Front. Electr. Electron. Eng. China 2010, 5(2): 143–146
DOI 10.1007/s11460-010-0014-1

RESEARCH ARTICLE

Wenhan YANG, Yinghua LU, Jun XU

Video information recovery from EM leakage of computers based on storage oscilloscope

Abstract A hardware platform using broadband antenna, oscilloscope, and spectrum analyzer is designed to receive radio frequency (RF) signals from electromagnetic radiation leakage of computers in the office environment. The process of receiving and the processing techniques have also been given. Then, the software radio-based computing models and software algorithms are proposed to demodulate and decode the RF signals. An experimental result shows that the text information can be recovered from electromagnetic (EM) leakage wave of computer by this interception system. This architecture not only reduces the cost of the system's hardware but also makes interception more flexible. The innovation points of this paper are recovering the video information in EM leakage wave of computers in an ordinary office environment based on public equipments and proposing the process of receiving processing techniques that only use the software radio-based computing models and software algorithms.

Keywords Transmitted Electromagnetic Pulse/Energy Standards and Testing (TEMPEST), electromagnetic leakage wave, video information recovering, software radio

1 Introduction

Reference [1] shows that display information leakage caused by electromagnetic radiation can be recovered very easily. Since then, people have done a series of experiments proving that electromagnetic radiation from data lines, hard drives, crystal ray tube (CRT), and central processing unit (CPU) could lead to information leakage [2–10]. In Refs. [3–10], the electromagnetic radiation is obtained through broadband antenna receiver, filtering, amplifying, analog-to-digital (A/D), etc. Then, the information is obtained by processing the digital signals through correlated filtering, recognition and reconstruction technology, etc. The experienced operators who adjust the intermediate frequency (IF) and bandwidth of receiver are always needed because the frequency, modulation, and other parameters of radiation signal are always unknown. The performance of video information interception will be directly affected by the receiver's capability, so high-performance broadband receivers (such as Dynamic Sciences R-1250) are used in Refs. [3,4,10]. The high-performance receiver is very expensive and also bulky in general, so the interception system based on it is not only high-cost and difficult to manufacture but also hard to buy.

In 1992, Joseph Mitola III introduced to the world the software-defined radio (SDR) concept. The kernel idea is to construct an open, standardized, and modular hardware platform in which the A/D and D/A converter are close to the antenna, and, using software to perform various functions in order to develop an open radio communication system with high flexibility [11].

Based on this idea, this paper built a hardware platform using a broadband antenna, a preamplifier, a spectrum analyzer, and an oscilloscope to receive video radio frequency (RF) signals and then demodulate and decode the digital signals by using computer software. At last, recover the texts message from electromagnetic (EM) leakage.

Without the high-performance receiver and specialized hardware, only general laboratory electronic test equipments are used in this interception system. Thus, Transmitted Electromagnetic Pulse/Energy Standards and Testing (TEMPEST) engineers can focus their work on the demodulation and decoding of leakage information, and let the electric engineers who design general test equipments improve the performance of the hardware platform. Video interception will also benefit greatly from processing the RF digital signals by using digital signal processing technology. For example, the IF and bandwidth of the interception can be obtained by using spectrum identify algorithm. Therefore, the experienced operators can be replaced by software, and the automation of the system can be improved.

Received January 30, 2010; accepted March 9, 2010

Wenhan YANG (✉), Yinghua LU, Jun XU
School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China
E-mail: Ywh.168@163.com

2 TEMPEST test in office environment

In this paper, we study on the text messages recovery from EM leakage of computers in office environment. The research object is a computer which is in the 640×480@60 Hz video mode, and we let CRT display a full screen picture filled with text.

Test equipments: oscilloscope (Tektronix TDS5054B), spectrum analyzer (HP8594), broadband antennas, pre-amplifier (Langer EMV-Technik PA 303), and computer.

First, we should identify the computer video signal from the complex electromagnetic environment and extract the frequency and bandwidth parameters by analysis of the spectrum of the RF signals received.

Step 1 Test the environmental spectrum when the computer is shut down.

Step 2 Test the RF signals' spectrum when the computer displays a picture.

