文章编号:1674-7070(2013)05-0402-07

计算机信息泄漏防护设备的设计

史小红[1]　姜禹[1]　孔繁珵[1]　金文[2]

摘要

针对目前计算机信息泄漏防护设备存在的问题,设计并实现了一种白化型信息隐藏防护设备,通过增加防护信号去白化泄漏信号,达到干扰和隐藏泄漏信息的目的.频域分析和实验测试结果表明,该设备有效隐藏了计算机的泄漏信息,并且相对于现有的泄漏信息防护设备,泄漏信息和原始信息的相关性显著下降,为计算机信息的保护提供了一种更可行的方式.

关键词

信息泄漏;信息隐藏;白化

中图分类号 TN918.91

文献标志码 A

收稿日期 2013-08-03

资助项目 国家科技支撑计划(2012BAH38B05);国家高技术研究发展计划(2013AA014001)

作者简介

史小红,女,硕士,工程师,主要研究方向为通信系统. sxh@seu.edu.cn

1 东南大学 信息科学与工程学院,南京,210096

2 中国电子科技集团公司第二十八研究所,南京,210007

0 引言

随着计算机信息技术应用的深入和广泛,其在军事、政务、商业领域的作用越来越重要.计算机设备采用了大量的电子器件,在处理信息的过程中,不可避免地泄漏出电磁信号.信息设备中的数据传输都需要依靠电信号,电信号的传递必然会产生电磁波的泄漏,这些电磁波就成为信息泄漏的载体,而敏感信息的泄漏会给国家和社会带来严重的危害[1-3].目前,我国许多涉密单位以及相关单位的涉密部门并没有采取有效的防护措施去处理电磁信息泄漏问题,绝大部分日常办公的电脑都不能达到低辐射标准,这存在巨大的安全隐患.

早在1985年的计算机安全会议上,Eck[4]就公开展示了他的研究成果:将黑白电视机经过改装作为接收设备,成功接收了计算机屏幕上正在显示的图像.随着设备的工作频率越来越高,电磁辐射中频率较高的信号,都可能产生频率更高的谐波信号,并向空中发射,就更易造成电磁辐射泄漏.

现有的电磁泄漏防护措施[5]可分为屏蔽技术和干扰技术两类.屏蔽技术[6]主要利用金属屏蔽层的反射、吸收及趋肤效应实现防止电磁干扰和辐射的目的.干扰技术属于人为干扰方式,它利用人工装置产生电磁能量影响和掩盖泄漏信息,使得泄漏信息难于侦测.白噪声干扰和相关干扰是目前主要的两种干扰技术[7].白噪声干扰的原理是使用人工装置产生强干扰作用的白噪声信号,降低空间泄漏信息的总体信噪比,以提高有效信息被截获恢复的难度.这种方法在靠电磁信号泄漏源较近的地方可起到一定作用,但发射的噪声功率需要足够强,而过强的信号可能会干扰其他无线设备的工作;此外,通过滤波和分离技术可以简单地分离出泄漏信息,所以白噪声干扰技术存在明显的缺点.相关干扰是在白噪声干扰的基础上发展出来的一种有效的干扰技术.相关干扰的原理是使用人工装置产生和泄漏信息序列具有相关性的干扰信号,利用这种相关噪声来淹没辐射信息并使其信号特征发生改变,从而使得泄漏的有效信息无法解调还原[8].因为相关干扰的原理和白噪声干扰不同,发射功率相对较弱且电磁污染小.

电磁泄漏不仅对周围的电子设备造成电磁干扰,导致信息泄密,而且会危害人体健康.因此,信号防护设备需要以低辐射高隐蔽性为目的.本文设计了一种新型的计算机信息泄漏防护设备,通过白化信

号的方式增加信号在空间中的隐蔽效果,通过比较分析发现,在相同的信号功率下,相对于现有的干扰技术其信息防护效果更好.

1 设计方案

1.1 总体设计

目前计算机系统包括4个部分的电磁泄漏辐射源:显示器辐射、输出设备辐射、主机辐射以及通信线路辐射.最主要的电磁泄漏辐射源是各类显示器,其次是主机[9].由于现在计算机处理的都是数字信息,而数字信息的信号频谱范围广,辐射泄漏的源头就是数字信息的脉冲信号串,这也是本文设备的防护对象.

