基于视觉效应的视频信息电磁泄漏抑制方法研究

王 森,邱 扬,田 锦,许清琳
(西安电子科技大学机电工程学院,陕西西安 710071)

摘 要: 计算机的电磁辐射会包含视频信息从而造成的信息泄漏,本文在随机置乱的基础上,根据人眼视觉效应提出了互补置乱的方法来抑制视频信息通过电磁辐射的泄漏.通过对相邻的每帧视频信息进行加减随机噪声,使得人眼视觉观察效果抵消掉噪声对视频图像的干扰,在叠加噪声的同时,保证了视频图像的清晰度,同样也达到了抑制视频信息电磁泄漏的功能.最后也通过实际截获实验,验证了该方法的可行性.

关键词: 视频信息;电磁泄漏;信息安全;互补置乱
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2017)08-2038-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.08.033

Research on Method for Preventing Digital Video Signal Electromagnetic Leakage Based on Visual Effect

WANG Sen, QIU Yang, TIAN Jin, XU Qing-lin
(*School of Mechani-Electronic Engineering of Xidian University, Xi'an, Shaanxi* 710071, *China*)

Abstract: The electromagnetic radiation of computer contains video information which causes the information leakage. In this paper, a method is proposed according to the effect of human visual, based on the random scrambling, which called complementary scrambling, for preventing the leakage of video information through the electromagnetic radiation. The effect of human visual can eliminate the interference of noise to video image by adding and subtracting the random noise to each contiguous frame of video information, and imposes noise on displayed screen images while keeping the quality of the image. And realize the function of preventing the video information electromagnetic leakage. Finally, the feasibility of the method is verified by experiments.

Key words: video information; electromagnetic leakage; information security; complementary scrambling

1 引言

从1985年Van Eck发表了计算机视频信息会通过电磁辐射造成信息泄漏[1],计算机信息的电磁辐射就引起人们的重视.随着TEMPEST(Transient Electromagnetic Pulse Emanation Surveillance Technology)技术的快速发展,各国对该技术的研究更加广泛和深入.电磁信息泄漏的抑制技术也应用而生,大量研究资料表明,计算机视频系统是整个计算机系统中电磁辐射最强、可视信息量最大的,其产生的泄漏信息最易于被接收和复现[2].

对基于VGA视频接口的防泄漏技术的研究已较为成熟,多采用屏蔽、滤波和抖动伪发射[3~5]等技术防止有用视频信息的泄漏.日本学者提出了外加一个相关噪声干扰装置[6],将视频信息相关的频谱分布进行覆盖,然而此方法会增加计算机的电磁辐射强度.对于近年来已被广泛使用的数字视频接口,英国剑桥大学Kuhn提出了把低重要位的视频数据随机化的防泄漏方法[7],实现了数字视频信号的噪声叠加,使其在时域和频域均为白噪声特性,从而无法被截获复现.但是,置乱后的文字图像在显示质量上大幅下降,给使用者正常的工作造成不便.

HDMI接口线缆 HDMI接口是现在比较主流的数字视频接口,笔记本、台式机等电脑均有HDMI接口,且HDMI线缆广泛应用于多种显示系统.高达Gbit/s传输速率的视频信号在HDMI线缆数据通道中串行传输,使得线缆的电磁辐射更强.

本文以HDMI接口线缆为研究对象,在数字视频系

收稿日期:2016-01-15;修回日期:2016-06-27;责任编辑:蓝红杰
基金项目:国家973重点基础研究发展规划(No.2015CB857103)

统防泄漏理论研究的基础上,结合人眼的视觉特性,找出了一种符合人眼感知的新的防泄漏技术—互补置乱,其在继承原有随机置乱技术在防泄漏方面优势的基础上,大大改善了置乱后图像的显示质量. 研制了HDMI 接口的数字信号处理板卡,经过视频信息电磁泄漏的截获测试,验证达到了数字视频信息安全性与可用性的平衡.

2　互补置乱原理

在随机置乱的基础上,利用人眼视觉暂留特性,人眼长期暴露在不断快速变化的颜色当中,会对快速变化的前后几帧图像产生视觉混合效应. 将随机置乱与混色原理相结合,通过对视频相邻两帧的图像信息上加/减噪声,人眼视觉的互补进而消除所叠加随机噪声对图像的影响,提高视频图像的清晰度.