The results are shown in Fig. 1, the red line is for the RF signals' spectrum, and the blue one is for the environmental spectrum. By comparison, we can identify that the RF signals of the video radiation is shown as the green color below.

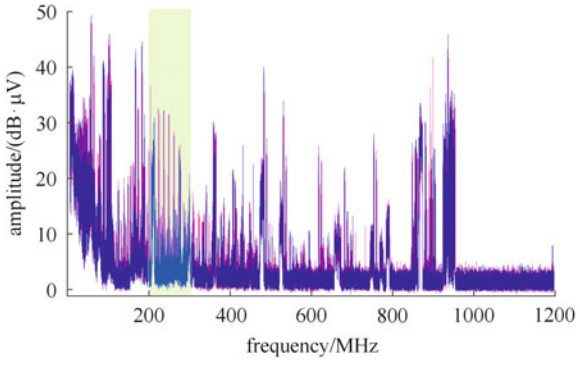

Fig. 1 Spectrum of received RF signal

After recognizing the leakage waves from the computer, we take the single color signals in 0.04 s period time by using the oscilloscope with 500 MHz digital sampling. Then, the horizontal and vertical synchronization of the video image signal can be got by using fast Fourier transform (FFT). The results are shown in Fig. 2.

In Fig. 2, we can find that the spectrum of the baseband video signal by FFT includes the field frequency, 60 Hz, line frequency, 31.32 kHz, and the point frequency, 25 MHz of the video signals. Analyzing this spectrum, we can find the following parameters: the field time period of the video picture, 1.76 ms, and the main frequency pattern width of it, 568 Hz; the line time period of the video picture, 6.9 μs, and the main frequency pattern width of it, 144.93 kHz, the point time period of the video picture, 40 ns, and the main

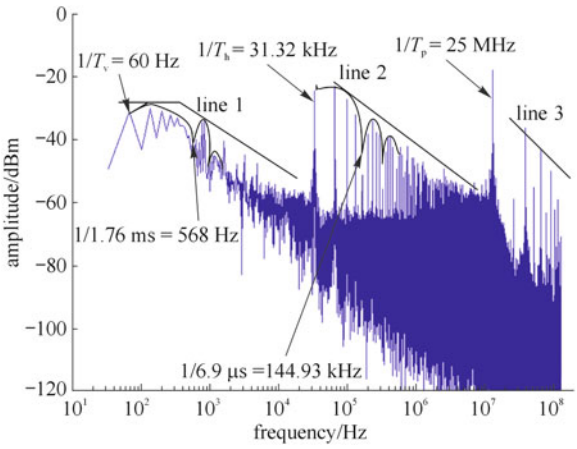

Fig. 2 Spectrum of baseband video signal by FFT

frequency pattern width of it, 25 MHz. We can find the means of the approximation lines in the spectrum, which are as follows: line 1 includes the frequency parameter of the field of the video picture; line 2 includes the frequency parameter of the line of the video picture; and line 3 includes the frequency parameter of the point of the video picture.

3 Text recovery

The traditional reproduction flow of electromagnetic leakage of information [9] is shown in Fig. 3. The electromagnetic radiation can be obtained through broad bandwidth antenna receiver, tuning, bandpass amplification, synchronization, phase locking, A/D, etc. When the control signals of row and frame frequency are picked up, the electromagnetic leakage should be processed through averaging filtering, recognition, reconstruction technology, etc. Then, the recovered word image can be obtained.

The reproduction process used in this paper is shown in Fig. 4. There are two dissimilarities between it and the traditional one. A/D converter is much close to antenna, and the analog processing units are replaced by the software processing. The hardware platform not only receives the radiation of computer video signals but also the radiation of universal serial bus (USB) cable, CPU, hard drive, keyboard, etc. Thus, we can analyze and restore the various information that leak from computers by modifying the software algorithm.

