视频显示器图像的电磁泄漏重建 [1]

吴昌英 张浩斌 董士伟 许家栋

(西北工业大学电子工程系 西安 710072)

摘 要 计算机数据的电磁辐射泄漏近来一直受到人们的关注. 该文提出了一套利用其辐射信号获取显示信息并重建之的系统. 该系统通过天线接收电磁辐射, 经放大, A/D 转换后, 输入计算机, 然后对该数据进行处理, 重建图像. 试验表明, 该系统完全可行, 并达到满意的效果.

关键词 视频显示器, 电磁泄漏, 重建, 辐射, 小波变换

中图号 TN061

1 引 言

电子设备在工作时不可避免地会向外界辐射电磁波, 由此可能干扰周围电子设备的正常工作. 科技工作者一直在研究如何尽可能地减小这种干扰, 即系统的电磁兼容性问题. 然而随着对计算机的电磁兼容性研究的深入, 发现其所辐射的电磁波中携带着正在处理的信息, 因此就有人致力于利用这种电磁波重建计算机中的信息 [1,2] .

50 年代, 美国首先注意到计算机系统杂散电磁波发射的信息泄漏和接收重建问题, 50 年代末, 美国和英国政府都提出了与此相关的 TEMPEST 计划, 计划涉及标准制定、产品测试规范、产品认证等. 1981 年, 美国颁布了 TEMPEST 标准; 1982 年, 英国和北约也颁布了类似标准, 这些标准都是非常机密的, 美国对这方面技术的保密与管理工作由国家安全局领导下的 TEMPEST 对抗工作组负责 [3] . 我国是从 80 年代中期开始注意这一领域的, 已经在计算机系统信息电磁泄漏机理、辐射信息的接收重建技术等方面取得了一些研究成果, 但因为起步晚, 许多课题尚有待深入研究和扩展 [4] .

信息技术设备在商业活动和现代战争中的地位日益突出, 计算机作为重要的信息处理和显示设备所产生的电磁辐射越来越受到人们的重视, 如果能够通过接收敌方信息技术设备的辐射检测出有用信息, 无疑会使我方在商业竞争和电子对抗处于主动地位. 本文主要针对计算机视频显示器进行电磁泄漏和信息重建的研究, 并提出了一套行之有效的方案.

2 计算机数据的电磁泄漏和重建原理

显示设备是计算机系统的重要组成部分, 它将计算机的内部信息转换成人眼能直接观察和识别的信息, 完成人机交互功能. 通过输入设备 (如键盘, 软驱, 光驱等) 将信息输入主机, 经过 CPU 处理后, 需要输出显示的数据被输送到显卡, 在时钟控制下, 显示器从显存中读取这些信息, 根据数据类型以字符或图形的形式将信息显示出来. 一般显示屏所采用的都是短余辉特性的阴极射线管, 要在显示屏上形成并维持一帧适合于观察的图像, 必须重复不断地向阴极射线管发送构成画面的信号, 这与普通的电视信号是相同的. 在显示器中, 不断地从存储器中读出数据, 经过字符或图像产生器, 产生一系列表示字符和图像的视频信号, 通过帧同步和行同步信号, 控制阴极射线管的阴极和扫描偏转系统, 在显示屏上显示并不断刷新画面. 电子束的强弱直接决定着像素点的亮度.

计算机的电磁辐射和信息泄漏主要有以下的途径: 显示器阴极射线管中的电子束、印刷电路板 (PCB) 、电缆与接口等基本部件 [5,6] . PCB 上的主要器件是集成电路芯片, 尺寸很小, 内部电路复杂, 驱动电流较小, 其总体辐射作用也很小. 而且信号大都是并行的, 因此辐射信号非常复杂, 即使能接收到也很难复原. 所以 PCB 对信息泄漏不会构成大的威胁. 计算机系统常用的显示器是 CRT 显示器, 一般都是串行控制. 正因为如此, 也是信息泄漏的主要部件之一, 其基本结构如图 1 所示.

