

CRT 显示器信息电磁泄漏保熵性研究¹

董士伟 许家栋

(西北工业大学电子工程系 西安 710072)

摘要: 将 CRT 显示器和侦收系统组视为一个通信系统, 建立了不同显示内容时的两种信源模型和与之对应的信宿模型。结合信源熵损失率和信宿熵获取率的概念, 讨论了此通信系统的保熵性, 指出 CRT 显示器显示图像时系统不具备保熵性而显示文本时具备保熵性, 分析了造成以上区别的原因, 并提出一种防止 CRT 显示器显示文本时信息电磁泄漏的方法。文中给出的算例和实验结果都与理论分析一致。

关键词: CRT 显示器, 信息电磁泄漏, 图像, 文本, 保熵性

中图分类号: TN141, O441 **文献标识码:** A **文章编号:** 1009-5896(2004)03-0405-05

On the Entropy Preservation of Information Electromagnetic Leakage from CRT Visual Display Unit

Dong Shi-wei Xu Jia-dong

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

Abstract Considering CRT visual display unit and reconnaissance-receiving system as a communication system, this paper sets up two information source models and their corresponding information sink models of information's electromagnetic leakage from CRT visual display unit when image and text are displayed on the screen. Entropy preservation of the system is discussed combined with the concept of entropy loss rate of information source and entropy acquisition rate of information sink. A measure is put forward to ensure the information security of CRT visual display unit. The computational and experimental results show the consistence with the theoretical analysis.

Key words CRT visual display unit, Information electromagnetic leakage, Image, Text, Entropy preservation

1 引言

近年来, 计算机系统的信息电磁泄漏问题引起了广泛的兴趣, 越来越多的子系统成为研究的对象, 尤其是目前普遍使用的阴极射线管 (CRT) 显示器, 因其开放性和丰富的串行信号而成为关注的焦点, 针对其信息电磁泄漏原理、侦收和防护的研究不断深入^[1-3]。文献 [2] 设计的数字化侦收系统和文献 [4] 设计的模拟侦收系统通过接收 CRT 显示器电磁辐射, 实现了原始屏幕信息的重建, 然而这些侦收系统并非在所有显示状态下都能有效地工作。对于显示状态对侦收系统有效性的限制一直缺乏有针对性的研究。本文从信息论角度出发, 把 CRT 显示器和侦收系统看作一个完整的通信系统, 通过研究此系统的保熵性对上述问题进行了讨论。

文献 [5] 讨论了数据总线等并行复合源信息电磁泄漏的非保熵性, 其研究对象并非侦收系统的攻击目标, 信源模型和有关结论也都不适用于 CRT 显示器的情况。本文对静态图像和静态文本两种显示状态建立了信源模型和信宿模型, 分析了信源熵损失率和信宿熵获取率以及保熵

¹ 2002-10-27 收到, 2003-05-19 改回

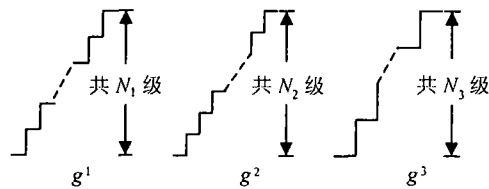


图 1 RGB 电子束电流密度级

性,指出只有在文本显示状态下,CRT 显示器信息电磁泄漏才具有保熵性,侦收系统才能有效工作。并根据研究提出一种防护 CRT 显示器信息电磁泄漏的方法。

2 CRT 显示器工作原理及其电磁辐射特性

目前显示器常用的是单枪三束 CRT, R, G, B 3 个电子束轰击屏幕玻璃内壁的三原色荧光粉,就形成具有一定色彩的像素。电子束在偏转系统控制下逐行扫描屏幕,实现图像的显示。

R, G, B 3 个电子束电流密度取值有一定的量化级别,如图 1 所示。显示器屏幕上的像素的色彩取决于 3 个电子束电流的强度及其比例,共有 $N_1 \times N_2 \times N_3$ 种可能的选择,一般 3 个电子束电流密度量化级别 g^1, g^2, g^3 分别由 n_1, n_2, n_3 位二进制数决定,则有 $N_1 = 2^{n_1}$, $N_2 = 2^{n_2}$, $N_3 = 2^{n_3}$ 。