综合考虑体积、接口、设计复杂度等因素,白化型干扰信息防护设备主要由主控制器、人机接口模块、功率控制电路、本振电路及混频器组成,图1是系统硬件结构.

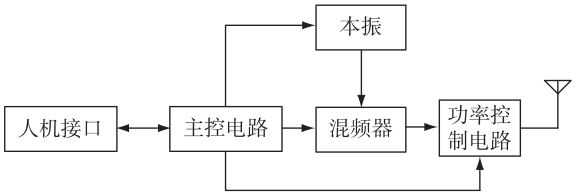

图1 系统硬件结构

Fig. 1 System hardware structure

1.2 主控电路设计

本设计中的主控电路采用了Ti公司的低功耗MSP430F149单片机芯片,主要部分电路原理如图2所示.该电路主要实现3个功能:一是产生与被干扰的泄漏信号频域特性一致的数字脉冲序列;二是控制本振电路产生的本振频率值,使干扰信号符合泄漏信号的频域分布特性,以达到白化频谱的效果;三是通过功率控制电路调整辐射信号的强度适应实际的应用需求.防护设备根据需要保护的设备和频率

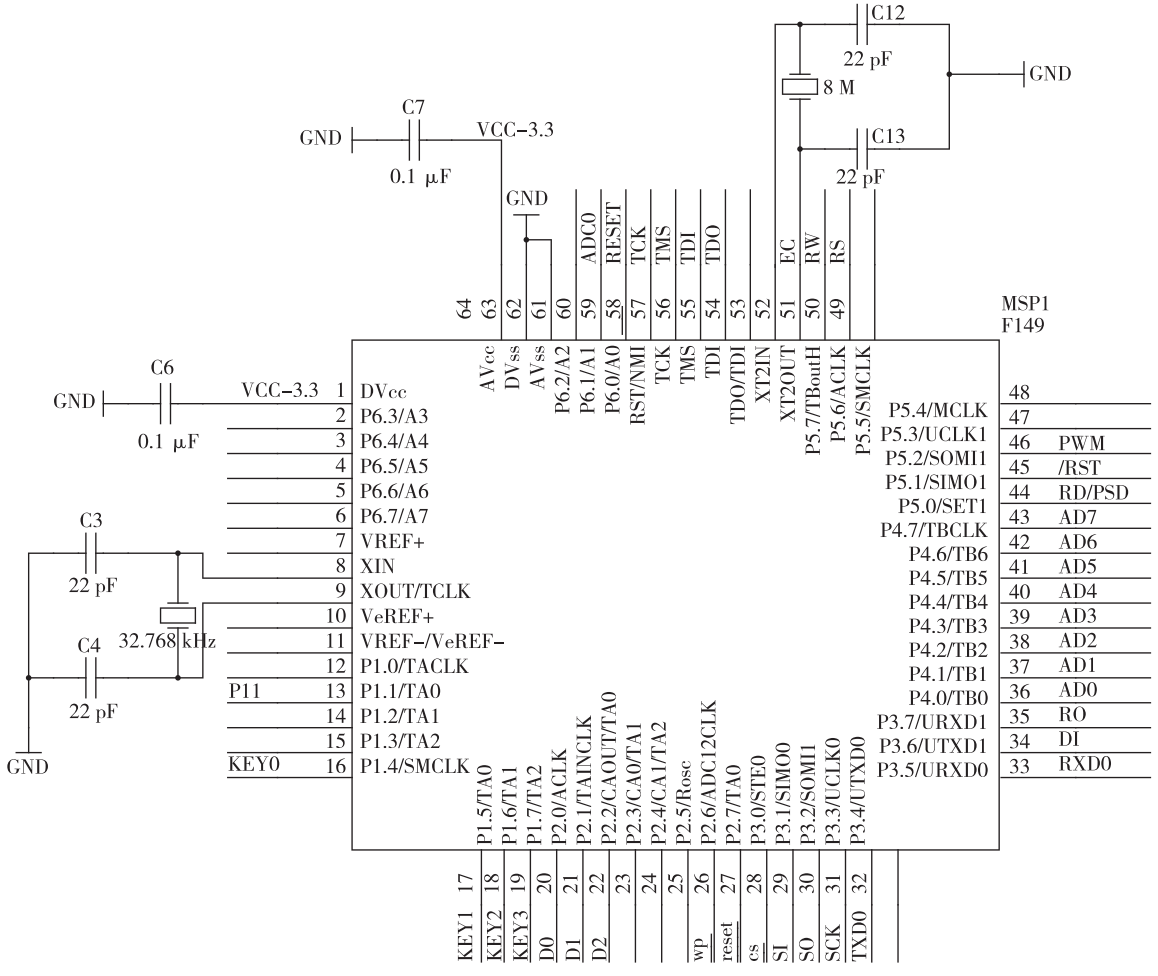

图2 主控电路主要部分电路原理

Fig. 2 Main part of the control circuit schematic

特性可以预先配置一些默认设置,也可以通过人机接口电路,包括键盘和小显示屏进行人工设置,人机接口电路直接和主控电路进行连接.

1.3 本地振荡电路设计

本地振荡电路采用了 Adi 公司的 ADF4351 芯片,其主要部分电路原理如图 3 所示. ADF4351 具有一个集成电压控制振荡器(VCO),其输出频率范围经过分频可以从 35 ~4 400 MHz,完全满足防护设备的应用频率范围. 所有片内寄存器均通过简单的三线式接口进行控制,不使用时可以关断频率输出,作为控制干扰信号的输出开关.

1.4 功率放大电路设计

功率放大电路由一个固定增益的放大器和一个可调增益的放大器组成,在实现混频信号放大的同时,也可根据电磁环境进行增益控制. 电路的工作增益越大,那么干扰效果就越好. 当需要减小对其他无线设备干扰时,可通过减小可调增益放大器的工作增益来实现. 本设计的主要部分电路原理如图 4 所示.

