Electromagnetic Information Leakage Detection for Computer Monitor

Mao Jian\textsuperscript{1,2}, Email: myjeans@sina.com
Liu Peiguo\textsuperscript{1}, Email: liu_jinming@126.com
Liu Jinming\textsuperscript{1,2}, Email: pg731@126.com
Han Zhenzhong\textsuperscript{1}, Email: 417668542@qq.com

1. College of Electronic Science and Engineering
   National University of Defense Technology
   Changsha, China
2. Computer Engineering College
   Jimei University
   Xiamen, China

Abstract

The computer monitors can generate the electromagnetic information leakage, which is related to the display principle. The refresh rate, the horizontal frequency, and the pixel frequency were confirmed as the key factors to reproduce the video images showed on the monitor from the electromagnetic radiation. To estimate the risk of information leakage, a detection method based on display principle was introduced. The method is to distinguish and match the spectrum interval from the radiated electromagnetic signals by multi-resolution spectrum analysis. The experiments under different circumstances have proved this method is effective by using a set of simple devices.

Key Words

Electromagnetic radiation, information leakage, information security, spectrum analysis, computer monitor

1. Introduction

Electromagnetic (EM) radiation will occur unintentionally when electronic information equipment is working, which can lead to information leakage [1]-[4]. It has been proved that the video information
showed on a computer monitor can be secretly eavesdropped and reconstructed without physical contact [5], [6]. Considering this potential security threat, it needs some means to detect whether or not the information leakage risk exists in the target electronic equipment.

In previous work, EM information leakage research usually focused on video or image reconstruction [7]-[13]. To obtain the high-quality images, wide-band signal receiver or some other reconstruction devices should be needed. However, for most electronic equipment users, information security is more valuable than information eavesdropping. For this reason, this paper introduces an effective method to detect the risk of information leakage on the monitor. The detection method is based on the displaying principle of monitor and implemented with a single signal analyzer.

2. Display Principle of Monitor

It is known that EM information leakage is closely related to the working frequency of the electronic equipment [14]. The working frequency and its harmonic tend to be the source of EM leakage. When the target equipment is the monitor, it means that analyzing the displaying principle and finding working frequency is vital for the leakage detection.

According to the monitor timing standard provided by video electronics standards association (VESA)[15], the working frequencies of monitor include refresh rate, horizontal frequency, and pixel frequency.
For a monitor with the resolution of $M \times N$, as shown in Fig.1, a frame of active video is composed of $N$ lines and $M$ pixels for each line. The monitor uses progressive scan technology to display the video. Actually, an integrated video frame includes not only the active video lines but also some transition lines on both sides, such as the top and bottom borders, and the blank area. The integrated video frames are synchronized with the vertical sync signal, as can be seen in the Fig.2. The frequency of vertical sync signal is defined as refresh rate, which is the reciprocal of the vertical sync time. In a frame, the pixel lines is showed from top to bottom on the screen. Similarly with the video frame, the video line also contains a few transitional pixels, as shown in the Fig.3. The pixel lines are synchronized with the horizontal sync signal, whose frequency is called as horizontal frequency. And in each line, the pixels are scanned and displayed sequentially according to the order from the left to the right. The rate of scanning each pixel is defined as the pixel frequency. VESA industry standards for computer display monitor timing have provided the formats of working frequencies in different resolutions. Table 1 shows three familiar formats of the monitor display.

<table>
<thead>
<tr>
<th>Resolution</th>
<th>Refresh Rate</th>
<th>Horizontal Frequency</th>
<th>Pixel Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>$800 \times 600$</td>
<td>60 Hz</td>
<td>37.9 KHz</td>
<td>40 MHz</td>
</tr>
<tr>
<td>$1024 \times 768$</td>
<td>60 Hz</td>
<td>48.4 KHz</td>
<td>65 MHz</td>
</tr>
<tr>
<td>$1280 \times 1024$</td>
<td>60 Hz</td>
<td>64.0 KHz</td>
<td>108 MHz</td>
</tr>
</tbody>
</table>
Obviously, there is a certain relationship among the three working frequencies of the monitor. The refresh rate and horizontal frequency both are determined by the pixel frequency. The pixel frequency is the fundamental frequency which comes from the crystal oscillator of the monitor. The horizontal frequency can be considered the divided pixel frequency. And after the second frequency division, the frequency is reduced to the refresh rate, as shown in Fig.4.
3. Method of EM information leakage detection