2.1　随机置乱

视频图像的数据信息(RGB)分别通过三个数据传输通道进行传输. HDMI 接口框图如图 1 所示. 当串行的数字视频信息通过 HDMI 线缆的电磁辐射而被截获者接收,即可获得视频图像信息,进而还原显示图像.

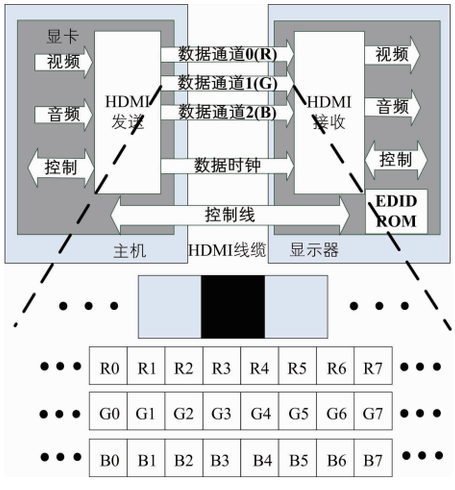


图1　HDMI接口框图

随机置乱的基本思想是在显卡后的串行传输的视频信号中混入伪随机序列,即在 HDMI 线缆上的视频信号叠加上随机噪声,使得 HDMI 线缆的电磁辐射具有趋向白噪声功率谱的特性,降低视频信号功率,增加噪声信号的功率,从而降低接收到电磁信号的信噪比,以抑制数字视频信息的截获恢复.

根据有用信息与背景之间不同颜色差别,确定视频数据重要位. 数字视频数据由 RGB 三个通道构成,每个通道用 8 位二进制数表示一个像素点的颜色,都可以表示 256 种颜色. 数值越大,表示这个通道对应颜色所占比例就越大. 不同的像素值对比如图 2 所示.

(*a*) RGB值为10 (00001010)　(*b*) RGB值为138 (10001010)　(*c*) RGB值为146 (10001110)

图2　视频数据像素对比

图 2(*a*)和(*b*)的像素序列只有最高位不同,其他都一样,但很明显颜色差别很大,而(*b*)和(*c*)的像素序列只有一个低位不同,其他一样,颜色差别却很小. 可见,二进制数的高位对于视频图像影响最大. 因此在置乱过程中选择将低重要位置换成伪随机序列,牺牲一部分图像细节来获得所需的置乱效果. 随机置乱方法如图 3 所示,如图中一个白色像素点的每个子像素置乱 4 位的情况,4 位二进制数的最大变化范围为 1111,也即十进制的 15,只占到量化范围的 6% 左右,因此仅在仔细观看时才能看到图像质量的下降,随着置乱位数的增加,子像素的取值变化范围也更大,如图 4 中置乱 5 位和 6 位的情况所示,图像质量的下降也愈明显.

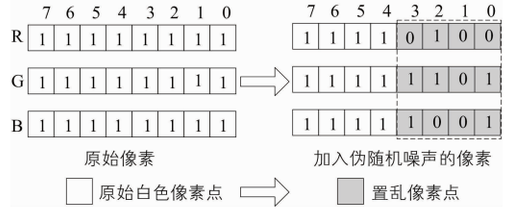


图3　随机置乱原理

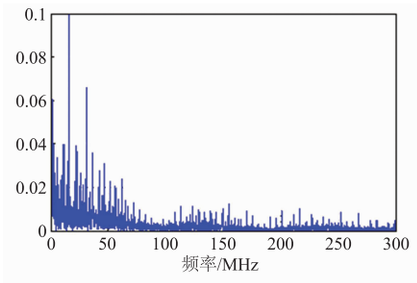
(*a*) 原始图像　(*b*) 置乱五位　(*c*) 置乱六位

图4　随机置乱图像效果

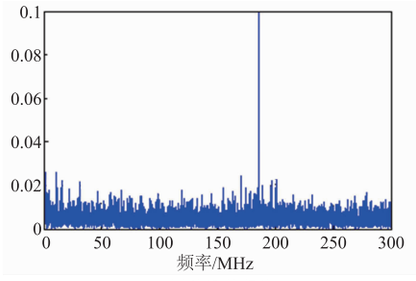
置乱程度的越高,即对视频数据置乱的位数越多,则电磁抑制效果越好,但图像质量会越差. 置乱程度的选取应在保证视频信息不能被截获还原情况下尽量保证图像质量. 图 5 为同一图像置乱前后 HDMI 线缆上传输时电磁辐射频谱仿真计算图,可见置乱后的频谱更为杂乱.