[1] 2001-11-30 收到, 2002-08-29 改回

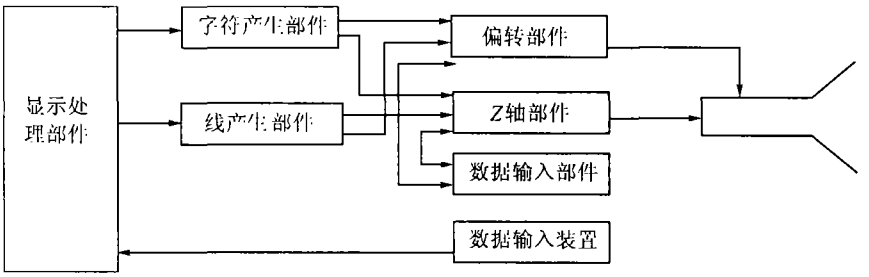


图 1　典型的 CRT 显示器结构图

目前，大多数的 CRT 采用光栅扫描方式显示信息，水平和垂直的同步信号控制电子束在 CRT 屏幕上从左到右，从上到下地有规律的运动，当电子束横扫过屏幕做水平运动时，用图像信号控制电子束在各点的亮度，以便在 CRT 屏幕上形成图像，当 Z 轴上的控制信号 (一般为视频信号) 改变时，屏幕上的信息也随之而改变。不难推断，以光栅扫描方式进行数据显示，其信息泄漏的主要来源是 Z 轴部件及与其控制信号相关的电子束电流。偏转信号中并不含有信息信号，但它含有同步信号，可以为泄漏信息的接收和重现过程中的扫描提供同步信息。另外，Z 轴部件的控制信号中还包含有与偏转扫描同步的控制信号 (消隐信号)。这样，只要能接收到这些辐射信号，通过必要的自适应滤波、放大、解调、锁相、分离等手段，便可以得到再现数据所必要的 Z 轴控制信号，和偏转扫描信号，从而使泄漏的数据信息得以复原。

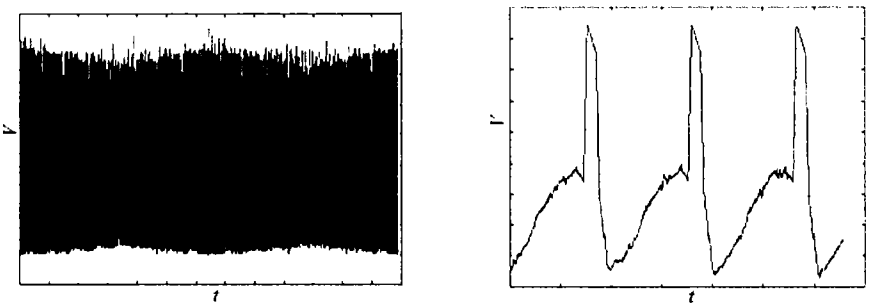
常用的偏转部件为磁偏转线圈，一组为水平偏转线圈，一组为垂直偏转线圈。在光栅扫描方式中，由水平和垂直偏转放大器产生的锯齿波电流激励偏转线圈，分别产生水平和垂直扫描所需要的磁场。根据锯齿波的傅里叶变换性质，容易得到锯齿波电流的傅里叶级数为

$$\left.\begin{aligned} I(t) &= \sum_{-\infty}^{\infty} C_n e^{jw_n t} \\ C_n &= \frac{I_0}{(T-t_r)jw_n}\frac{\sin(\pi t_r f_n)}{\pi t_r f_n}e^{j\pi t_r f_n} \end{aligned}\right\} \tag{1}$$

其中 T 为信号周期，t_r 为信号上升时间。通过研究其频谱衰减规律发现，在低频段辐射谱按每 10 倍频 20dB 增加，而在高频段，辐射谱按每 10 倍频 0dB 变化，即在高频段辐射也不会衰减，这就使得在远距离情况下，通过接收高次谐波来恢复同步信息成为可能。

CRT 中的电子束电流可达 0.2–1mA，由于电子束是受视频信号控制的，所以这种时变的电子束电流会在很宽的频率范围内产生辐射。其辐射场可以将电子束等效为导线中的电流进行分析。分析和试验结果表明，在低频段，辐射强度随频率增加而增加，在高频段，辐射则减弱，因此可以预言，CRT 电子束的辐射将主要集中在中、低谐波的频带上。计算机的时钟信号及其它各种周期信号的辐射频谱将是窄带的分离频谱，而各种随机信号等非周期信号的辐射频谱将是连续的宽带频谱。图 2 为显示器的辐射信号。

图 2(a) 是两帧的辐射信号，图 2(b) 是其中连续三行的信号。可以看出其中含有很强的行同步信号和帧同步信号，同时隐藏着视频信息。如果能提取其中的视频信息，再使用行同步和帧同步进行同步处理，便可以重建出原显示器上的图像了。