CRT 显示器发射的“红信号”主要源自电子束的电磁辐射,侦收系统接收到的场强由两部分构成,一部分是电子束的辐射场,按照 A. J. Poggio 等人的观点^[6],其计算公式为

$$H(r, t) = \frac{1}{4\pi} \sum_{i=1}^3 \int_L \left[\left(\frac{1}{|r - r'|} + \frac{1}{c} \frac{\partial}{\partial \tau} \right) J_i(r', \tau) \times \frac{r - r'}{|r - r'|^2} \right] dL' \quad (1)$$

其中 r 和 r' 分别为场点和源点位置矢量, J_1, J_2, J_3 分别为 3 个电子束电流密度, c 为光速, $\tau = |r - r'|/c$ 。式中的积分沿电子束轴向进行。另一部分是显示器内部金属表面的散射场^[7]:

$$H^s(r, t) = \frac{1}{4\pi} \left[\nabla \times \int_S \frac{J(r', \tau)}{|r - r'|} dS' \right] \quad (2)$$

$J(r', \tau)$ 为金属表面上的电流密度,积分在金属表面上进行。这两种场都与电子束电流密度对时间的导数有关,而这种求导不会引起信息的丢失。

3 保熵性研究

3.1 信源模型

为简化讨论,本文的研究针对静态图像和静态文本展开。不考虑图像或文本像素色彩之间的约束,显示器屏幕所有像素色彩序列可看作一个离散无记忆源。

如前所述,一个像素的色彩由 R, G, B 3 个电子束电流决定,而它们分别有 N_1, N_2, N_3 种可能的取值,这样,可将 3 个电子束电流密度级别 (g^1, g^2, g^3) 视为三元随机变量,各随机变量相互独立,其样本容量为 $N_1 \times N_2 \times N_3$,联合概率分布为

$$(p(g_k^1, g_m^2, g_n^3))_{\substack{k=1,2,\dots,N_1 \\ m=1,2,\dots,N_2 \\ n=1,2,\dots,N_3}} = \frac{1}{N_1 \times N_2 \times N_3} \quad (3)$$

三元随机变量联合熵即信源熵^[8],可写为

$$H_{\text{Sou}}(G^1, G^2, G^3) = - \sum_{k=1}^{N_1} \sum_{m=1}^{N_2} \sum_{n=1}^{N_3} p(g_k^1, g_m^2, g_n^3) \lg(p(g_k^1, g_m^2, g_n^3)) \quad (4)$$

如果 CRT 显示器屏幕设为 $u \times v$ 像素, 则一屏图像的总熵为

$$H_{\text{sou}} = H_{\text{sou}}(G^1, G^2, G^3) \times u \times v \quad (5)$$

对普通“白底黑字”的静态文本, 像素只有两种可能的色彩, 每个电子束电流只有两个量化级别, 而且其中一个电子束电流级别取定, 另两个电子束电流随之而定, 这样, 信源模型就退化为一元随机变量, 样本容量为 2, 假设样本空间为 $\{0, 1\}$, 概率分布为

$$\begin{bmatrix} G \\ P(g) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0.5 & 0.5 \end{bmatrix}$$

根据熵的定义, 其信源熵为

$$H_{\text{sou}}(G) = - \sum_{n=1}^2 p_n \lg p_n = 1 \quad (6)$$

一屏文本的总信源熵为

$$H_{\text{sou}} = 1 \times u \times v \quad (7)$$

3.2 信宿模型

由式 (1) 可知, 作为信宿的侦收系统只是获取 3 个电流的总场信息, 原因是作为信源的三个电子束在空间相距太近, 实际侦收距离远大于此, 以致侦收系统根本无法分辨这 3 个电流, 那么信宿模型为一元随机变量, 其样本值为信源样本值的重量, 即 $g = g^1 + g^2 + g^3$ 。

对于显示图像的情况, 信宿随机变量样本容量为 $(N_1 + N_2 + N_3 - 2)$, 样本空间为 $\{0, 1, 2, \dots, N_1 + N_2 + N_3 - 3\}$ 。信宿获取的熵为

$$H_{\text{sin}}(G) = - \sum_{n=1}^{N_1+N_2+N_3-2} p_n \lg p_n \quad (8)$$

对于显示白底黑字文本的情况, 信宿样本容量为 2, 样本空间为 $\{0, 3\}$, 概率分布为

$$\begin{bmatrix} G \\ P(g) \end{bmatrix} = \begin{bmatrix} 0 & 3 \\ 0.5 & 0.5 \end{bmatrix}$$