具体置乱程度的电磁泄漏抑制效果则需要在实际的电磁泄漏截获测试中确定. 本文中,经过多次测试验证置乱 5 位后则不能截获还原图像信息.

当置乱程度为 5 位时,像素信息数据的 8 位原始数据中的 5 位被置换为随机序列,其中有用信号的位数只剩 3 位. 根据 TMDS 编码规则,TMDS 编码后,一个像素信息数据的 10 位数据中有 7 位是随机序列,有用信息



(*a*) 置乱前的频谱



(*b*) 置乱后的频谱

图5 随机置乱前后频谱图

只占30%. 根据信噪比SNR计算公式,信号的电压值与噪声的电压值相同,故SNR为0dB,且噪声所占比例比信号所占比例要高. 在文献[8]中的研究表明,当SNR低于0dB时,则图像信息不能被截获还原.

2.2 混色原理

根据人眼的视觉特性和格拉斯曼(Grassman)定律可知,计算机在传输和重现文字图像时,只是重现其不同的颜色感. 而几乎所有的颜色都可以由三种基色按不同的比例混合得到. 这就是著名的颜色计量基础——三基色原理.

计算机液晶显示器也应用了三基色原理,将自然界中的任意景象分解成红、绿、蓝三种基色,再将三基色经编码处理送到接收端,在接收端将红、绿、蓝三种基色相加混色,在显示屏幕上恢复原来的彩色景物. 常用的RGB色深为256,则可以构成1600万种颜色. 计算机显示图像信息如图6所示.

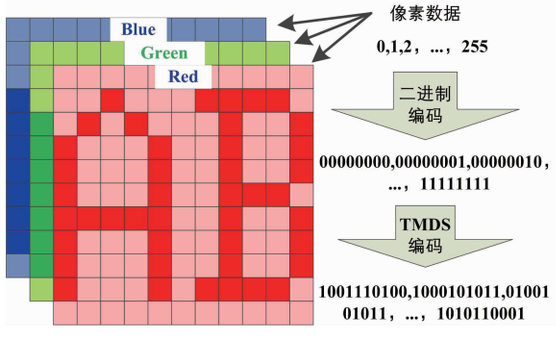


图6 像素RGB信息

如果进行混色的各种颜色的相对强度发生变化,那么就会产生不同的新颜色. 在混色原理中,由两种等量的基色相混合而产生的第三种颜色称为补色,因此与红、绿、蓝三基色对应的三补色为青、紫、黄.

相加混色有很多种方式,其中一种方式为时间混色. 在这种混色方法中,各基色是在不同时间出现的. 将三基色光按一定比例轮流投射到同一屏幕上,只要交替的速度足够快,由于人眼的视觉暂留特性,产生的彩色视觉与三基色直接相混时一样. 当人眼看到的影像消失后,人眼能继续保留其影像0.05–0.2秒左右的图像,当连续的图像变化超过每秒24帧画面的时候,人眼便无法分辨每幅单独的静态画面,因而看上去是平滑连续的诗句效果. 而计算机显示器在显示图像时,以60帧每秒以上的速度进行刷新屏幕,所以人眼无法对每帧图像进行独立观察. 时间混色原理正是互补置乱技术的理论出发点.

2.3 互补置乱理论

根据上述的随机置乱原理和时间混色原理,本文提出了互补置乱方法对视频数据进行处理,在达到叠加随机噪声抑制视频信息电磁泄漏的同时保证图像的视觉清晰程度. 在数字视频信息传输过程中,通过对前后相邻两帧图像数据序列分别加上和减去同一伪随机序列数,使视频数据在传输过程中在时域上表现为随机序列,在频域上上表现为随机频谱,从而无法被截获复现. 此过程与随机置乱所达到的防泄漏效果类似,都是通过对视频数据叠加噪声,降低视频信号的信噪比. 但互补置乱的优势在于显示过程中,同一位置的像素点在前后两帧加上和减去的伪随机数相同,根据时间混色原理,在显示时达到相邻帧间的图像颜色像素值在人眼视觉效果下达到了混合互补,平均了由于置乱所引入的伪随机噪声,使得互补置乱后的图像整体上更加接近于原始图像的显示效果,如图7所示.

