*Available online www.jocpr.com*

**Journal of Chemical and Pharmaceutical Research, 2014, 6(5):210-217**

**Research Article**

**ISSN : 0975-7384**
**CODEN(USA) : JCPRC5**

# Research of computer electromagnetic information leakage based on three layers of protection model

**Yuanhui Yu* and Ying Deng**

**School of Computer Engineering, Jimei University, Xiamen, China*
*Xiamen Institute of Technology, Huaqiao University, Xiamen, China*

---

**ABSTRACT**

*The electromagnetic waves emitted by computer system at work, and may cause information leakage, will be a serious threat to information security. This paper first analyzed the mechanism of the electromagnetic information leakage based on electromagnetics and antenna theory, for the process of resulting in electromagnetic information leakage, "anti-radiation leakage"," preventing electromagnetic interception", "preventing electromagnetic emersion" is put forward. Finally, concrete implementation means of the three layers of protection model of computer electromagnetic information leakage is discussed in detail from two aspects of hardware and software protection.*

**Key words:** electromagnetic information leakage, three layers of protection, anti-radiation leakage, preventing electromagnetic interception, preventing electromagnetic emersion

---

## INTRODUCTION

With the rapid development of information technology, computer has been widely used in security organs, confidential departments and other important institutions and enterprises such as banking and finance, etc. During work, Computer and external equipment will unavoidably produce electromagnetic radiation wave in the form of conduction or radiation, and electromagnetic radiation wave is often "entrained" useful information, which resulting in information disclosure. Relevant research data show that the equipment of receiving and recurrence computer electromagnetic radiation information in the 1000 meters away have been developed abroad,, thus an adverse party can obtain information concealment, timely and continuous in this way [1][2][3]. Especially after the end of the cold war, some economic and military power, for more financial and human resources in an attempt to through the electronic eavesdropping technology for other important military intelligence; But at present, domestic and overseas criminal gangs also attempt by unfair means, using high-tech means stealing state or group important political or commercial secrets [4]. Therefore, prevent computer electromagnetic information leakage has become imperative, and study and master effective protective measures against electromagnetic information leakage is especially important.

## THE RELATED BASIC THEORY OF ELECTROMAGNETIC INFORMATION LEAKAGE

The electromagnetism theory and the experiment shows that space moving charge can form time-varying current of space and then generate time-varying electric field, and time-varying electric field will generate time-varying magnetic field. The two relate to each other, forming an integral of time-varying electromagnetic field. The relationship of charge, electric current and electromagnetic field can be described with Maxwell's equations. Basic Maxwell's equation is transient form of Maxwell's equation, also known as time-domain Maxwell's equations. It is divided into differential form and integral form. The integral form as follows:

$$\int_l E \cdot dl = -\iint_S \frac{\partial B}{\partial t} \cdot dS \tag{1}$$

$$\int_l H \cdot dl = \iint_S (J + \frac{\partial D}{\partial t}) \cdot dS \tag{2}$$

$$\iint_S D \cdot dS = \iiint_V \rho dV \tag{3}$$

$$\iint_S B \cdot dS = 0 \tag{4}$$

Differential form as follows：

$$\nabla \times E = -\frac{\partial B}{\partial t} \tag{5}$$

$$\nabla \times H = J + \frac{\partial D}{\partial t} \tag{6}$$

$$\nabla \cdot D = \rho \tag{7}$$

$$\nabla \cdot B = 0 \tag{8}$$

The above formula：

B——Magnetic induction intensity/magnetic flux density (Wb/ m2);

E——electric field intensity (V/m);

H——magnetic field intensity (A/m);

D——the electric displacement vector/electric flux density(C/m2);

J——ampere density (A/ m2);

ρ ——electric density(C/ m3);

According to the above Maxwell equation, we may know as long as there is charge or current changes over time in circuit, around can produce electric field and magnetic field changes over time, this kind of time-varying electric field and magnetic field can convert each other, and have volatility, and performance in the form of electromagnetic wave at a certain speed in space communication, the process is also an energy transmission process, that is the electromagnetic radiation.