第一级功率放大器采用了 Adi 公司的 ADL5331 芯片. ADL5331 是一款高性能、电压控制可变增益放大器,适合频率最高为 1.2 GHz 的应用. 通过单片机对 ADL5331 的控制实现自适应增益调整,信号电流施加于一个专有电压控制衰减器,图 4 中的 GainCtrl 端口在线性接口的控制下精确定义整体增益. GAIN 引脚接受 0 ~1.4 V 的电压,增益控制范围从 -15 ~ +15 dB.

第二级功率放大器采用了 ADL5523 芯片实现固定增益放大. ADL5523 是一款高性能的低噪声放大器,可以为单一下变频转换 IF 采样接收机架构和直接下变频转换接收机提供高增益和低噪声系数. 该器件具有高集成度,内置有源偏置电路和隔直电容,不仅非常易于使用,而且不会影响设计灵活性. ADL5523 只需极少外部元件,便可轻松进行调整. 该器件可在 3 ~5 V 电压下工作,并可通过外部偏置电阻调整电流吸取,从而满足要求极低功耗的应用需求. 经过两级放大器放大后的干扰叠加信号最后通过宽带天线辐射到空中.

2 设备信息隐藏效果比较

作为信息泄露最敏感的设备,本文测试的原始计算机信号采用 LCD 显示器信号. 目前常用的计算机基本不使用 CRT 显示器而都换上了轻薄的 LCD 显示器,由于显示原理的不同,LCD 显示器电磁泄漏的情况要比 CRT 显示器好得多,但其驱动电路部分的高电压模块仍然会产生电磁泄漏. 显示器工作时产生的二进制脉冲信号串的频率[10],由其分辨率、场频和显示模式决定,关系如下:

$$f = m \times n \times r \times 1.388, \tag{1}$$

其中分辨率为 $m \times n$,f 为脉冲信号串频率,场频为 r,1.388 为修正行,即场消隐影响系数. 由于目前使用的 LCD 显示器多为宽屏显示器,因此选取显示刷新频率 60 Hz,分辨率为 1 440 像素 ×900 像素来分析. 由式