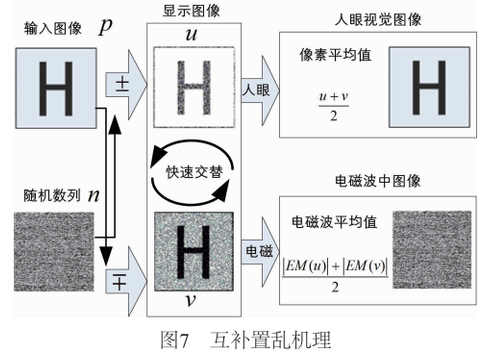


图7 互补置乱机理

当在计算机显示器进行多帧图像序列顺序显示,如图8所示,经过加减置乱快速交替进行,可以达到互补置乱时间混色的视觉效果.

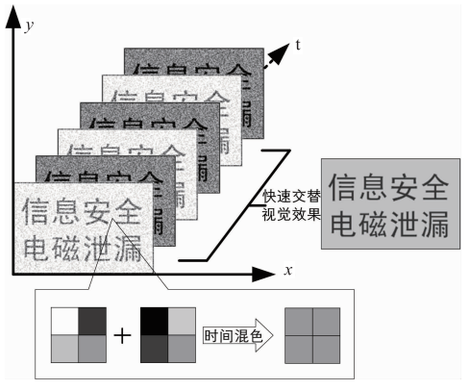


图8　数字视频互补置乱显示示意图

以 $n_{x,y}$ 代表产生的噪声,则原始像素 $p_{x,y}$ 加减噪声产生的两幅子图像分别为 $p'_{x,y}=p_{x,y}-n_{x,y}$;$p''_{x,y}=p_{x,y}+n_{x,y}$. 当以最快的刷新频率切换这两帧的时候,人眼观察到的将是两帧的平均值[9]:

$$\frac{p'_{x,y}+p''_{x,y}}{2}=\frac{p_{x,y}-n_{x,y}+p_{x,y}+n_{x,y}}{2}=p_{x,y} \tag{1}$$

两帧平均值又返回到原始像素值,验证了互补算法在提高视觉效果上的结论.

每一帧加载的噪声必须满足是相关的噪声,即要保证截获接收方不能通过互相关的方式滤掉噪声. 假设所加载相同的噪声皆为 $n_{(t)}$,则前一帧置乱视频数据为 $p_{x,y}+n_{x,y}$,后一帧置乱视频数据为 $p_{x,y}-n_{x,y}$,对两者做相关运算得到前后两帧视频数据的相关系数 $\Phi_{sv}(\tau)$:

$$\begin{aligned}&\Phi_{sv}(\tau)\\&=\int_{-\infty}^{+\infty}[p_{x,y}(t+\tau)+n_{x,y}(t+\tau)][p_{x,y}(t)-n_{x,y}(t)]\mathrm{d}t\\&=\int_{-\infty}^{+\infty}p_{x,y}(t+\tau)p_{x,y}(t)\mathrm{d}t-\int_{-\infty}^{+\infty}p_{x,y}(t+\tau)n_{x,y}(t)\mathrm{d}t\\&+\int_{-\infty}^{+\infty}n_{x,y}(t+\tau)p_{x,y}(t)\mathrm{d}t-\int_{-\infty}^{+\infty}n_{x,y}(t+\tau)n_{x,y}(t)\mathrm{d}t\\&\approx R_{vv}(\tau)-R_{nn}(\tau)\end{aligned} \tag{2}$$

从式(2)看到,如果前后两帧所加的噪声没有相关性,则经过截获接收的相关去噪功能会把所加的噪声滤掉. 而由于前后相同噪声的具有相关性,截获机做相关去噪后最终得到的依然是视频数据减去一帧噪声,并不能从视频数据中滤除噪声.

3　互补置乱过程

根据 HDMI 接口的视频传输协议,对计算机显卡输出后的视频信号进行泄漏抑制的信号处理,具体方案如图 9 所示. 显卡 HDMI 端口输出的视频信号接收后分离出视频信号,将视频信号进行互补置乱处理,即对相邻帧的视频信息分别加减噪声.

