Modern Applied Science
www.ccsenet.org/mas.html
Vol. 1, No. 2
July 2007

Reconstruction of Video Electromagnetic Leakage from Computer

Bo Hu
Department of Physics and Electronics, Binzhou University, Binzhou 256603, China
Tel: 86-543-319 1767 E-mail: hubobz@163.com

Abstract

TEMPEST technology has been concerned much more in recent years. Video Displayer Unit, which is one of the most import parts that may result in computer information leakage, offers the interface for man-machine conversation directly and its video electromagnetic radiation contains the displaying information. The interception and recovery system of video electromagnetic information leakage of the computer is designed. After the electromagnetic leakage is intercepted, the method to recover the word image is presented using the reconstruction techniques such as synchronization, related filtering, phase lock on etc. This means that the original useful information can be reconstructed by the electromagnetic leakage under certain conditions, and this will menace information security. It is one of the most important factors that should be concerned in information security and electronic antagonism fields.

Keywords: TEMPEST, Electromagnetic Radiation, Electromagnetic leakage, Filtering, Information Reconstruction

1. Introduction

Electronic equipments deal with data information by controlling the changes of electric current (or voltage). But the time-variant electric current will bring electromagnetic radiation which contains abundant frequency spectrum and information that can be unscrambled.

According to the investigation and analysis from the domestic and aboard if the radioactive electromagnetic wave is detected and intercepted the digit signal can be abstracted. As a result, it will cause information leaking by means of reproduce the original information. Therefore, it is one of the key technologies to reduce or remove the problem of information leaking caused by electromagnetic radiation .The video information radiation from electromagnetic radiation coming with the working computer can received the transmitting signals can be monitored .The emission of electromagnetism has two main influences on the information technologic equipment: the first one is the electromagnetic disturbing and information leaking caused by the electromagnetic emission of their own ,the other the disturbing and destroying from outside. The two kinds of influences have not only the problem of electromagnetic disturbing but also the problem of information leaking. TEMPEST, advanced during 1980s is a technology based on computer information leaking. It is a new technique developed from the field of electromagnetic annexation bringing great threaten to the information safety. Acquiring the intelligence from the leakage from TEMPEST is one of important methods used by ELINT to get information .In the Bay-War happened in 1991, America used the most advanced TEMPEST technique to intercept and capture the intelligence about politics ,military affairs and economy of Iraq and Bay area. Although the TEMPEST technique is based on the principle of electromagnetic radiation, it pays more attention to abstract useful information handling and identifying to deal with this useful information. The computer system is the most important component of various information technique devices, so it is the primary research objective among all the TEMPEST technique problems. The computer's make up circuits are complex and contain many kinds of clock information, all of which exist electromagnetic radiation to a certain degree. The sources of radiation can be divided into CPU, communication circuits, and transform equipments, output devices and so on...All of them will lead to information leaking phenomenon. These leakages contain synchronism signal, clock signal, digit signal, being processing and information being displayed on the screen.

From the middle age of 1980s, our country has begun to research on TEMPEST. In the early age of 1990s, several internal units researched some key-pointing problems of TEMPEST technique and got many important achievements on many subjects, for example: computer information leakage and principle of protection from it, the technique of receiving and receiving and restoring micro-mini computer radioactive information, safety evaluation, the test of technical production, laboratory and scene testing, distinguishing from red and black signals, the technique of electromagnetic leakage protection in micro-mini computer system, and so on. In 1980s in the nationwide exhibition of computer application, the department of public security demonstrated that they reappeared the showing content of micro-mini computer's screen on TV's screen by using TV receiving antenna to aim at the computer. Xi'an electronic technique university and so on used black-and-white television to receive screen information. Changchun light machine office of Chinese Academy of Science carried out the interception and reappearance about the video leaking information of the computer whose showing method is CGA. The receiving scope is usually limited to about 3 meters for reappearing display text information by means of black-and-white television structure. But Van.Eck came up in his thesis that it can receive and deoxidize the video frequency information among 1000 meters. During 1990s, English reported that they can receive and deoxidize information in 1600m.In comparison, Beijing Postal and label services university carried out a receiving machine which realized the reappearance of computer word leakage and got word reseen picture located at far range. In 2004, the university completed a simulation platform, which was used to reappearance computer video electro magnetic linking information and realize the ration evaluation about the leaking threshold of information and the reinforcing function of computer.

