

DOI:10.19651/j.cnki.emt.2106333

一种低采样率下 VGA 线缆辐射信息恢复方法

杨旺霖¹ 苏新彦¹ 姚金杰¹ 石森² 马欣瑜¹

(1.中北大学 信息探测与处理技术重点实验室 太原 030051; 2.中国电子科技集团公司 信息产业信息记录及防泄漏产品质量监督检验中心 太原 030032)

摘要: 在计算机系统电磁辐射的信息泄漏中,视频信号是最容易被截获及恢复的信息。针对计算机系统 VGA 线缆传导发射的视频信号的恢复问题,建立了计算机模拟视频信号在 VGA 传输通道中的传输及电磁辐射模型,分析了模拟视频信号的成像规则以及采集过程中模拟视频信号在各个阶段的时域特性,得到了 VGA 线缆辐射的模拟视频信号的恢复步骤。由于低采样率下恢复的单帧视频信号质量差,故根据视频信号的成像规则将连续多帧恢复图像重叠,即可在低采样率下得到质量较高的恢复图像。仿真结果表明,该方法可有效增加视频图像的恢复质量,在低采样率下恢复质量的提升尤为明显。为验证仿真结果的正确性,对实际截获的 VGA 线缆辐射信息进行还原,所得结果与仿真基本符合。

关键词: 视频信息;信号处理;TEMPEST;电磁辐射;信息安全

中图分类号: TP309.1 **文献标识码:** A **国家标准学科分类代码:** 520.10

A recovery method of VGA cable radiation information at low sampling rate

Yang Wanglin¹ Su Xinyan¹ Yao Jinjie¹ Shi Sen² Ma Xinyu¹(1. State Key Laboratory of Electronic Testing and Proceeding Technology, North University of China, Taiyuan 030051, China;
2. Information Industry Information Record and Anti Leakage Product Quality Supervision and Inspection Center, China Electronic Technology Group Corporation, Taiyuan 030032, China)

Abstract: In the electromagnetic radiation information leakage of computer system, video signal can be intercepted and recovered easily. Aiming at the problem of video signal recovery of VGA cable radiation in computer system. The transmission and electromagnetic radiation model of computer analog video signal in VGA transmission channel are established. The imaging rules of analog video signal and the time domain characteristics of analog video signal in each stage during transmission are analyzed. The recovery steps of analog video signal radiated by VGA cable are obtained. Due to the poor quality of the quality of single frame video signal recovered at low sampling rate, according to the image presentation rules of video signal, multiple consecutive recovered images are overlapped, and the recovered image with high quality can be obtained at low sampling rate. Simulation results show that this method can effectively improve the quality of video image restoration, especially at low sampling rate. In order to verify the correctness of the simulation results, the actual intercepted VGA cable radiation information is restored, and the results are in accordance with the simulation.

Keywords: video information; signal processing; TEMPEST; electromagnetic radiation; information security

0 引 言

近年来,随着物联网技术的蓬勃发展,大量电子设备的使用导致电磁辐射广泛存在于人们的生产活动中^[1]。大量的电磁辐射除造成电磁兼容问题外,电磁辐射中携带的有效信息还会引发信息泄漏的风险^[2-3]。视频信号作为计算

机系统中最易被截获和复现的有用信息,对其在线缆传导发射的采集与恢复一直都是电磁信息安全研究的热点^[4]。由于模拟视频信号在计算机系统的显示设备中被广泛使用,故对 VGA 线缆传导发射的模拟视频信号的恢复开展研究在信息安全领域的意义重大。

在模拟视频信号被投入使用至今,对 VGA 线缆电磁

辐射的模拟视频信号的恢复已存在多方面的研究。已有研究从显示设备类型^[3]、信噪比^[6]、视频信号内容^[7]等方面对视频信号的恢复质量的影响展开探讨。对视频信号频率的获取,主要有自相关方法^[8]和脉冲波时频特性法^[9]两种。

以上研究虽然较为深入地讨论了恢复 VGA 线缆辐射中模拟视频信号的问题,但研究中视频信号的采样频率均高于视频信号频率的 10 倍以上,在采样信号的带宽上足够充裕,故它们并未对采样率与视频信号恢复质量的关系进行探究,亦没有探讨低采样率下恢复 VGA 线缆辐射中视频信号的可行性。为此,本文根据模拟视频信号的组成及呈像规则,讨论了模拟视频信号的时域特性,分析了电磁截获模拟视频信号的恢复过程,并提出了在低采样率下提高电磁截获模拟视频信号恢复质量的方法。此方法大幅增加了低采样率下视频信号的恢复质量,使视频图像中的细节更为显著,更好地避免了视频图像信息丢失。