The decoding process is shown in Fig. 4, and the waveforms of digital signal processing are shown in Fig. 5. The analog RF signal is changed to digital signal (Fig. 5(a)) by the storage oscilloscope. We can find that the video information is completely submerged in the noise. Then, the video IF signal (Fig. 5(b)) can be obtained through a bandpass filter. The vertical blanking is so clear in the video IF signal. Finally, we can obtain the baseband video

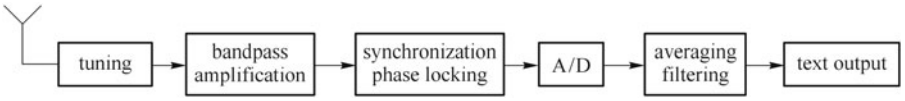

Fig. 3 Reconstruction flow of EM leakage of information from a computer

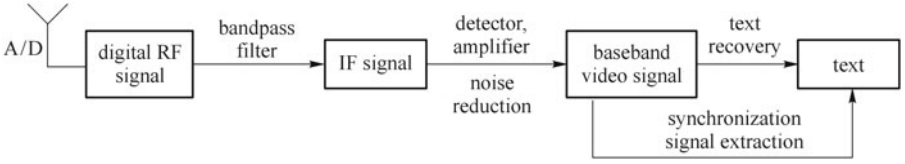

Fig. 4 SDR reconstruction flow of EM leakage of information from a computer

signal (Fig. 5(c)) through detection, amplification, and noise reduction.

We should extract the horizontal and vertical synchronization by analyzing the spectrum of video signal [9,12] before text recovery. In this paper, the period of horizontal and vertical sync are recorded as T_{h} and T_{v}. Finally, text messages can be recovered according to sync signal.

Video signal can be expressed as follows:

$$S_{\mathrm{P}}(t) = \sum_{n=-\infty}^{+\infty} a_n g_{\mathrm{T}}(t - nT_{\mathrm{p}}), \tag{1}$$

where $g_{\mathrm{T}}(t)$ is the trapezoidal pulse whose width is T_{p} and amplitude is 1. For the gray image of 256 levels, a_n is one of the 256 discrete values within the range of 0–0.7 V, where 0 indicates that the pixel is black, and 0.7 indicates white. Decoding is to restore the one-dimensional signal in time domain into two-dimensional images. First, resample the signal to sequence a_n by the rate of $1/T_{\mathrm{p}}$. Then, arranged the sequence a_n to a series of $x_{\mathrm{t}} \times y_{\mathrm{t}}$ ($x_{\mathrm{t}} = T_{\mathrm{h}}/T_{\mathrm{p}}$, $y_{\mathrm{t}} = T_{\mathrm{v}}/T_{\mathrm{h}}$) pixels images. At last, we can obtain the video information by showing these pictures in order at the speed of $1/T_{\mathrm{v}}$.

Traditional method first generated the horizontal and vertical sync pulses by hardware, and then, acquisition equipment can recover images by controlling the sampling and framing according to the sync pulses. Different from the traditional one, this paper restores the video information only using software. Figure 6 illustrates that the words have been recovered from EM leakage.