信宿获取的通信熵为

$$H_{\text{sin}}(G) = - \sum_{n=1}^2 p_n \lg p_n = 1 \quad (9)$$

3.3 保熵性

如果定义通信系统中, 侦收系统的熵获取率为信宿熵与信源熵之比, 即

$$\eta = H_{\text{sin}}/H_{\text{sou}} \quad (10)$$

那么同时可以定义 CRT 显示器信息电磁泄漏的熵损失率

$$\bar{\eta} = 1 - \eta \quad (11)$$

η 越大, $\bar{\eta}$ 越小, 越有利于侦收系统重建 CRT 显示器的信息, 对 CRT 显示器的信息安全危害越大, 或反之。特别地, 当 $\eta = 1$, $\bar{\eta} = 0$ 时, 称 CRT 显示器信息电磁泄漏具备保熵性, 侦收系统可以完全恢复出 CRT 显示器的显示内容, 否则不具备保熵性。

显示图像时, 有

$$\eta = \frac{H_{\text{sin}}(G)}{H_{\text{sou}}(G^1, G^2, G^3)} = \frac{-\sum_{n=1}^{N_1+N_2+N_3-2} p_n \lg p_n}{-\sum_{k=1}^{N_1} \sum_{m=1}^{N_2} \sum_{n=1}^{N_3} p(g_k^1, g_m^2, g_n^3) \lg(p(g_k^1, g_m^2, g_n^3))}$$

由熵的基本性质可知 $\eta < 1$, 此时通信系统不具备保熵性。

显示白底黑字文本时, 有 $\eta = 1$, 说明通信系统具备保熵性。

3.4 算例及讨论

下面针对 3 种 CRT 显示器设置状态进行计算: (1) 全彩 (full color) 图像显示, 即 $n_1 = n_2 = n_3 = 8$, 则 $N_1 = N_2 = N_3 = 256$; (2) 256 色图像显示, 假设 $n_1 = 2, n_2 = 3, n_3 = 3$, 则 $N_1 = 4, N_2 = 8, N_3 = 8$; (3) 普通的文本显示。屏幕设置都是 1024×768 像素。按照前面的讨论, 分别计算信源熵、信宿熵和信源熵损失率, 结果列在表 1 中。

表 1 计算结果

设置 状态	像素信源 熵 (bit)	总信源熵 (bit)	像素信宿 熵 (bit)	总信宿熵 (bit)	信源熵 损失率 $\bar{\eta}$	信宿熵 获取率 η
(1)	24	18874368	9.0377	7107536.486	0.62343	0.37657
(2)	8	6291456	3.8065	2993553.408	0.52419	0.47581
(3)	1	786432	1	786432	0	1

根据表 1 的计算结果, CRT 显示器显示图像时, 电磁泄漏会损失 50% 以上的信息, 信宿仅获得一部分信源信息, CRT 显示器信息电磁泄漏不具备保熵性, 侦收系统远不能将其恢复出来; 显示文本时, 信宿获得所有的信源信息, 信息电磁泄漏具备保熵性, 侦收系统可以恢复出 CRT 显示器的屏幕信息。

下面就几个问题作较为深入的讨论:

(1) 上面的模型和计算没有计入各像素色彩之间的约束关系, 如果考虑这种约束, 信源模型和信宿模型都成为马尔可夫过程, 信源熵和信宿熵会同时减少, 但熵损失率和熵获取率都不变。

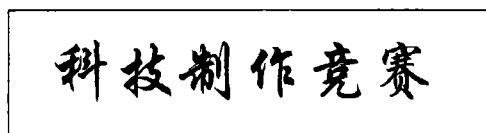
(2) 通信系统中信宿熵获取率从全彩图像显示时的 0.37657 提高到白底黑字文本显示时的 1, 其根本原因在于信源 3 个随机变量之间条件熵的降低及各随机变量样本容量的减少。