1 模拟视频系统构成

模拟视频信号为复合信号,且其各个部分存在时序上的联系。显示设备根据信号各部分的时序关系,通过特定的呈像规则,即可将模拟视频信号恢复为视频图像。了解模拟视频信号的构成以及其呈像规则,是将 VGA 线缆辐射的模拟视频信号还原成视频图像的前提。

1.1 模拟视频信号的组成

模拟视频信号是由 RGB 信号、行同步信号和场同步信号组成的复合信号。其中,RGB 信号通过 3 个并行分量对 G、R、B 三原色进行叠加以决定每一个像素的颜色,行同步信号决定了每一行像素刷新的频率,场同步信号决定了每一帧视频刷新的频率^[10]。

RGB 信号、行同步信号和场同步信号均由时钟脉冲信号调制得到,可将它们看作脉冲幅度调制(PAM)信号。假设视频信号的一帧尺寸为 $\lambda_1 \times \lambda_2$, 则视频信号中各信号分量频率如式(1)所示。

$$f_p = \lambda_1 f_w = \lambda_1 \lambda_2 f_v \quad (1)$$

式中: f_p 为 RGB 信号的频率(简称点频), f_w 为行同步信号的频率(简称行频), f_v 为场同步信号的频率(简称场频)。根据该式可知,行频与点频的比值为单帧图像中每一行像素的个数,场频与行频的比值为每一帧图像中像素的行数。即行、场同步信号不仅决定了屏幕刷新率,还决定了视频图像的尺寸。

1.2 模拟视频信号的时域特性

在模拟视频信号中,RGB 信号除了包含屏幕分辨率尺寸范围的有效视频信息外,还有仅含黑色像素(低电平值)的消隐间隔。行、场同步信号的脉冲均在消隐间隔内,它们之间的关系如图 1 所示。

由图 1 可知,行同步信号的冲激在 RGB 信号中每两行图像之间,场同步信号的冲激在 RGB 信号中每两帧图像之间。显示设备检测到同步信号的冲激时,将换行或是换帧刷新显示图像。

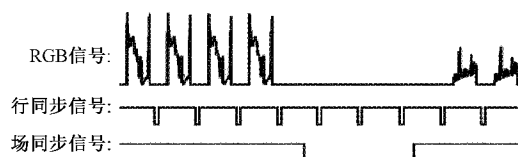


图 1 视频信号各分量的时域关系

1.3 模拟视频信号的呈像

模拟视频信号通过 VGA 线缆传输至恢复设备后,将被转换为串行数字信号,再对应至恢复设备中的每一个像素位置上进行呈像。其呈像规则如图 2 所示。

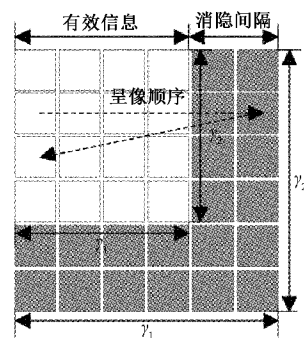


图 2 视频信号呈像规则

模拟视频信号被转为串行数字信号后,将信号中对应的每一个像素点灰度值按照从左往右、从上往下的排列顺序对应至恢复设备的每一个像素点。呈像过程中,像素的换行及换帧均由行同步信号和场同步信号的脉冲决定,因此行频与场频的比值 $\lambda_2 = f_w/f_v$ 及场频与行频的比值 $\lambda_1 = f_p/f_w$ 决定了每一帧视频图像的尺寸^[11]。结合图 1,有效信息和消隐间隔组成了每一帧视频图像。有效信息部分的视频图像将由恢复设备进行呈像,而消隐区间部分的黑色像素将不被呈像。故图像分辨率对应的尺寸为有效信息部分的尺寸 $\gamma_1 \times \gamma_2$, 而非式(1)根据模拟视频信号频率得到的 $\lambda_1 \times \lambda_2$ 。

2 VGA 线缆辐射视频信号的采集及恢复

模拟视频信号电磁泄漏的途径主要分为如下两个部分:显示设备的电磁辐射以及传输通道的电磁辐射,其中传输通道的电磁辐射分为 VGA 线缆的电磁辐射和 VGA 插槽的电磁辐射。但是 LCD 显示组件的电磁泄漏为各行像素的混叠信号,其无法作为良好的辐射泄漏源,故应在传输通道上完成视频信号电磁泄漏的截获。通过高增益天线或是电流卡钳即可在 VGA 传输通道上对模拟视频信号的电磁泄露进行采集,再根据模拟视频信号的呈像规则对采集的信号进行恢复,即可从 VGA 线缆辐射中得到计算机系统的视频图像。