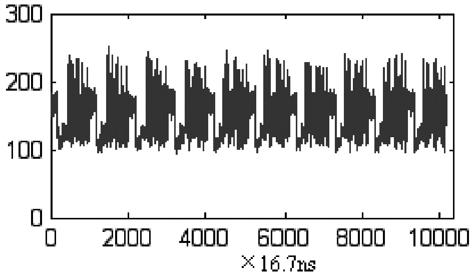
Through the video frequency channel we can realize the communication between man and computer directly. The reason why the video frequency signal is a main scores of information leakage is that the electromagnetic leakage caused by video signal radiation including useful information that can be recognized an abstract easily. Regarding the character information, they are random digit signal can produce electromagnetic radiation easily an take on wide frequency spectrum area owning to there are more causes and components caused information leakage this article have design the system method for the computer electromagnetic leakage. Dealing with the real data use many technique like synchronism, related filtering, phase lock and so on to obtain the word and image reappearance from electromagnetic leakage.

From the research we can discovery the electromagnetism radiation caused by digit pulse video frequency signal processing a wide frequency spectrum area. In addition, owning to the effect of muti-patches effect will be neglected under strong noise when transmitting through the wireless channel. At the same time the signal has been deformed. Because the received video signal radiation has low S/N, wide spectrum and will be deformed, so to capture and deal with the electromagnetism leakage information is different from to receive and do with the classical communication signal either in theory or in technique. In this article, when the electromagnetic leakage from computer captured, the technique of abstracting the filed synchronism signal and row synchronism signal, phase clock, related filtering, be used to reappear the word image of common song-character displaying on the computer screen away from 10 miters. It's a breakthrough to the recorder of the distance researched about the leakage information.

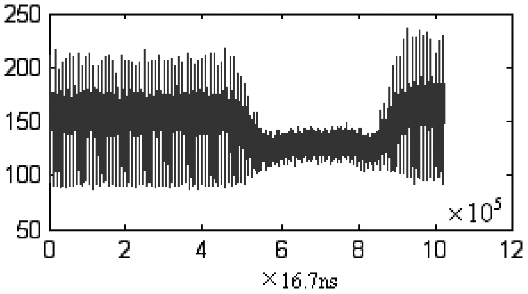
2. The Distill of the Synchronous Signal in Electromagnetic Leakage

The references [21,22] gave the metrical results of the Electromagnetic Leakage. In this paper, we designed the frame of interception and rebuild of the Electromagnetic Leakage information. After the interception with the help of the wide-band antenna, the information was transferred into digital. The signal processing was finished by software applications. The sample rate of the system is 60M.

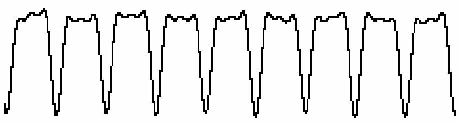
In the near filed, to output though amplify, demodulation and detector after digital sampling, we could get the character signal of Electromagnetic Leakage when computer display character information near the receive center frequency. Which sketch 2(a)(b) is field synchronous information and row synchronous information of Electromagnetic Leakage information separately, sketch 2(c)(d) is field synchronous signals and row synchronous signals which is abstracted by Electromagnetic Leakage information. Sketch 2(e) is one row of the video signal of Electromagnetic Leakage information; sketch 2(f) is the abstracting video signal after signal processing. corresponding to sketch 2(e) which vertical is relative amplitude of the Electromagnetic Leakage information after signal processing, horizontal is the number of sampling point corresponding to the time is 16.7 ns.



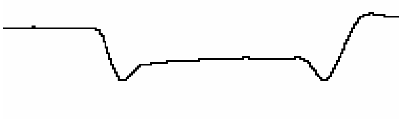
the row synchronous character information of the Electromagnetic Leakage information.



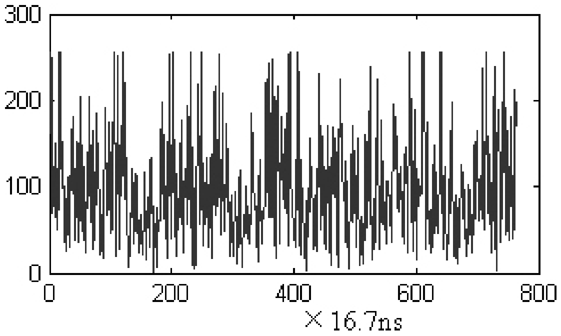
the filed synchronous character information of the Electromagnetic Leakage information.