(3) 在较为敏感的文本显示情况下, 为了提高 CRT 显示器的熵损失率, 保证其信息安全, 可以使 3 个电子束在扫描底色和字体时总电流尽量接近。一种简单的情况是采用绿底红字, 即扫描底色时只有 G 电子束, 扫描字体时只有 R 电子束, 二者电流幅度设为相等, 这样 CRT 显示器的熵损失率提高到 1。

(4) 就信息技术设备信息电磁泄漏发展起来的 TEMPEST 技术是信息战的一种途径, 作为信息战的攻防双方, CRT 显示器的设计目的是尽量提高其熵损失率, 侦收系统的设计目的是尽量提高其熵获取率, 最高目的是获得通信系统的保熵性。

4 实验结果

用文献 [2] 设计的侦收系统对 CRT 显示器进行了侦收实验。CRT 显示器显示白底黑字的文本时, 侦收系统可以完全恢复出原始信息, 如图 2 所示。当 CRT 显示器采取了第 3 节提出的措施, 将文本设为绿底红字, 侦收系统就无能为力了, 如图 3 所示, 这时只能通过计算机系统中其他部分的电磁泄漏获取信息。

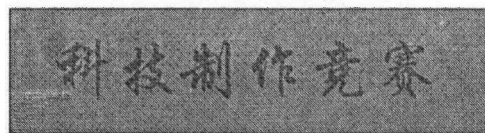


(a) CRT 显示器屏幕信息

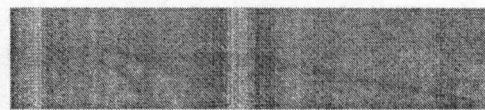


(b) 侦收系统重建信息

图2 侦收结果之一



(a) CRT 显示器屏幕信息



(b) 侦收系统重建信息

图3 侦收结果之二

5 结论

本文结合单枪三束 CRT 显示器的信息电磁泄漏机理和侦收系统原理, 根据显示内容的不同建立了不同的信源模型, 即图像显示时的三元离散无记忆源和文本显示时的一元离散无记忆源, 同时建立了一元离散信宿模型。文章分别讨论了两种信源模型下 CRT 显示器的信息电磁泄漏的保熵性, 指出信源为前者时不具备保熵性, 而信源为后者时具备保熵性。

为了保障 CRT 显示器的信息安全, 文章提出一种提高信源熵损失率的方法, 既破坏了 TEMPEST 通信系统的保熵性, 又保证了文本的可读性。文章提供的实验结果与理论分析一致。

本文从信息论角度研究了 CRT 显示器的信息电磁泄漏与侦收, 分析了信息战攻防双方的设计目的, 为 TEMPEST 技术研究提供了基础性理论依据。

参 考 文 献

- [1] Han Fang. Radiation emission from CRT of computer VDU. Rec. 1990 IEEE Int. Symp. on EMC, Washington D. C., USA, 1990: 483-487.
- [2] Dong Shiwei, Xu Jiadong, Zhang Haobin, *et al.*. On compromising emanations from computer VDU and its intercepting. 2002 3rd International Symposium on Electromagnetic Compatibility Proceedings, Beijing, China, May 21-24, 2002: 692-695.
- [3] Kuhn M G, Anderson R J. Soft tempest: Hidden data transmission using electromagnetic emanations. in David Aucsmith (Ed.), Information Hiding, Second International Workshop, Portland, Oregon, USA, April 15-17, 1998, Springer, LNCS 1525: 124-142.
- [4] Wim van Eck. Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security*, 1985, 4(4): 269-286.
- [5] 董文彬, 殷明, 康四军. 并行“复合源”电磁信息泄漏的非保熵性. 微波电磁兼容及超高频移动通信技术第三届全国学术会议论文集, 湖南张家界, Oct. 1996: 45-52.
- [6] R. 米特拉著, 金元松译. 计算机技术在电磁学中的应用. 北京: 人民邮电出版社, 1983: 197-207.
- [7] Rao S M, Wilton D R. Transient scattering by conducting surfaces of arbitrary shape. *IEEE Trans. on Antennas and Propagation*, 1991, 39(1): 56-61.
- [8] 朱雪龙. 应用信息论基础. 北京: 清华大学出版社, 2001: 14-38.

董士伟: 男, 1974 年生, 博士生, 研究领域为电磁兼容与通信安全技术。

许家栋: 男, 1948 年生, 博士生导师, 从事微波技术与计算电磁场方面的研究。