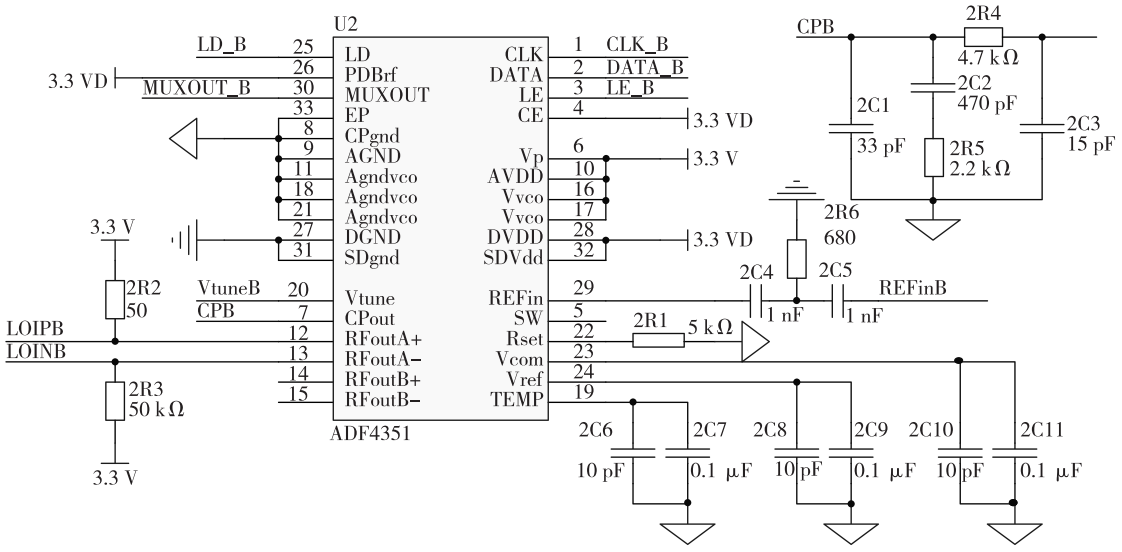

图 3 本振电路主要部分电路原理

Fig. 3 Main part of the oscillation circuit schematic

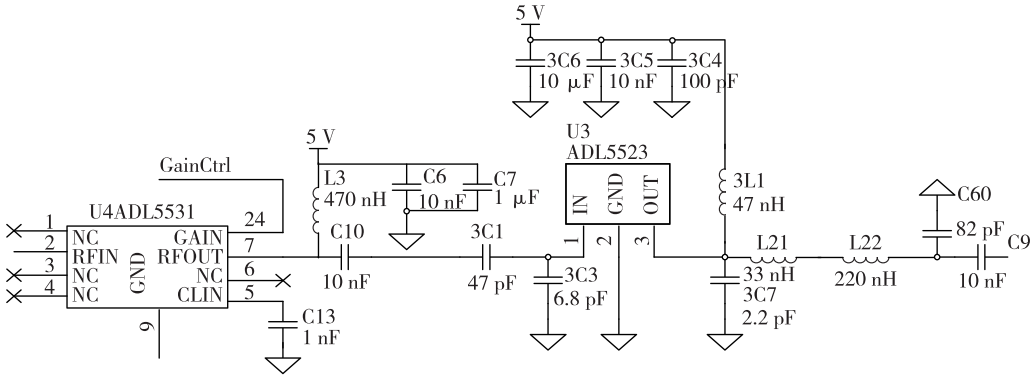

图 4　功率控制电路主要部分电路原理

Fig. 4　Main part of the power control circuit schematic

(1)得,信号串频率 f 为 108 MHz. 为了有效分析此泄漏信号的特性,首先观察其频域分布,对于一个 108 MHz 的二进制脉冲信号串的幅频曲线如图 5 所示.