And according to the antenna theory, a computer can generate electromagnetic radiation components (all kinds of transmission lines work inside the machine, signal processing circuit, clock circuit, display, printed circuit boards, switch circuit, etc.) can be regarded as equivalent antenna. In addition, all kinds of lines of the computer (power cord, telephone wires, ground wire, etc.) can also cause a leak about the transmission of electromagnetic energy. These metal conductors also can be treated as equivalent antenna. According to the principle of information theory, Equivalent antenna of the radiation of electromagnetic waves can be regarded as a source of communication system, the free space of transmission of electromagnetic wave can regarded as a channel. If under the ideal condition (i.e., noiseless environment), electromagnetic wave signal of electromagnetic radiation leakage of computers can be seen as electromagnetic information coding. If the listener by intercepting device intercept to the leakage of electromagnetic wave signals is equivalent to obtain the electromagnetic information coding, then it is possible to reproduce the useful information of them.

**THREE LAYERS OF PROTECTION MODEL**

According to the related basic theory of electromagnetic information leakage, the process of computer electromagnetic information leakage mainly reflected in three areas: leak source (information source), radiation of electromagnetic waves (channel), and intercept and capture equipment (information sink). In view of the characteristics of computer electromagnetic information leakage, the author puts forward to three Layers of Protection Model of “anti radiation leakage", "preventing electromagnetic interception", "preventing electromagnetic emersion". First of all, take steps to blocking-up or inhibition of computer electromagnetic leakage, which make it leak out the least amount of electromagnetic radiation; Second, because the computer electromagnetic leakage can't completely be shielding, there will always be part of the electromagnetic wave leaked, so maximize by technical means to increase the difficulty of obtaining computer leakage of electromagnetic wave of the intercepted device, so that it is difficult to receive computer leakage of electromagnetic wave; Finally, if the intercepted device can obtain the computer equipment leakage of electromagnetic waves, also should adopt the necessary method to increase the difficulty of recurrence of information carried by electromagnetic waves as much as possible. Fig.1 shows the schematic for three layers of Protection Model of computer electromagnetic information leakage.

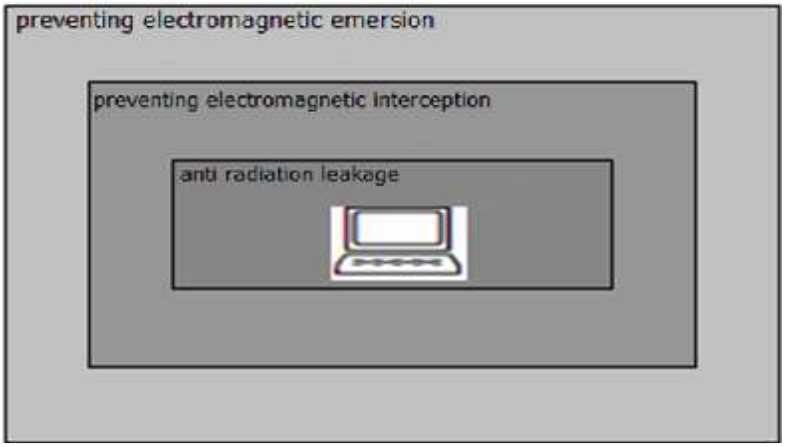


**Fig. 1:Three Layers of Protection Model of computer electromagnetic information leakage**

In Fig.1, the three layers protection strategy model of computer is not isolated between the layers. “Radiation protection leakage”, “anti electromagnetic interception" and "preventing electromagnetic emersion" connected to each other, and complement each other between each layer. For leakage mechanism from different parts of the computer, the realization of the three layers of protection strategy should take comprehensive consideration in factors such as technology, cost, and effect, etc.; weigh the pros and cons in order to take the most effective protection technique.