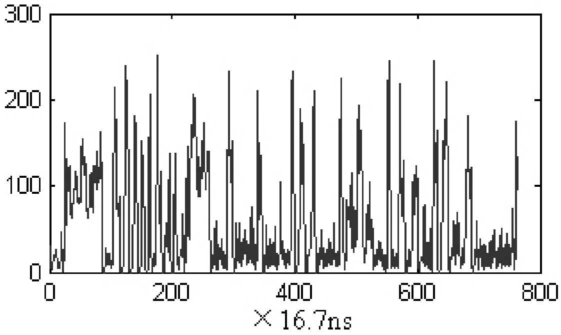
the row synchronous signal abstracted from Electromagnetic Leakage information.



the filled synchronous signal abstracted from Electromagnetic Leakage information.



The video signal leaked from character information and picture information.



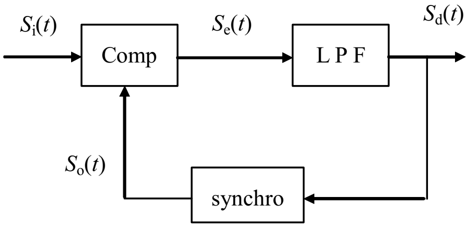
The video signal abstracted after signal processing.

3. The Technology of Signal Processing

3.1 The principle of phase lock on

The recovery technology of get field synchronous signals and row synchronous signals though signal processing of the collected Electromagnetic Leakage from Computer is one of the key technology of Electromagnetic Leakage's Reconstruction. To make the field synchronous signals and row synchronous signals steady ,we adopt the digital phase lock on: technology, make use of phase lock on loop circuit accurate fix the output synchronous signals position. The basic of the structure of phase lock on such as the sketch 3.It consist of 3 base component part:

comparer, LPF, and synchronous signals producer (synchronous circuit), the input signals is the field synchronous signals and row synchronous signals which is picked up by receiver. The comparer compare the input signals Si(t)and the output synchronous signals So(t) which pass the circuit. Product error voltage Se(t) corresponding to two signals. The function of LPF is filter the high frequency component and noise of the error voltage Se(t), the purpose is to ensure the functions which is needed by the loop, and enhance the stability of system. The synchronous circuit is controlled by the control voltage Sd(t). make the synchronous signals approach to the input signals, until clearing the error to lock on.



Sketch 3 digital look on principle

3.2 correlate filter wave

We could adopt the measure called shifting of function enhance the SNR to reduce noise. Assume the signal include noise is

$$x(t) = s(t) + n(t) \tag{1}$$

Which s(t) is the signal whose circle is T, n(t) is the independent white noise whose average value is 0, square different is .The input signal SNR is :

$$SNR_i = W / \delta^2 \tag{2}$$

Assume the frame frequency of monitor is M, so the output of the system after following operation as following:

$$y(t)=\frac{1}{M}\sum_{k=1}^{M}x(t+kT)=s(t)+\sum_{k=1}^{M}n(t+kT)=s(t)+N(t) \tag{3}$$

Which N(t) is measure err Its average value is obvious 0.its square err is

$$\sigma = D\left[N(t)\right]=\frac{1}{M}\sum_{k=1}^{M}E\left[n(t+T)^2\right]=\frac{\delta^2}{M} \tag{4}$$

Now, the processed SNR is

$$SNR_o = \frac{W}{\sigma} = M \cdot SNR_i \tag{5}$$

It is thus clear that SNR increase M times. It is easy to protect the pass function is

$$\left|H(\omega)\right| = \frac{1}{M}\left|\frac{1-e^{-jNM\omega\Delta t}}{1-e^{-jN\omega\Delta t}}\right| = \frac{1}{M}\left|\frac{\sin(\pi M\omega/\omega_0)}{\sin(\pi\omega/\omega_0)}\right| \tag{6}$$

it is thus clear that the gain of pass function of the filter when w=kw0,This process is equal to comb filter whose central frequency is w=kw0, called correlate filter.

3.3 matching filter

Matching filter could be considered one correlate device which accurate input signals correlate function. The shape of wave become autocorrelation integral shape after passing match filter, and it is symmetrical about point t=t0.

t0 is also the maximum point of the output signal. Consider the output signal is so(t) :

$$s_0(t) = \int_{-\infty}^{\infty} s(t-u)Ks(t_0-u)du \tag{7}$$