When the monitor is displaying the video, the three working frequencies described in the previous section are used as sync signals to modulate one-dimensional pixel sequences to two-dimensional videos on the screen. At the same time, the process of displaying video can generate the EM radiation that contains the video information. On the contrary, for the eavesdropper, it is necessary to capture the working frequencies as sync signals to demodulate radiated spectrum signals to reconstruct the video information. And the working frequencies themselves are the important information about the monitor’s performance, which can be used to deduce the type of the monitor. All these can make the eavesdropping easier. Therefore, whether can obtain the working frequencies or their time-domain signals should judge whether the monitor is in the risk of EM information leakage.

Because the sync signals of the monitor are periodic, so they can be expressed in terms of the Fourier series:

\[ S(t) = \sum_{n=-\infty}^{\infty} F_n e^{jnt} \]  

(1)

\( S(t) \) is the sync signal, in theory, which can be regard as the periodic rectangular signal. \( \omega \) is the angular frequency of the signal, which can be calculated with the signal period \( T_s \) or the frequency \( f_s \), as described in the following equation:

\[ \omega = 2\pi/T_s = 2\pi f_s \]  

(2)

The Fourier coefficients can be calculated by the following formula:

\[ F_n = \frac{1}{T_s} \int_{-T_s/2}^{T_s/2} S(t)e^{-jnt} dt \]  

(3)
The frequency-domain form of the signal \( S(f) \) can be obtained by the Fourier Transform:

\[
S(f) = \sum_{n=-\infty}^{\infty} F_n \int_{-\infty}^{\infty} e^{j2\pi(n-f)\tau} d\tau = \sum_{n=-\infty}^{\infty} F_n \delta(f - f_n)
\]  

(4)

As can be seen in (4), the sync signal is discrete with the interval of \( f_s \) in the form of spectrum. For the vertical sync signal, the spectrum should be arranged at the regular interval, which is matched for the refresh rate. And the horizontal frequency should correspond to the spectrum spacing of horizontal sync signal. The radiation energy of sync signal is usually stronger than other signals, so the regular interval feature of spectrum can be detected easily.

The information leakage detection of the monitor is based on the seeking the equal interval feature of the radiated spectrum, which came from the sync signals. The working frequencies of the monitor are in different orders of magnitude. As can be seen in Table 1, the value of horizontal frequency is about one thousand times of refresh rate, and the value of pixel frequency is more than one thousand times of horizontal frequency. So the detection should be carried out on different spectrum resolutions to match the corresponding magnitudes of working frequencies.

The detection method can be described as following steps:

1) Scan the radiated spectrum with 1 MHz resolution bandwidth (RBW), search for the peak frequency as the possible EM leakage point, and set it as the center frequency. If all the peaks are excluded from leakage points by the step 2 and 3, the monitor can be regarded as safe equipment about the EM information security.

2) Change the RBW to 1 KHz and scan spectrum with 1 MHz span, distinguish whether the spectrum has uniformly-spaced lines. If it has, search for the new peak and set it as new center frequency, else return
to step 1.

3) Judge whether the spectrum is still uniformly-spaced with 1 KHz span and narrower RBW. If yes, the current center frequency is the EM leakage point, and the monitor is facing the risk of information leakage. If not, return to step 2.

Through the regular interval judgments with different spectrum resolutions, the method can determine whether the monitor is under the threat about EM information security. And the two possible spectrum intervals should be connected with horizontal frequency and refresh rate. By them, the video resolution could be speculated so that the video images might be reconstructed from the spectrum signals.