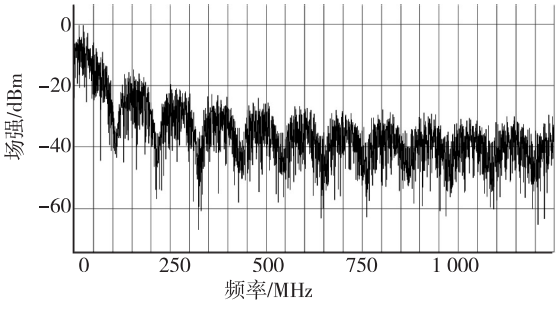

图 5　显示信号的频谱分布

Fig. 5　Spectral distribution diagram of the display signal

图 5 中的幅频曲线反映了原始显示信号的频域分布,曲线中的每个波瓣都是原始信息的高次谐波,信息窃听者在窃收时,只需要经过带通滤波器获得信号频谱的一个波瓣,对接收信号进行检波、限幅、整形、放大等操作,就可以还原出泄漏的信息[11]. 相关干扰型防护设备进行信息保护时产生的空间信号叠加频谱如图 6 所示.

如图 6 所示,由于相关干扰信号要达到相关干扰的目的,其信号本身和原始显示信号必须具有很强的相关性,那么其频率和原始信号必须相同,因此通过比较图 5 和 6 的曲线分布可以发现,叠加信号的频谱和原始信号的频谱在形状上是基本一致的. 在这种情况下,窃听者通过频谱分析仪或信号场强检测设备就可以很容易侦测到无线环境中存在泄漏信息,而相关干扰信号并不能有效覆盖泄漏信息,窃听者可以通过选取不同地理位置找到干扰信号的覆盖薄弱点,这些都是信息泄漏潜在的安全隐患. 从以

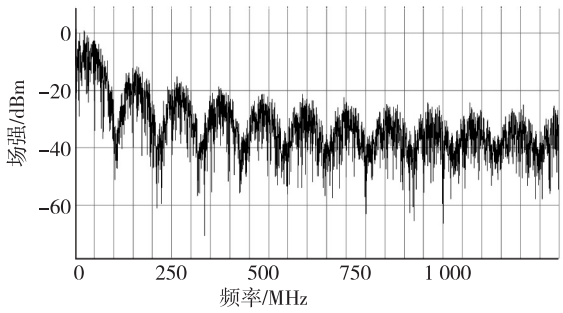

图 6　叠加信号的频谱分布

Fig. 6　Spectral distribution of the superimposed signal

上分析不难发现,除了对计算机的泄漏信息进行干扰防护以外,对其信息的隐藏更加重要. 如果通过信息防护设备达到信息隐藏的作用,那么对窃听者来说找到泄漏信息存在位置的难度远大于从泄漏信息中提取有效信息. 针对以上问题,本文设计了高隐蔽性的白化型干扰信息防护设备.

对白化型干扰信息防护设备进行分析,空中叠加信号的频谱如图 7 所示. 当频率超过 160 MHz,空中信号的频谱形状逐渐平坦,近似白噪声的谱形,相对图 6 的结果,白化干扰法更好地隐藏了泄漏信号,得到了有效的空中隐藏. 单从信息隐藏的角度来看,白化型干扰信息防护设备的防护效果要好于相关型干扰信息防护设备.

3　设备信息干扰效果比较

下面通过分析泄漏信息的时域特性来观察和比较白化干扰法以及相关干扰法的实际使用效果. 仍然以前文采用的 LCD 显示器的显示信号为例,信号串频率为 108 MHz.

如果没有任何防护措施,按照文献[12]的结论,

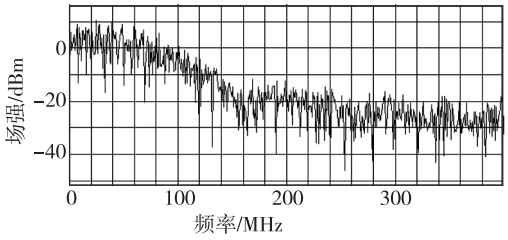

图 7　白化叠加信号的频谱分布

Fig. 7　Spectral distribution of the whitening superimposed signal

脉冲信号串经过接收设备恢复后和原信号波形几乎一致,并能从恢复波形中得到部分原始信息,假设其还原出的信号串是 s_{bpf};当脉冲信号串在相关干扰设备的干扰作用下,并使用同样的恢复方法还原得到信号串为 s_{cor};而使用白化型防护设备进行干扰防护并还原得到信号串为 s_{whiten}.

