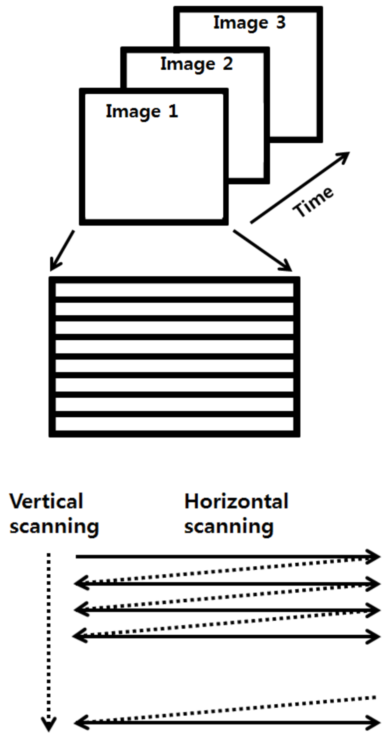
in this paper, The monitor is studied on the principle of operation of digital signal level and the method of restoring the screen information based on it is studied.

2. Introduction to Video Process

In order to perform TEMPEST using the electromagnetic waves leaked from the monitor, you should study the operation principle of the monitor. The input signals of the monitor are RGB, which is analog signal, and dvi, which is a digital signal. There are various kinds of panels such as LCD, LED and so on. However, the image signal passing through the FFC cable connected to the AD inverter and the LED panel uses the same restoration method regardless of the panel type, regardless of the input signal type.

In case of FFC cable, it is the longest transmission line on the monitor, so there is a characteristic that many electromagnetic waves are radiated. TEMPEST is studied by receiving electromagnetic waves radiated from FFC cable.

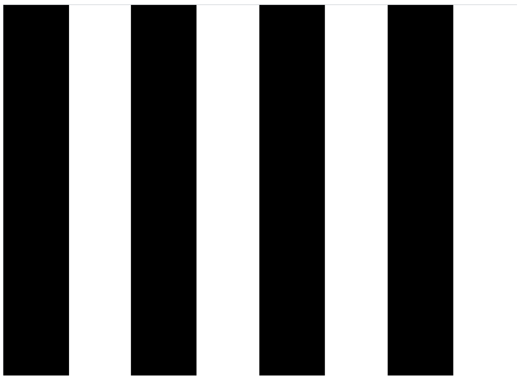
In the case of a video image, the picture look like a movie with a fast expression. To display small pixels in the picture, the monitor panel requires three pieces of data to represent the values of the color data red, blue, and green. And they are transmitted in parallel. Pixels are displayed one after the other, so when one row is filled, another is filled and a picture appears. Therefore, TEMPEST is studied by searching for the changed line. The cycle in which the rows change is called horizontal sync. If the location where the row changes does not appear, no information can be found on the recovered screen.



(a)

(b)

Figure 1. Schematic of monitor operation.



(a)

(b)

Figure 2. Tempest destination image.

3. Signal Processing for TEMPEST

The purpose of the tempest is to recover screen information using electromagnetic waves emitted from the monitor. Figure 2 (a) is that the data in all the rows of the monitor is the same shape. Therefore, Figure 2 (a) will be a very useful figure for understanding the correlation of electromagnetic waves and data generated by monitors, and it is suitable as verification material before restoring complex pictures.

Figure 2 (b) is a complex picture in terms of monitor screen restoration. Because the shape of the figure is very thin overall, a relatively small number of pixels represent different colors. The letters are in English, and the numbers next to the letters indicate the font size of the letter. The size of letter points is expressed in 32 ~ 6 point size. As a result, Figure 2. (b) is used to compare the effect of the slope on the screen and how small pixels can be recovered.

Figure 3 shows a portion of the electromagnetic waves emitted by the monitor with the screen shown in Figure 2 (a), and is the electromagnetic wave information emitted for 6 rows of image data. Since the data in all the rows in Figure 2 (a) are the same, the repeatability of the data in Figure 3 is shown.

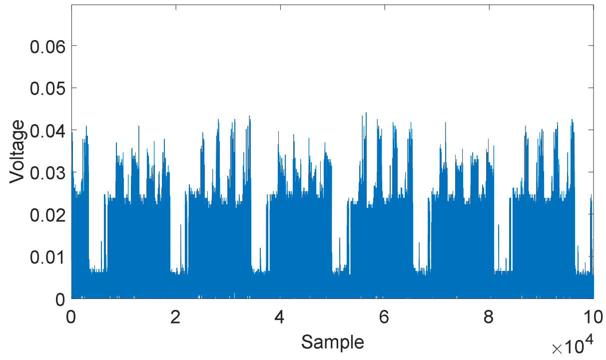
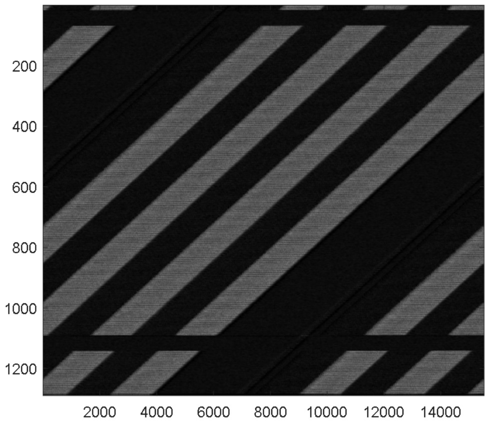