3.1　互补置乱算法

当读入第 n 帧图像,对这一帧图像加上事先生成的噪声 $n_{(x,y)}$,然后读入第 $n+1$ 帧图像,对这一帧图像减去同样的噪声 $n_{(x,y)}$. $p_{(x,y)}$ 代表了一帧图像中坐标为(x,y)的像素,$u_{(x,y)}$ 和 $v_{(x,y)}$ 分别代表了新生成的前后两帧子图像中的坐标为(x,y)的像素.

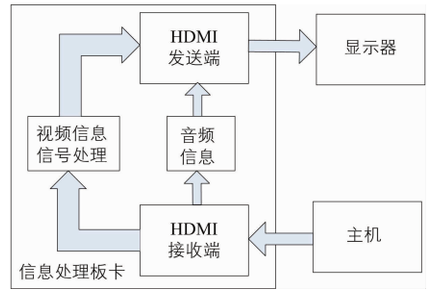


图9　HDMI接口视频信息泄漏抑制方案

互补置乱核心算法流程如下所示:

(1)生成一帧视频图像大小的噪声,$n_{(x,y)}$ 代表了其中的每个随机噪声值,由 2.1 节可知置乱 5 位即可,故 $n_{(x,y)}$ 为 0 ~ 31 的随机值.

(2)读入 $p_{(x,y)}$;

(3)计算 $u_{(x,y)}=p_{(x,y)}+n_{(x,y)}$,如果 $u_{(x,y)}>255$,则取 $u_{(x,y)}=255$;

(4)计算 $v_{(x,y)}=p_{(x,y)}-n_{(x,y)}$,如果 $v_{(x,y)}<0$,取 $v_{(x,y)}=0$;

(5)以最高的刷新速率轮流显示 $u_{(x,y)}$ 和 $v_{(x,y)}$.

3.2　黑白文字的互补置乱

通常文本信息均是白底黑字,黑白文字所携带的信息量是最大的,而互补置乱在黑白文字的加减噪声上会出现一种杂乱的颜色变化. 由上节引入的算法第三条,计算 $u_{(x,y)}=p_{(x,y)}+n_{(x,y)}$,如果 $u_{(x,y)}>255$,则取 $u_{(x,y)}=255$;计算 $v_{(x,y)}=p_{(x,y)}-n_{(x,y)}$,如果 $v_{(x,y)}<0$,取 $v_{(x,y)}=0$. 当显示一幅纯黑白文字时,以白色为例上来说明这种镂空:前一帧白色 255 加噪声 $n_{x,y}$ 仍然为 255,下一帧减 $n_{x,y}$ 不做替代,所以有:

$$\begin{aligned}\frac{p'_{x,y}+p''_{x,y}}{2}&=\frac{p_{x,y}-n_{x,y}+p_{x,y}+n_{x,y}}{2}\\&=\frac{255-n_{x,y}+255}{2}=255-\frac{n_{x,y}}{2}\neq p_{x,y}\end{aligned} \tag{3}$$

由此可见,平均后的值不再是原先像素值,出现了颜色杂乱变化. 加噪声时,所有的白色像素点不变,而仅仅黑色像素点加上了噪声同理,在减噪声时,所有的黑色像素点不变,而仅仅白色像素点减上了噪声.

所以鉴于黑白文字这种特殊情况,采取将黑白文字加减一个常数后,即变成灰阶文字图像后再采用互补置乱. 将原始图像黑/白像素 $P_R(x,y)$ 进行加/减一个常数 C 后,再进行前一帧加,后一帧减运算,并且限制所加噪声在参数 C 的范围内变化. $PW_R(x,y)$ 代表白色

像素点，$PB_R(x,y)$代表黑色像素点，则加噪声后生成的一帧子图像中白色像素和黑色像素分别为：

$$\begin{cases} P'W_{(x,y)} = PW_{R(x,y)} - C + C \oplus N_{(x,y)} \\ P'B_{(x,y)} = PB_{R(x,y)} + C + C \oplus N_{(x,y)} \\ C = \sum_{i=0}^{n} 2^i, n = 0,1,2\cdots 7, \\ \text{s.t. } N(x,y) \in [0,1] \end{cases} \tag{4}$$

减噪声后生成的一帧子图像中白色像素和黑色像素分别为：

$$\begin{cases} P''W_{(x,y)} = PW_{R(x,y)} - C - C \oplus N_{(x,y)} \\ P''B_{(x,y)} = PB_{R(x,y)} + C - C \oplus N_{(x,y)} \\ C = \sum_{i=0}^{n} 2^i, n = 0,1,2\cdots 7, \\ \text{s.t. } N(x,y) \in [0,1] \end{cases} \tag{5}$$

其中 C 的取值限制于图像可识别性和视频信息安全性. 其值越大，则加载噪声位数越多，视频信息就越安全，但图像可识别性随之下降，见表 1 所示.