**PROTECTION TECHNOLOGY**

Usually, hardware and software protection technology can be used to realize three Layers of Protection Model of computer electromagnetic information leakage. At present, computer electromagnetic information leakage protection technology based on the hardware mainly includes: use of low radiation equipment, shielding, filtering, noise interference source, and optical fiber transmission technology. Based on the software mainly includes: TEMPEST font technology, RGB color configuration technology, and image noising technology etc.

*A.Protection Technology Based on the hardware*

1)Use of low radiation equipment

Low radiation equipment namely the TEMPEST devices, is the important measure of the radiation leak proof. The United States is one of the earliest countries which study the computer technology of information leakage prevention (that is, the TEMPEST computer) [5]. The computer of preventing information leakage takes measures to prevent radiation in the design and production, which suppress the electromagnetic leakage of equipment to a minimum. Such as a display is important peripherals of computer electromagnetic information leakage, choose low radiation monitors is particularly important, and the electromagnetic radiation of monochromatic display is lower than the color display, plasma display and liquid crystal display can also further reduce the radiation [6].

2)Shielding technology

Shielding technology by means of restraining transmission of electromagnetic radiation along the space (that is cut off the way of radiation) to achieve the goal of electromagnetic information leakage protection. The essence of

which is to place the computer or computer circuit, components in the shield room or Faraday shielding box, achieve the purpose of preventing electromagnetic radiation. The technology is one of the most widely used and the most reliable of all radiation leak prevention technology. Shielding room or shielding box usually adopt electrostatic shielding, the alternating electric field shielding, alternating magnetic field shielding, alternating electromagnetic shielding and other methods to achieve the goal of prevent computer radiation. Such as the high performance shielding room developed by the United States, the shielding effect of electric field can reach 140 db; the microwave field can reach 120 db, the magnetic field of up to 100 db [7].

Due to electromagnetic places physical media with different conductive and magnetic properties, so in the medium there is a certain relationship among the electric displacement vector D, the magnetic induction intensity B, current density J and electric field intensity E and magnetic field intensity H. This relationship can be described using structural equation:

$$D = \varepsilon E \tag{9}$$

$$B = \mu H \tag{10}$$

$$J = \sigma E \tag{11}$$

In the above formula, ε is the dielectric constant, μ is the magnetic permeability of the medium, and σ is the electrical conductivity of the medium. They are the three important electromagnetic parameters of electromagnetic wave propagation medium.

The vacuum dielectric constant is:

$$\varepsilon_0 = \frac{1}{36\pi} \times 10^{-9} \approx 8.854 \times 10^{-12} (F/m) \tag{12}$$

The magnetic permeability is:

$$\mu_0 = 4\pi \times 10^{-9} (H/m) \tag{13}$$

The dielectric constant value and magnetic permeability value in dry air is approximately equal to that in the vacuum, the magnetic permeability of common medium(with the exception of magnetic material) is very close to the μ0.

The electrical conductivity of ideal conductor $\sigma \to \infty$, that the charge can move freely in the conductor. Medium with great conductivity can be approximated as an ideal conductor, such as gold, silver, copper and other metals. Metal materials with great conductivity often used as electromagnetic shielding materials.

Domestic scholars have put forward the design requirements of high-performance electromagnetic shielding square, square design should pay attention to several parts are pointed out：（1）Choose better shielding performance of the aluminum plate as a square wall inside and outside of the envelope. In order to further improve the shielding effectiveness, wall plate juncture place can use high, low-frequency performance has good tin-coated copper tape；（2）when design cabin door can add the epoxy which resistivity is less than 0.0 l Ω · cm or silicone conductive adhesive ; and paste conductive shielding tape in the interface；（3）when design the vents can increase its thickness (the depth of the hole) appropriately, reduce pore size, reduce the area of the individual ventilation window, at the same time also ensure air vents and bulkhead seamless electrical connection；(4)Air conditioning hole wall tube can use copper pipe, and when the copper pipe through the square tank plate adopts special fingering reed to make it close to the bulkhead；（5）Turn interface can use conductive socket and mount conductive liner such as conductive rubber etc. between the socket and switch board [7].