4. Experiment
The experiment was carried out in a normal indoor environment without shielding measures. Fig.5 shows the experiment system of EM information leakage detection which consists of the computer monitor, the signal detector, and the signal analyzer. As the test target, the type of monitor is LG L1753T. The signal detector is a TEMPEST current monitoring probe. The detector can capture the EM radiation from the VGA cable which connected the working monitor. The signal analyzer is an Agilent PXA N9030A, which is used to analyze and save the spectrum signals radiated from the monitor.

![Experiment devices](image)

Figure 5. Experiment devices.

4.1 EM Information Leakage Detection
In this experiment, the monitor was displaying video with the resolution of $1024 \times 768$ and the refresh rate
of 60 Hz. As can be seen in the Table 1, the horizontal frequency should be 48.4 KHz, and the pixel frequency is 65 MHz.

According to the detection method, the signal analyzer scanned the leaked spectrum from 10 MHz to 50 MHz with the RBW of 1 MHz. The result of scanning is shown in Fig.6. There is obvious signal fluctuation can be seen in the spectrum. It means that EM information leakage possibly occurred in this frequency band. After scanning, 26.89 MHz was locked as the peak frequency. Next, 26.89 MHz was set as the center frequency with the 1 MHz span and 1 KHz RBW to carry out the second spectrum scanning. As shown in the Fig.7, the periodic feature can be found in the scanning result. The peaks of the spectrum are partly periodic, and the spacing between the neighboring spectral peaks is about 50 KHz, which is matched for the horizontal frequency. So the current spectrum could be further expanded with the 1 KHz span and 1 Hz RBW, as shown in the Fig.8. It can be seen that the spectrum is nearly periodic from 26889.62 KHz to 26890.22 KHz. And the period is about 60 Hz, which is equal to the refresh rate. By these operations, the working frequencies belong to the target monitor was detected. That means the useful information has leaked from the monitor through the EM radiation. By this experiment, the detection method was verified to be feasible.

![Figure 6. The spectrum between 10 MHz and 50 MHz.](image)
If a signal receiver was integrated into the detection system for the time-frequency signal acquisition, the original video image could be reconstructed based on the leakage frequency and the monitor working frequencies that have been detected, as shown in the Fig.9. Actually, for the information security, the detection method is enough to identify the existence of EM information leakage without the further information reconstruction.
4.2 Horizontal Frequency Detection under Different Display Formats

In the result of previous experiment, as shown in the Fig.7, the interval between the spectrum peaks is matched for the horizontal frequency of monitor with the $1024 \times 768$ resolution. To verify the relationship between the display format and the leaked spectrum, the experiments were repeated in the conditions of other two display resolutions.

The first test was carried out with the 1st format of monitor timing standard in the Table 1. The target monitor was set as the resolution of $800 \times 600$ and the refresh rate of 60 Hz. The signal analyzer processed the leaked spectrum in the center frequency of 15.947 MHz and the RBW of 110 Hz. The spectrum is shown in the Fig.10. Several dash lines were drawn in the interval of 37.9 KHz which is the horizontal frequency of the current display format. It is obvious that the positions of the spectrum peaks are exactly consistent with the dash lines. So the periodic spacing of spectrum peaks is just the horizontal frequency.

And the second test was operated almost under the same circumstance except that the resolution had been reset as $1280 \times 1024$. According to the standard of display format, the horizontal frequency should be changed to 64.0 KHz. The test reconfirmed that the periodic spacing of spectrum peaks is exactly consistent with the horizontal frequency, as shown in the Fig.11, in which the interval of dash lines is 64.0 KHz.

The results of two tests proved that the leaked spectrum are closely related with the display format of the monitor, and the horizontal frequency can be easily obtained by the spectrum analyzing. As a key information of the computer monitor, the horizontal frequency can be used to deduce the other performance indicators of the monitor, such as the display resolution. The validity of the detection method was confirmed again by the tests.
5. Conclusion

Based on the display principle of the monitor, a method of EM information leakage detection has been introduced in this paper. The method used the multi-resolution analysis to find the equal interval feature of radiated EM spectrum. The experiment results showed that the information about working frequencies of the electronic equipment can be extracted effectively by this method. So the detection method can be used for seeking security holes of electronic display device to prevent the EM information leakage risk.

References


and Intelligent Systems, 43(2), 2015.