表 1 评价结果对照表

参数范围 \ C	3	7	15	31	63	127
置乱位数	2	3	4	5	6	7
白色置乱范围	0 ~ 3	0 ~ 7	0 ~ 15	0 ~ 31	0 ~ 63	0 ~ 127
黑色置乱范围	252 ~ 255	248 ~ 255	240 ~ 255	224 ~ 255	192 ~ 255	128 ~ 255
最小色阶差值	249	241	225	193	129	1

由于八位数值分别为：128、64、32、16、8、4、2 和 1，当 C 值取 63 时（即低 6 位的和为 63），表示可对低六位进行置乱，置乱程度达到 6 位. 若 C 取 64 表示只对第 1 位和第 7 位置乱，置乱位数反而只有 2 位，并不合理. 所以 C 一般在表 1 所示的特殊值上取值.

经过表中对比及实验中的实际显示对比，本文取 C 值为 31 最为合理. 白色像素（255）减去 C，像素值在 224 ~ 255 之间变动；黑色像素（0）加上 C，像素值在 0 ~ 31 之间变动，背景色与前景色之间色阶至少相差 193，置乱程度也达到 5 位，同时满足了图像可识别性和视频信息安全性.

4 测试验证

针对 HDMI 接口的计算机，研制了基于数字信号处理的信息泄漏抑制板卡（如图 10），信号处理板卡主要分为 HDMI 信号接收解码模块、信号处理模块、HDMI 信号发送编码模块以及电源模块. 信号处理模块采用 FPGA 芯片，通过编程采用本文提出的方法对原始信号进行处理发送到显示器. 板卡的安装如图 11 所示.

对视频图像的处理效果如图 12 所示，可见基于视觉效应提出的互补置乱弥补了随机置乱算法带来的视觉损失效应，图像的清晰度以及亮度都得到极大的提升. 对计算机进行实际图像的截获测试，测试结果如图 13 所示.

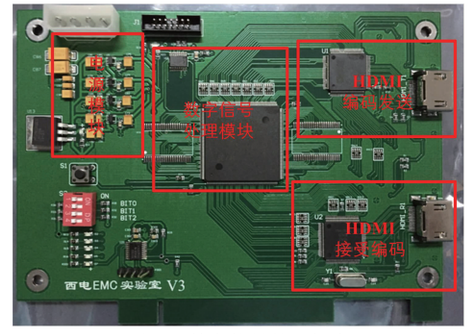


图10 数字信号处理板卡

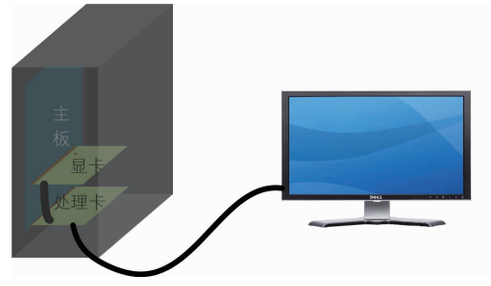


图11 板卡安装示意图

(*a*) 原始图像

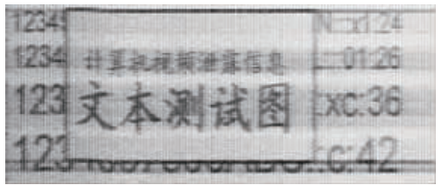
(*b*) 随机置乱图像

(*c*) 互补置乱图像

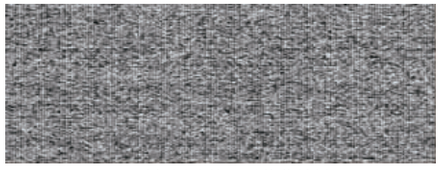
图12 互补置乱的视觉质量改善效果图

由图 13 可知，未处理的视频图像截获接收机可以将图像完整再现，而随机置乱和互补置乱后则截获接收机则不能将图像复现，但是互补置乱处理后的计算机显示器所显示的图像比随机置乱后的图像要清晰很多. 根据图像信噪比计算公式：