In addition, the shielding window and shielding cable is also frequently used. Shielding window refers to installed electromagnetic shielding glass on the computer monitor; it is made of adding the special treatment of metal mesh between two layers of glass or translucent resin. Electromagnetic shielding glass can guide most of the information into the ground through ground wire, only a little radiation hook signal pass, even if the listener has a way of intercepting these signals, they cannot revert to as clear and complete information, so as to achieve the purpose of

confidentiality. Shielding cable is mainly refers to the external equipped with computer cable shielding layer, the shield can be woven by single wire, double wire or wire mesh and metal foil, , it not only can enhance the coverage of signal in the cable, and also can provide good conduction for radiation shielding of cables.

3)Filtering technology

Filtering technology is the important content in the TEMPEST computer technology. Filtering technology plays a part of filter is mainly by restraining some frequency range of the electromagnetic wave of computer radiation in shield can't went out of the radiation shielding body, so as to realize the protection of computer electromagnetic information leakage. Filtering technology is commonly realized by filter; the basic functions of filter are selection signal and suppress interference [8]. Filter regard signal as analog signals which is composed of different frequency superposition sine wave, when according to the frequency filtering, often by choosing different frequency components to achieve the signal filtering, generally includes: the high-pass filter, low-pass filter, band-pass filter and band stop filter. Filter can be divided into signal filter and the power supply filter according to use. Signal filter including plate filter and connector filter two kinds. Plate filter is installed on the signal output end of the PCB (printed circuit board). Connector filter is used on the interface cable between equipments, have functions of filtering and shielding, in the same connector filter can mixed different filter frequency according to user requirements. Power filter is a kind of passive bidirectional network, it is able to filtering frequency point of specific frequencies in the power supply or frequency beyond the frequency point effectively, and its one end connects to the power, the other end connected to the load. Power filter is mainly used to filter out communication component, dc, to maintain the output voltage stability; the ac power is only allowed through a particular frequency. At present, filter produced by the domestic manufacturers have been able to substantially filter out the higher harmonic radiation by the various lines on the PCB board in the computer, effectively preventing electromagnetic radiation leakage of computers.

**Figure 2 The GRQ – 03C computer-related jammer**

4)Use of noise interference sources

With noise interference sources are mainly mixed electromagnetic waves emissions from Jammers together with the computer, to cover up content, characteristics, etc. in the information carried by the computer radiation electromagnetic waves, to prevent electromagnetic interception and the purpose of preventing electromagnetic emersion. Jammers usually include white noise jammer and related jammer. White noise jammer is an early jammer product, using a noise emitters, in a relatively wide frequency band to create very strong noise, to cover signal of electromagnetic radiation leakage of computers; Related jammer firstly collected computer electromagnetic radiation signals, and after digital processing, automatically launch an interference signal which intensity is not very big, but related to computer electromagnetic radiation; Two jammers can improve the difficulty of intercepting computer electromagnetic radiation signals to listeners[9]. For related jammers, even when the listener has a way to intercept the electromagnetic signals, but also unable to reappear the original information for digital signal processing, further improve the effect of the electromagnetic information leakage of protection. Interference sources are usually installed in the computer nearby, so that the interference sources and electromagnetic information generated by computer radiation radiated outward together, makes the computer radiation of electromagnetic wave is not easy to be intercepted and repetition. At present, our country has developed GRQ – 03C computer-related jammer (Fig. 2 shows the GRQ-03C jammer), the product through the Chinese people's liberation army information security certification center B grade certification. It uses USB interface power supply without external power supply, do not need to install software, compatible with desktop and notebook computers, the launch of the disturbance signals can automatically tracking computer display mode change, automatically to adapt to different work mode of display terminal, achieved at the same time domain, and frequency domain related, and has strong ability of Anti-receiving and reducing of the Video.