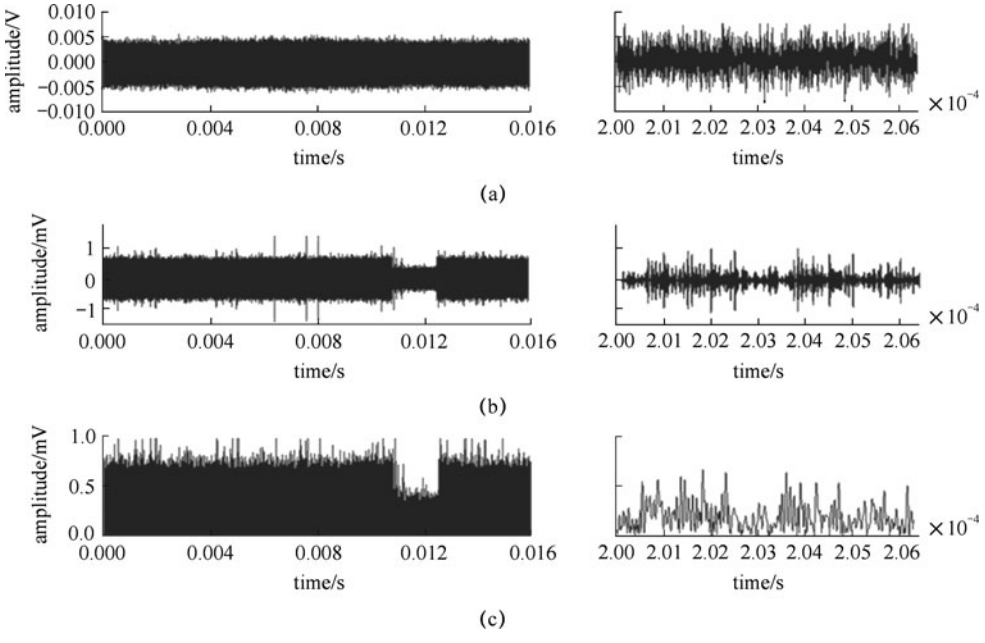

Fig. 5 Signal processing. (a) Received RF signal; (b) video IF signal; (c) baseband video signal

Fig. 6 Words image recovered from electromagnetic leakage

4 Conclusion

This paper sets up a hardware platform by using public equipment, such as broadband antenna, oscilloscope, and spectrum analyzer, and recovers the text image from EM leakage of computers in the office environment effectively. The process of receiving and the processing techniques are also given. Then, the software radio-based computing models and software algorithms are proposed to demodulate and decode the RF signals. An experimental result shows that the text information can be recovered from EM leakage wave of computer by this interception system. This architecture not only reduces the cost of the system's hardware but also makes interception more flexible. The innovation points of this paper are recovering the video information in EM leakage wave of computers in an ordinary office environment based on public equipment and proposing the process of receiving processing techniques that only use the software radio-based computing models and software algorithms.

Acknowledgements This work was supported by the National Natural Science Foundation of China (Grant Nos. 60871081, 60671055, and 60771060), and the Specialized Research Fund for the Doctoral Program of Higher Education of China (Nos. 20070013002 and 20070013004).

References

1. Van Eck W. Electromagnetic radiation from video display units: an eavesdropping risk? Computers and Security, 1985, 4(4): 269–286
2. Smulders P. The threat of information theft by reception of electromagnetic radiation from RS-232 cables. Computers and Security, 1990, 9(1): 53–58
3. Kuhn M G, Anderson R J. Soft tempest: hidden data transmission using electromagnetic emanations. In: Proceedings of the Second International Workshop on Information Hiding. 1998, 124–142
4. Kuhn M G. Compromising Emanations: Eavesdropping Risks of Computer Displays. University of Cambridge (Computer Laboratory) Technical Report 577. 2003
5. Kuhn M G. Optical time-domain eavesdropping risks of CRT displays. In: Proceedings of the 2002 IEEE Symposium on Security and Privacy. 2002, 3–18
6. Zhong H X, Lu Y H, Bao Y F. The study on the electromagnetic radiation from the aperture on coaxial cable based on FDTD/MoM method. Journal of Beijing University of Posts and Telecommunications, 2004, 27(2): 61–65 (in Chinese)
7. Zhang H X, Lu Y H, Han Y N, Qiu Y C. Study on information reconcilability of electromagnetic radiation arising from computer. Chinese Journal of Radio Science, 2004, 19(5): 553–559 (in Chinese)
8. Lu L, Nie Y, Zhang H J. The electromagnetic leakage and protection for computer. In: Proceedings of 1997 International Symposium on Electromagnetic Compatibility. 1997, 378–382
9. Zhang H X, Lu Y H, He P F, Wang H X. Text recovery from EM leakage of computers. Journal of Southwest Jiaotong University, 2007, 42(6): 653–658 (in Chinese)
10. Tanaka H, Takizawa O, Yamamura A. A trial of the interception of display image using emanation of electromagnetic wave. Journal of the National Institute of Information and Communications Technology, 2005, 52(1/2): 213–223
11. Yang X N, Lou C Y, Xu J L. Theory and Application of Software Radio. Beijing: Publishing House of Electronics Industry, 2001 (in Chinese)
12. Xiang C B, Zhang H Z, Song J Z, Qiao S. Automatic synchronous signal extraction and steady display of non standard video information. Journal of Data Acquisition & Processing, 2007, 22 (4): 486–490 (in Chinese)