对上述几个信号串进行互相关运算分析相关设备的泄漏信息干扰效果. s_{bpf}和 s_{cor}互相关运算结果如图 8 所示,s_{bpf}和 s_{whiten}互相关运算结果如图 9 所示. 从图 8 可以看出,s_{bpf}和 s_{cor}互相关的最大峰值在 128,其相关峰值要明显大于周围值,表明经过相关干扰后的泄漏信息和不经处理的泄漏信息仍有一定的相关性. 从图 9 可以看出,s_{bpf}和 s_{whiten}互相关的最大峰值在 21,其相关峰值和周围值已经比较接近,表明经过本文设计的白化干扰后的泄漏信息和不经处理的泄漏信息的相关性已经很弱. 从图 8 和 9 的对比结果可知,白化干扰设备的泄漏信息干扰效果要优于相关干扰设备.

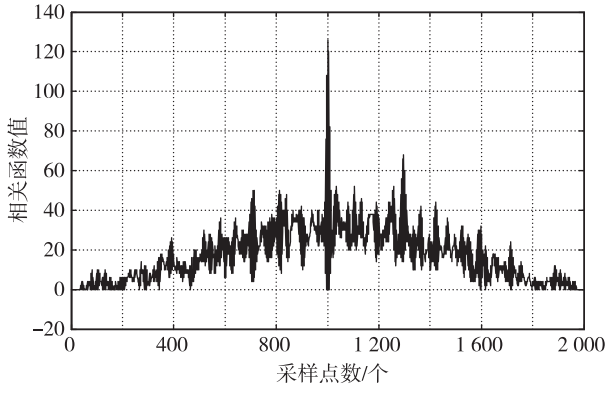

图 8　s_{bpf}和 s_{cor}互相关运算结果

Fig. 8　Mutual correlation result between s_{bpf} and s_{cor}

为了进一步分析,对信号串 s_{bpf}、s_{cor}和 s_{whiten}分别经过接收判决后的二进制数字序列进行相关运算. 这 3 个序列和原始序列的互相关运算的结果及原始

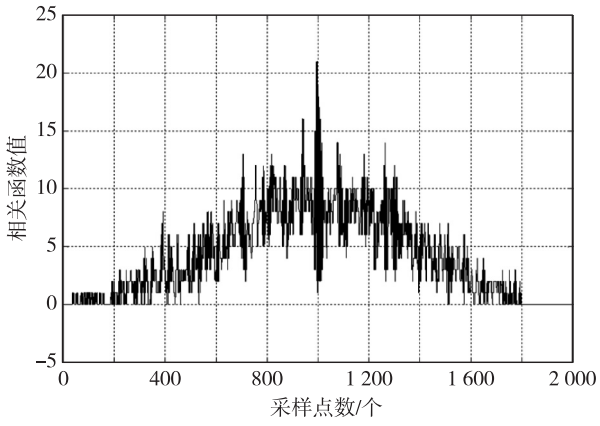

图 9　s_{bpf}和 s_{whiten}互相关运算结果

Fig. 9　Mutual correlation result between s_{bpf} and s_{whiten}

序列自相关的结果如图 10 所示. 图 10a 是原始序列自相关运算的结果,由于本例中选用了自相关性很强的 PN 序列作为原始信息序列,其自相关的峰值在 1 000 左右. 图 10b 是原始序列和 s_{bpf}间的互相关运算的结果,其自相关的峰值在 70 左右,和原序列的相关性已大大下降. 图 10c 是原始序列和 s_{cor}间的互相关运算的结果,其自相关的峰值在 60 左右,图 10 d 是原始序列和 s_{whiten}间的互相关运算的结果,其自相关的峰值在 15 左右.

由图 10 的分析表明,对计算机泄漏信息白化干扰的效果最好,其次是相关干扰. 从恢复的泄漏信息和原始信息的相关性看,白化干扰设备要优于相关干扰设备,而信息的相关性越大,其可能被恢复的威胁也越大. 因此,白化型干扰信息防护设备在相同的泄漏信号功率和防护信号功率下相对相关型干扰信息防护设备抗干扰效果更好.