(a) 两帧辐射信号 (b) 三行辐射信号

图 2 显示器辐射信号

3 重建系统的组成及算法

为了实验验证视频信息所处的频段，本文从频域上对比了白屏和多组图像所辐射的信号，发现在 10MHz 以下有较明显的不同，因此可以断定 10MHz 以下包含了绝大多数的视频信息．从提高信躁比的角度考虑，对接收到的信号进行了 10MHz 的低通滤波，后经低噪声放大，再由 20M 高速 A/D 采集卡将其转化为数字信号存入计算机．图 3 为整个系统的结构框图．

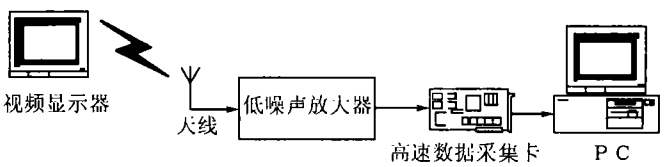


图 3 重建系统结构框图

计算机显示器上的图像是一种慢变化的信号．屏幕每秒刷新 60–120 帧，在一般情况下，图像在数秒钟并不会有较大的变化．也就是说，显示器上的图像在数百帧内可近似认为是不变的．显而易见，不同帧的信号是相关的，而不同帧中的噪声则是不相关的．按照帧周期对不同帧同一位置的信号进行多次积累，由于有用信号之间是相关的，因此 m 次积累后会加强 m 倍，而噪声信号是不相关的，m 次积累后只加强 $\sqrt{m}$ 倍．从 (2) 式可以看出累加次数越多，信号提取的效果越明显 [7] ．

$$\mathrm{SNIR} = (S/N)_{m\ 次积累}/(S/N)_{\ 不积累} = (mS/\sqrt{m}N)/(S/N) = \sqrt{m} \tag{2}$$

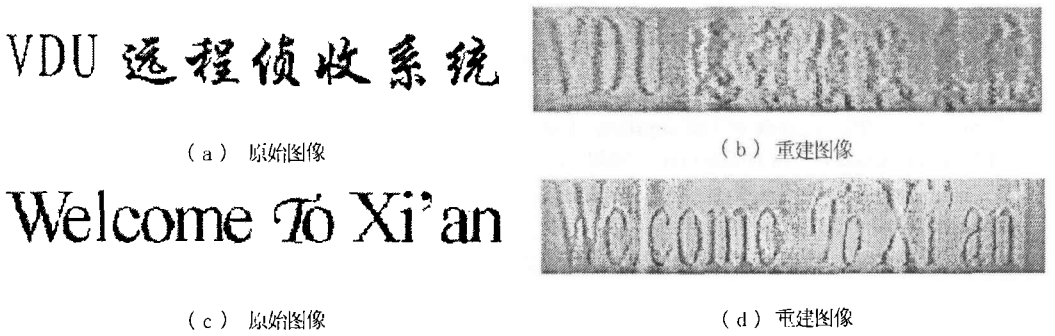
此时，视频信息仍然掩埋在很强的同步信号之中．然而同步信号有明显的规律，它不随图像的变化而变化．因此可以将一个白屏的辐射信号作为基准，用采集到的其它信号与之相减，则留下的主要是图像信息了．可是在实际应用时，白屏基准很难得到，鉴于各行的同步信号非常相似，而图像信息又有一定的随机性，文中取帧内各行信号的平均值作为基准．

采用上述方法得到一帧的数据之后，再按照行同步将其截断为一个二维的数组，该数组各元素的值就是所复原图像在该点的灰度．为了使效果更佳，有必要对所得的图像进一步处理．文中采用小波处理的方法提取图像特征，结果更清楚．

4 试验结果

显然，图像越复杂，则辐射信号的频率越高，这样对放大器和采集卡的要求越苛刻，同时后续的处理算法也有一定的难度．为了获得较好的效果，在实验的初期采用了简洁的图像进行重建．