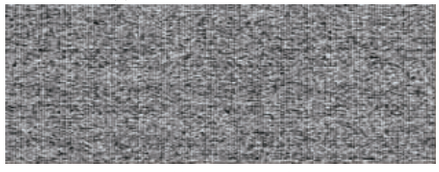
$$PSNR = 10\lg\left(\frac{MAX^2}{MSE}\right) \tag{6}$$



(*a*) 未处理截获结果



(*b*) 随机置乱处理后截获结果



(*c*) 互补置乱后处理结果

图13　互补置乱的视频截获结果

$$MSE = \frac{1}{mn}\sum_{i=0}^{i=m-1}\sum_{j=0}^{j=n-1} I(i,j) - K(i,j)^2$$

式中 $I(i,j)$ 为原始图像值,$K(i,j)$ 为处理后的图像值.

图 12(*b*)的图像信噪比为 23.01dB,而图 12(*c*)的图像信噪比为 38.44dB. 互补置乱与随机置乱都实现了噪声叠加,但互补置乱达到最小的视觉损失效果.

5　结论

本文在随机置乱的基础上,根据人眼视觉效应提出了互补置乱的方法来抑制视频信息通过电磁辐射的泄漏,通过对相邻的每帧视频信息进行加减随机噪声,使得人眼视觉观察效果抵消掉噪声对视频图像的干扰,在叠加噪声的同时,保证了视频图像的清晰度,同样也达到了抑制视频信息电磁泄漏的功能. 最后也通过实际截获实验,验证了该方法的可行性.

参考文献

[1] Wim van Eck. Electromagnetic radiation from video display units: an eavesdropping risk? [J]. Computers & Security, 1985, vol 4: 269 – 286.

[2] Y-I Hayashi, N Homma, T Watanabe. Introduction to the special section on electromagnetic information security[J]. IEEE Trans on EMC, 2013, 55(3): 539 – 546.

[3] 邱扬,任华胜,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, et al. Information electromagnetic emanation analysis of the video display unit for computers [J]. Journal of Xidian University, 2002, 29(5): 693 – 697. (in Chinese)

[4] 邱扬,魏丽丽,等. 基于数字滤波的计算机视频信息防泄漏研究[J]. 电子学报,2008,36(6): 1188 – 1192.
Qiu Yang, Wei Lili, et al. Research on anti-leakage of computer video signal based on digital filtering[J]. Acta Electronica Sinica, 2008, 36(6): 1188 – 1192. (in Chinese)

[5] 邱扬,闫美云,等. 基于抖动及图像融合的计算机视频信息防泄漏研究[J]. 电子学报, 2008, 36(12): 2493 – 2496.
Qiu Yang, Yan Meiyun, et al. Research on Anti-leakage of computer video signal based on dither and image fusion [J]. Acta Electronica Sinica, 2008, 36(12): 2493 – 2496. (in Chinese)

[6] Y Suzuki, Y Akiyama. Jamming technique to prevent information leakage caused by unintentional emissions of PC video signals[A]. IEEE International Symposium on Electromagnetic Compatibility[C]. IEEE, 2010. 132 – 137.

[7] Markus Kuhn. Electromagnetic eavesdropping risks of Flat-Panel displays[A]. 4th Workshop on Privacy Enhancing Technologies [C]. Berlin, Heidelberg: Springer, 2004. 1 – 20.

[8] Tae-Lim Song, Yi-Ru Jeong, Jong-Gwan Yook. Modeling of leaked digital video signal and information recovery rate as a function of SNR[J]. IEEE Trans EMC, 2015, 57(2): 164 – 172.

[9] Aoki Hisashi, Sato Soichi, Yoshida Tetsushi, Takei Jiro. Liquid crystal display by means of time-division color mixing and voltage driving methods using birefringence[P]. United States Patent: 6115014, 2000.

作者简介

王　森　男,1989 年生于河北石家庄. 西安电子科技大学机电工程学院博士研究生. 研究方向为电磁兼容与计算机电磁信息安全.
E-mail: wangsen3356@126.com

邱　扬　男,1957 年生于陕西西安. 西安电子科技大学机电工程学院教授,博士生导师,电磁兼容性国防科技重点实验室客座教授. 主要研究方向为移动通信系统电磁兼容设计、信息技术设备的信息安全技术、强电磁脉冲防护.