4　结束语

本文在分析现有的白噪声以及相关噪声泄漏信息防护方法的基础上,提出了一种白化泄漏信号的防护方法,并设计实现了白化型信息防护设备,最后通过与现有防护技术的比较,测试分析了白化型信息防护设备的特性.

区别于现有防护技术的实现方法,白化型信息防护设备不仅对泄漏信息实现了干扰防护,同时使得泄漏信息的频谱淹没在防护信号中,使得空中的叠加频谱趋于白噪声的谱形,有效隐藏了泄漏信息并减少了信息泄漏风险. 理论分析和实验测试结果表明,白化型信息防护设备比现有的泄漏信息防护设备防护效果更好.

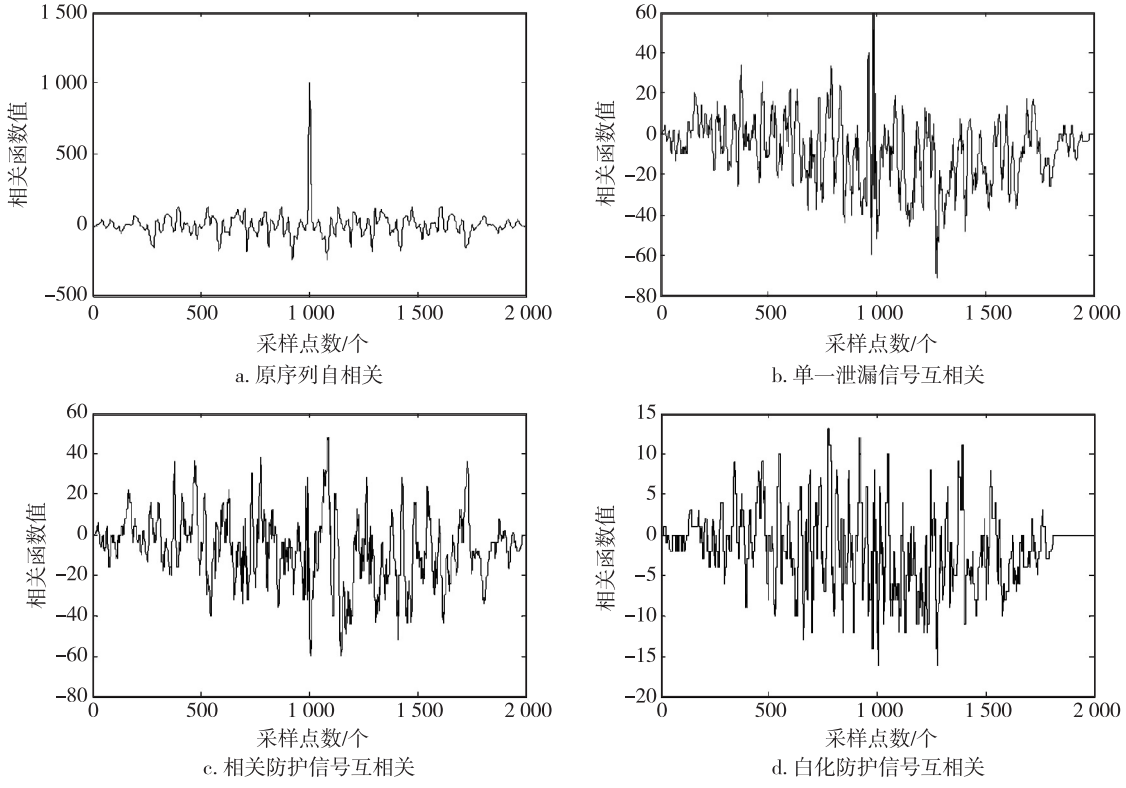

图 10　各接收判决序列和原始序列的相关运算结果

Fig. 10　Correlation results between the receiving sequences and the original sequences

参考文献

References

[1] 刘杰,刘济林. TEMPEST Attack 对信息安全的威胁与对策[J]. 浙江大学学报:理工版,2004,31(5):528-534
LIU Jie, LIU Jilin. Threat and its countermeasures of TEMPEST Attack on computer information security[J]. Journal of Zhejiang University:Sciences Edition,2004,31(5):528-534