5)Optical fiber transmission technology

Optical fiber transmission is the main non conductive medium transmission technology. The light wave in optical fiber communication is mainly laser, laser has significant advantages of high monochromaticity, high directivity and high coherence etc.When transmit waves with optical fiber, optical signal can be completely limits in optical fiber, optical fiber composition is glass fiber, glass fiber can not radio electromagnetic wave outward, and the intercepted possibility is almost zero. Around by the optical fiber is opaque plastic skin, even if appear the leaks of electromagnetic wave, the leaked radiation can be absorbed by the plastic skin. Therefore, optical fiber transmission technology has the very high levels of electromagnetic information leakage prevention [10]. Reported by the discovery channel of theUnited States on November 1, 2012, Wright, the air force research laboratory of Ohio - air force Patterson base collaborate with the space photonics company of the Arkansas Fayetteville, developed a called "" free space optical communications" system of infrared laser, infrared laser system is shown in the Fig.3 below. The amount of information carried by the laser communications exceeds that of Wi-Fi and other wireless signals. Due to the infrared laser beam is very narrow, the eavesdropper cannot eavesdrop and intercept, unless they are in transmission lines. The eavesdropper once pass into the laser beam transmission lines, laser beam will interrupt and immediately give an alarm, so the system has high security.

**Figure 3 Infrared laser system schematic diagram**

B. protection technique Based on the software

1)Tmpest font technology

When Computer monitors working, there are accompanied by large amounts of digital/analog conversion, high frequency spectrum produced by this process will contain lots of wave crest, the wave crest can be apart from the noise signal easily. Eavesdroppers often reproduce the computer display images by using of high frequency spectrum as clues. So, remove the high-frequency components is in favor of improving the difficulty of electromagnetic repetition, can effectively prevent the radiation electromagnetic information leakage of computer monitors. British Kuhn and Anderson, invented a kind of electromagnetic information protection method known as the Tempest font, the using of Tempest font is equal to the low pass filter, image or video signal of computer was filtered by software filter, remove the top 30% parts of the signal level spectrum, that is to reduce the font of the high frequency energy, this kind of electromagnetic wave signal which is processed by the Tempest font even if is intercepted, the content of leakage information can't be reproduced. And TEMPEST font technology is more flexible than hardware protection technology and low cost, thus has more application value [11].

2)RGB color configuration technology

The implementation principle of touch screen is roughly the same that is adding transparent touch panel on the normal LCD panel. The classification of touch screen at present basically has resistance-type, capacitance, and infrared-type, surface acoustic wave four types. In real life we contact most is resistance-type touch screen. Typical resistance-type touch screen generally includes two layers of transparent resistance conductor layer, isolation layer between the two layers, and electrode three parts. When the touch screen works and is equal to the resistance network. When a layer of electrodes is connected to a positive voltage, the voltage gradient is formed on the network. When finger pressing a point of the touch screen, make the above and below layer of the screen contact at that point, then at another without voltage layer of electrode can be measured the voltage of the contact point, so as to get the coordinates of contact point, and then through the interface (such as RS - 232 serial port) to the CPU, so as to determine the input information, finally displayed the input information on the LCD panel. In the process of external force squeezing touch screen, because the pressure of each pixel in The compressed place change, lead to the RGB components voltage difference of corresponding pixels change when the light reaches the LCD, the electromagnetic radiation signal can appear in the process, , the radiation is essentially comes from the emission of electromagnetic signals when RGB signal analog voltage change in raster scan process of liquid crystal screen. If the eavesdropper managed to intercept these electromagnetic radiation signals, can reproduce the information displayed on the touch screen by the technology of image analysis and reconstruction.