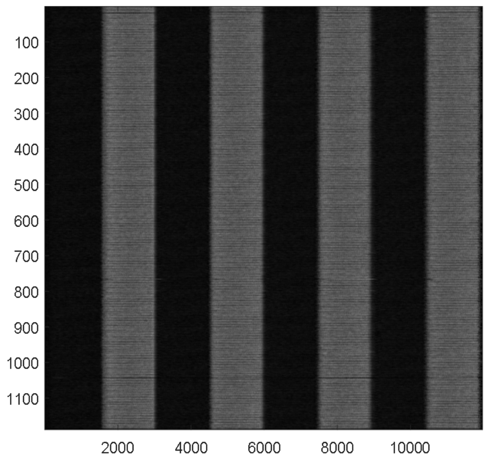
Figure 3. Electromagnetic waves leakaged from the monitor.

Figure 3 provides a variety of information. The most important information is information about the color of the pixel and information about the horizontal sync. In the case of color information, it can be seen from the amplitude of the emitted electromagnetic wave. However, since the data for RGB is displayed at the same time, it can not be classified and information about the correct color can not be obtained. As a result, the color difference is simply recovered to the black and white screen. Actual monitor operation is based on the horizontal sync signal and is expressed in a row. However, since the frequency of the horizontal synchronization signal is lower than the frequency of the RGB signal, it is difficult to obtain the electromagnetic wave generated by the horizontal synchronization. Hence, information on horizontal synchronization is obtained by analyzing electromagnetic waves emitted by RGB signals. Information about the horizontal sync signal is displayed in a blank position. An empty space is a virtual space where the panel can not be expressed to operate reliably, and the size of the RGB signal is zero. There is a very small amount of radiated electromagnetic radiation with a certain periodicity that is the location of the void space. Horizontal synchronization appears because the next image data is right behind the blank space. Therefore, the horizontal sync can be found without using the autocorrelation function.

Figure 4 and Figure 5 show the recovered monitor screen. Figure 4 shows the result of restoring the screen of Figure 2 (a). Figure 4 (a) shows the reconstruction method with slope and Figure 4 (b) shows the result of the reconstruction method without slope. Both (a) and (b) in Figure 4 can be deduced from the original data. The reason for the difference in the number of data between the two results is that the result of Figure 4 (b) is the restoration of the screen except for the blank space data. Figure 5 shows the result of restoring the screen of Figure 2 (b). Figure 5 also shows that (a) is the result with slope and (b) is the result of slope removal. In the results with relatively large letters, both (a) and (b) in Figure 5 can infer the original data. However, if the size of the character point is less than 20, it is difficult to deduce the original data in figure 5 (a).

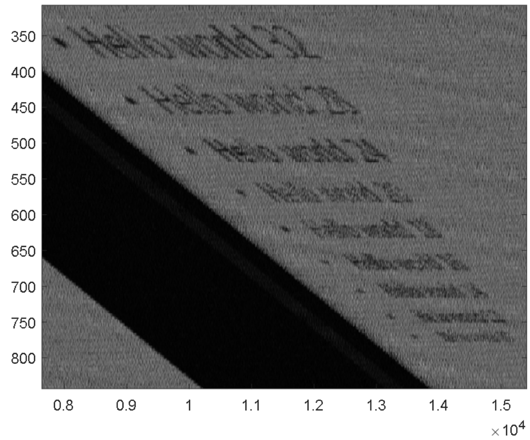


(a)

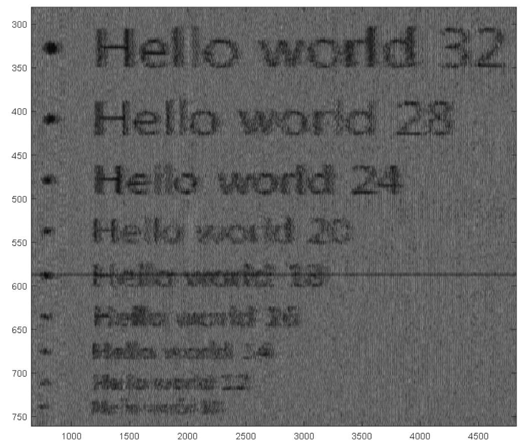


(b)

Figure 4. TEMPEST result of simple image.



(a)



(b)

Figure 5. TEMPEST result of complex image.

4. Conclusion

In this paper, Simplified screen restoration technique is studied through monitor operation and analysis of color data. As a result, in Figure 4 and Figure 5, the slope-free method of this paper and the conventional method are not significantly different when restoring large data, but differ when restoring small data. Therefore, it can be concluded that the method presented in the paper is useful. However, further research is necessary to overcome this problem, since the clarity of small letters is not clear in the restoration results.

5. References

1. Hayashi, Y., Homma, N., Miura, M., Aoki, T., and Sone, H., "A threat for tablet pcs in public space: Remote visualization of screen images using EM emanation," *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, November 2014, pp. 954-865, DOI:10.1145/2660267.2660292
2. Lee, H. S., Choi, D. H., Sim, K., & Yook, J. G., "Information Recovery Using Electromagnetic Emanations From Display Devices Under Realistic Environment," *IEEE Transactions on Electromagnetic Compatibility*, 99, July 2018, pp. 1-9. DOI:10.1109/TEMC.2018.2855448
3. Wim van Eck, ``Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?," Computers \& Security, 4, 1985, pp. 269-286.