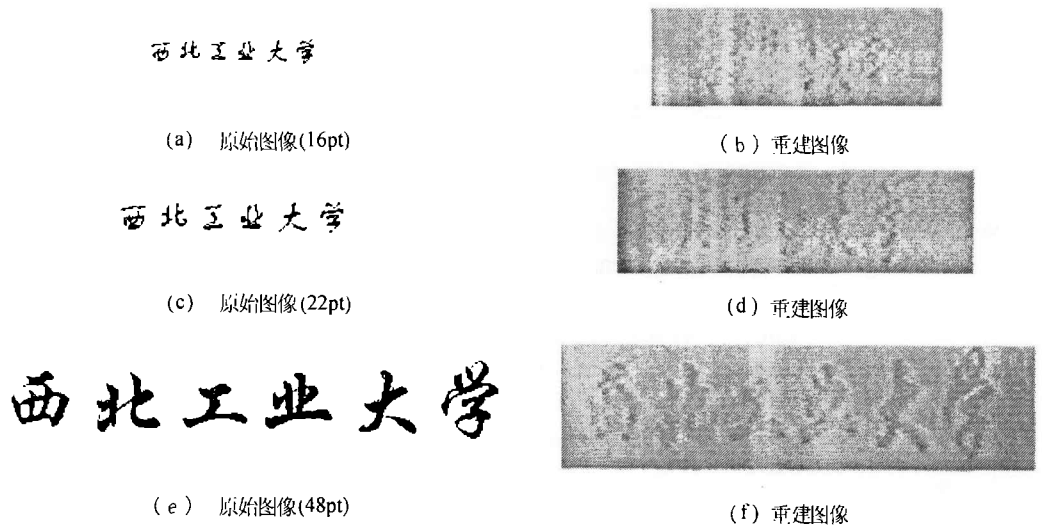
图 4 为原始图像和重建的图像，其中文字的大小均为 36 磅。可以看出由于英文字本身结构比较简洁，所以采用同样的采集系统和重建算法，它相对于结构复杂的汉字效果好一些。同样字体越大，所得到的图像将会更清楚，图 5 对不同大小的字体所重建的图像作了对比。



（a） 原始图像　　（b） 重建图像

（c） 原始图像　　（d） 重建图像

图 4　重建结果



(a)　原始图像(16pt)　　（b） 重建图像

(c)　原始图像(22pt)　　(d) 重建图像

（e） 原始图像(48pt)　　(f) 重建图像

图 5　不同大小字体的重建结果

5 结 论

本文给出了利用计算机显示器的电磁辐射泄漏获取其显示的信息的行之有效的侦收重建系统。基于理论分析的基础上，进行了整个系统的实现。试验结果表明图像越复杂，重建效果越差；字体越大，则得到的图像越清楚。该方法和采用电视机纯硬件重建系统相比，虽然实时性较差，但有很强的灵活性，易于功能扩展。

以上的实验结果是天线和被侦收的显示器相距 1m 并且单机工作的情况下测出来的。如果进一步提高侦收距离和清晰度以及侦收的定向性，则将会在军事、情报和商业等竞争领域内发挥重要的作用。

参 考 文 献

[1] H. J. Highland, Electromagnetic radiation revisited, Computers & Security, 1986, 5(1), 85–93.

[2] M. J. Riezenman, The rebirth of radio, IEEE Spectrum, 2001, (1), 62–64.

[3] M. G. Kuhn, R. J. Anderson, Soft Tempest: hidden data transmission using electromagnetic emanations, Second Workshop on Information Hiding, Portland, Oregon, 1998, (4), 124–142.

[4] 韩放著，计算机信息电磁泄漏与防护，北京，科学出版社，1993.12，第一章.

[5] P. Smulders, The threat of information theft by reception of electromagnetic radiation from RS-232 cables, Computers & Security, 1990, 9(1), 53–58.

[6] W. van Eck, Electromagnetic radiation from video display units: an eavesdropping risk?, Computer & Security, 1985, 4(3), 269–286.

[7] 林理忠，宋敏编著，微弱信号检测学导论，北京，中国计量出版社，1996.3，第四章.

RECONSTRUCTION OF THE IMAGE ON VIDEO DISPLAY UNIT BY ELECTROMAGNETIC LEAKAGE

Wu Changying Zhang Haobin Dong Shiwei Xu Jiadong

(*Dept. of Electronic Eng., Northwestern Polytechnical University, Xi'an* 710072, *China*)

Abstract Electromagnetic leakage of video display unit becomes the focus of wide interest recently. An image-reconstruction system is presented here using electromagnetic leakage from video display unit. In this system a loop antenna is employed to receive the radiation. After being magnified, A/D transferred, the received data are processed by computer to reconstruct the image. The experiment shows the feasibility and good performance of this system.

Key words Video display unit, Electromagnetic leakage, Reconstruction, Radiation, Wavelet transform

吴昌英： 男，1977 年生，博士生，主要从事于电磁场微波原理及天线理论的研究与应用.

张浩斌： 男，1976 年生，博士生，研究方向为飞机进气道雷达散射截面积理论与计算.

董士伟： 男，1974 年生，博士生，研究领域为电磁兼容与电磁防护.

许家栋： 男，1949 年生，教授，博士生导师，主要从事于电磁场与微波技术的理论研究工作.