RGB color configuration technology is mainly through optimizing configuration buttons color of touch screen, makes the relative analog voltage difference of touch screen remain constant before and after the button is pressed, namely the RGB signal analog voltage difference between adjacent pixels remain constant. So even if eavesdroppers intercepted the electromagnetic radiation signals let out by key stroking, and also is unable to determine the state of the button to hide the user input information, realizes the electromagnetic radiation information leakage caused by electromagnetic noise of touch screen. At present, the RGB color configuration technology has been widely applied in commercial information touch screen devices, such as ATM, entrance guard control terminal, credit card machines, etc.

3)Image noising technology

Image noising technology realizes the aim of preventing electromagnetic information leakage by adding noise in the image on the basis of does not disturb the visual effect. Usually the image noising technology include two kinds: one kind is to add salt and pepper noise, the other is to add Gaussian noise.

(1) Add salt and pepper noise

Salt and pepper noise also known as impulse noise, it is black and white bright dark spot noise generated by the image sensor, transmission channel, decoding processing , is caused by the pulse signal strength, it randomly changing pixel values. Salt and pepper noise includes two types of noise: one kind of is salt noise, belongs to the high intensity noise, showing a white noise points; the other is a pepper noise, belongs to the low intensity noise, showing a black point. The two kinds of noise appears at the same time when adding salt and pepper noise to computer image, and the effect of image is presented is all black and white points. Fig.4 shows the contrast effect of before and after Add salt and pepper noise images.

**Figure 4 the contrast effect of before and after Add salt and pepper noise images**

(2) Add the Gaussian noise

Gaussian noise is a random noise, refers to the type of noise which probability density function is obey Gaussian distribution (i.e., normal distribution). Add Gaussian noise to the image usually make the image appear a large number of tiny spots, make the image become blurred. The contrast effect of before and after Add Gaussian noise images is shown in the Fig.5 below.

**Figure 5 the contrast effect of before and after Add Gaussian noise images**

## CONCLUSION

The procedure of computer information processing involved in a lot of classified information, some even is related to social and economic stability and national security, and we should pay high attention to information leakage. For the protection of computer system electromagnetic information, we should take into full account both “preventing radiation leak ", “preventing electromagnetic interception", and "preventing electromagnetic emersion" three aspects. The protection of computer electromagnetic information leakage is complex system engineering, must adopts the corresponding hardware and software protection measures to harness and protection according to the characteristics of the computer system, thus can achieve the best protection effect.

**Acknowledgments**
The authors wish to thank the provincial colleges and universities special Foundation of Fujian Science and Technology Department of China for contract JK2012026, under which the present work was possible.

## REFERENCES

[1] Zhao Lihua, Liu Rongping. *Net info Security*, no.3, pp.39–40, **2002**.
[2] Hong Zhao, Guofeng Li, Ninghui Wang, Shunli Zheng, Lijun Yu. *Journal of Computers*, no.9, pp.2240–2247, **2012**.
[3] Tao Wen, Tao Wen, Tuo Chen. *Special Issue: Advances in Computational Intelligence Journal of Computers*, no.2, pp.308–312, **2013**.
[4] Fan Wenqi. *Electronic Product Reliability and Environmental Testing*, no.12, pp.111–112, **2005**.
[5] Zhang Hongxin,LvYinghua. *Safety & EMC*, no.6, pp.39–43, **2004**.
[6] Li Wubin, Zhang Zhihua, Dai Dongyuan. *Electro-Mechanical Engineering*, v 28, n 6, p 8-12, **2012**.
[7] Zhu Jing. *Modern electronic engineering*, no.1, pp.78–83, **2004**.
[8] Liu Xinggang. *Chinese Journal of PowerSource*, v 33, n 7, p 608-610, **2009**.
[9] Xia Zhijun, Zhang Xinhua, hang Yu-ce, GuoHuidong. *Ship Science and Technology*, v 30, n 4, p 161-164, **2008**.
[10] Wang Jingguo, Zhu Shoaling. *Optical Communication Technology*, no.10, pp.60–62, **2009**.
[11] Yuan Qigang, Guo Wei. *Equipment Environmental Engineering*, v 3, n 5, p 7-11, **2006**.