[2] 胡延军,孙德刚,杜虹. 我国 TEMPEST 发展亟待解决的问题与对策[J]. 信息安全与通信保密,2003,25(6):18-21
HU Yanjun,SUN Degang,DU Hong. Problems and countermeasures demanding prompt solution in China's development of TEMPEST[J]. China Information Security,2003,25(6):18-21

[3] 李敏,孙德刚,杜虹. TEMPEST:威胁与检测技术[J]. 信息安全与通信保密,2003,25(1):31-34
LI Min, SUN Degang, DU Hong. TEMPEST: Threat and detect technology[J]. China Information Security,2003,25(1):31-34

[4] Eck W V. Electromagnetic radiation from video display units:an eavesdropping risk[J]. Computers & Security,1985,4(4):269-286

[5] Herndon R L. Electromagnetic Pulse (EMP) and TEMPEST protection for facilities[M]. Washington DC: US Army Corps of Engineers,1990:91-95

[6] 陈万金,陈燕俐,蔡捷. 辐射及其安全防护技术[M]. 北京:化学工业出版社,2006:29-46
CHEN Wanjin,CHEN Yanli,CAI Jie. Radiation and security protection technology[M]. Beijing: Chemical Industry Press,2006:29-46

[7] 周旭. 电子设备防干扰原理与技术[M]. 北京:国防工业出版社,2005:57-71
ZHOU Xu. Electronic devices interference principle and technology[M]. Beijing: National Defence Industry Press,2005:57-71

[8] 张月芳,郝万军,张忠伦. 电磁辐射污染及其防护技术[M]. 北京:冶金工业出版社,2010:65-70
ZHANG Yuefang, HAO Wanjun, ZHANG Zhonglun. Electromagnetic radiation pollution and protection technology[M]. Beijing: Metallurgical Industry Press, 2010: 65-70

[9] 杨顺辽,卢凌,聂明新,等. 基于微波暗室的计算机电磁泄漏测试[J]. 武汉理工大学学报:交通科学与工程版,2004,28(5):725-728
YANG Shunliao,LU Ling,NIE Mingxin,et al. Measuring electromagnetic leakages from computer based on EMC microwave anechoic chamber[J]. Journal of Wuhan University of Technology: Transportation Science & Engineering,2004,28(5):725-728

[10] VESA and industry standards and guidelines for computer display monitor timing (DMT) version 1.0, revision 10 [S]. Milpitas: Video Electronics Standards Association,

2004
[11] 张洪欣,吕英华,邱玉春,等. 计算机视频电磁信息泄漏效应研究[J]. 通信学报,2004,25(4):41-48
ZHANG Hongxin, LÜ Yinghua, QIU Yuchun, et al. The study on video electromagnetic information leakage of computer[J]. Journal of China Institute of Communications, 2004, 25(4): 41-48
[12] 邱扬,任华胜,田锦,等. 计算机视频系统的信息电磁泄漏分析[J]. 西安电子科技大学学报,2002,29(5):693-697
QIU Yang, REN Huasheng, TIAN Jing, et al. Information electronic magnetic emanation analysis of the video display unit for computers[J]. Jounal of Xidian University, 2002, 29(5): 693-697

Design of computer information leakage protection equipment

SHI Xiaohong[1] JIANG Yu[1] KONG Fancheng[1] JIN Wen[2]
1 Information Science and Engineering School, Southeast University, Nanjing 210096
2 The 28th Research Institute of China Electronics Technology Group Corporation, Nanjing 210007

Abstract Aiming at the problems of the computer information leakage protection equipment at present, an information hiding and protection equipment was designed and implemented based on the whitening technology. The protection signal was used to whiten the leakage in order to hide and interfere with the leaked information. Frequency domain analysis and experimental results show that the device hides the leaked information effectively. Compared to the existing leakage protection equipment, the correlation of the leakage and the original information decreases significantly. This device provides a more practical way to protect the computer information.

Key words information leakage; information hiding; whitening