2.1 VGA 线缆辐射视频信号的采集

在视频线缆传输信息时,信号电压的上下跳变会产生电磁辐射,此时使用电磁截获系统对该电磁辐射进行接收

及存储,即可实现对视频信号的采集^[12]。VGA线缆辐射模拟视频信号的截获方式如图3所示。

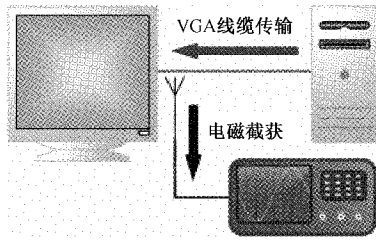


图3 视频信号电磁截获方式

根据电磁场原理,VGA线缆辐射的信号是VGA线缆传输信号的微分^[13]。线缆传输信号与辐射信号的关系如式(2)所示。

$$U = K \frac{dU_0}{dt} \quad (2)$$

式中: U 为电磁泄漏信号, U_0 为线缆传输信号, K 为一环境常量,其值与电路间距及耦合长度有关。由式(2)可知,电磁截获前后模拟视频信号的时序关系如图4所示。

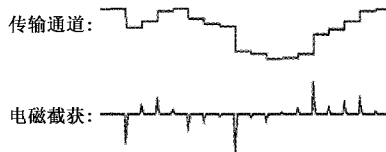


图4 模拟视频信号电磁截获前后的时序关系

2.2 VGA线缆辐射视频信号的恢复

VGA线缆辐射视频信号被截获后,根据模拟视频信号的呈像规则以及模拟视频信号电磁截获前后的时序关系,对截获的信号根据信号频率进行分段,再对分段后的信号进行重抽样,即可得到恢复的视频图像。

模拟视频信号为复合信号,其频率分别由点频 f_p 、行频 f_w 以及场频 f_v 组成,其中最为重要且最易在频谱中获取的频率为行频 f_w 。由图1可知,每相邻的两个行同步脉冲之间的间距均等于RGB信号中传输视频图像中一行像素的信号长度。故以行同步信号的周期 $T_w = 1/f_w$ 对电磁截获视频信号进行分段,即可确保对每一段重抽样的结果与视频图像中每一行像素对应。图5为实际截获的VGA线缆辐射信号的频域部分,对其进行分析即可得到模拟视频信号的行频 f_w 。

如图5所示,对VGA线缆辐射视频信号进行快速傅里叶变换,可在频域中观测到等间距尖峰。周期脉冲信号的频域即是等间距尖峰,且两相邻尖峰的间距即是该周期脉冲的频率。故结合行频 f_w 可能的取值范围,即可确定截获的视频信号的行频。由于外部环境噪声及内部频谱仪噪声的存在,信号频域将存在间距不同的等间隔尖峰^[14]。故在通过频域确定行频 f_w 时,需限定行频 f_w 的取值范围。

确定行频并对电磁截获视频信号分段后,对每一段信号进行重抽样,即可将该段信号对应的视频图像单行像素

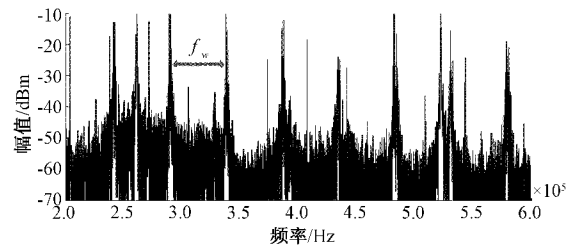


图5 模拟视频信号行频的确定

进行恢复。重抽样示例如图6所示。

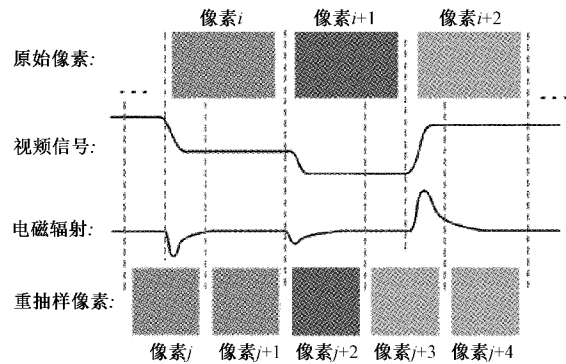


图6 重抽样恢复视频图像的步骤

图6中,由于重抽样频率 f'_p 与视频信号的点频 f_p 不一致,致使恢复的单行图像长度与原本图像尺寸不匹配。设信号采样频率为 f_s ,则第 i 个原始像素与第 j 个重抽样像素对应的采样区间为:

$$S_i = \left[(i-1) \frac{f_s}{f_p}, i \frac{f_s}{f_p} \right] \quad (3)$$

$$S'_j = \left[(j-1) \frac{f_s}{f'_p}, j \frac{f_s}{f'_p} \right] \quad (4)$$

有第 j_0 个重抽样点对应的采样区间为 S'_{j_0} ,其下界、上界分别第 i_1, i_2 个原始像素对应的采样区间 S_{i_1}, S_{i_2} 内,即:

$$\begin{cases} (i_1 - 1) \frac{f_s}{f_p} \leq (j_0 - 1) \frac{f_s}{f'_p} < i_1 \frac{f_s}{f_p} \\ (i_2 - 1) \frac{f_s}{f_p} \leq j_0 \frac{f_s}{f'_p} < i_2 \frac{f_s}{f_p} \end{cases} \quad (5)$$

根据式(5)可知 i_1, i_2 与 j_0 的关系:

$$\begin{cases} i_1 = \left\lceil (j_0 - 1) \frac{f_p}{f'_p} \right\rceil \\ i_2 = \left\lfloor j_0 \frac{f_p}{f'_p} \right\rfloor \end{cases} \quad (6)$$

即第 j_0 个重抽样像素与第 i_1 到第 i_2 个原始像素对应。当 $i_1 = i_2$ 时,第 j_0 个重抽样像素仅与第 i_1 个原始像素对应。因此,重抽样后得到的像素均与1个或多个原始像素对应。故重抽样频率 f'_p 与视频信号的点频 f_p 的不一致不会导致视频信号恢复的失败,只会使恢复图像的尺寸被拉伸或是压缩。

3 低采样率下 VGA 线缆辐射信号的恢复方法

根据奈奎斯特采样定理可知,随着采样率的降低,采样信号与实际信号的差异将不断增大。在模拟视频图像的恢复中,采样率的不断降低则会导致恢复的视频图像失真情况愈发严重。考虑到低采样率下的采样频段问题,故在对采集信息恢复时无法对其进行带通滤波。

由于模拟视频信号的帧数大都在 60 帧以上,故基本可认为连续几帧的视频图像几乎不会存在差异。在恢复时,采集连续数个场频周期时间的模拟视频信号,并将恢复的数帧图像信息进行重叠,即可达到提升图像质量的效果。

3.1 总体恢复流程

图 7 为低采样率下 VGA 线缆辐射信息的恢复流程。将在 VGA 传输通道的传导发射信号通过如下 4 个步骤即可得到质量较高的恢复图像。

- 1) 对电磁截获信号进行频谱分析以获取行频 f_w ;
- 2) 以行频周期 T_w 将电磁截获信号分段并重抽样;
- 3) 将重抽样得到的单行像素以时序关系进行排列得到含多帧信息的完整恢复图像;
- 4) 将完整图像中不同帧重叠,即得到高质恢复图像。

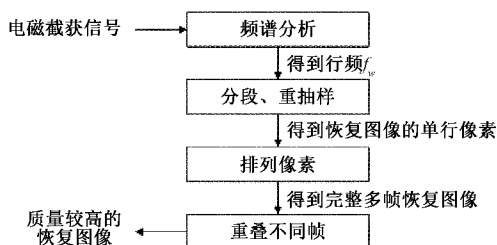


图 7 VGA 线缆辐射信息的恢复流程

在使用电磁截获设备对 VGA 线缆辐射信息进行采集时,使获取的视频信号内包含帧数尽量多的视频图像,即可在多帧重叠时得到恢复质量更好的视频图像。

多帧重叠即是多帧图像的对应像素点进行均值操作。假设采集到的视频信号中含有 m 帧模拟视频图像,则最终恢复的图像的第 i 个像素点的灰度值 Pf_i 与各帧图像的第 i 个像素点灰度值 P_i 的关系如下:

$$Pf_i = \sum_{j=1}^m P_i^j / m \quad (7)$$

当采样频率 f_s 足够低,采样频率与点频的比值 n_f 足够小时,极易出现部分信息未被采样导致丢失图像信息,其在像素灰度值变化频繁的图像中尤为明显。当连续采集多帧视频信号时,采样的多帧视频信号同时丢失同一信号部分的概率远低于单帧视频信号丢失该信号部分的概率。因此,多帧图像重叠后得到的恢复视频图像质量将得到有效提高。

通过数据仿真,得到多帧重叠前后视频图像恢复质量对比结果如图 8 所示。

图 8 为在采样同一视频信号下恢复单帧图像与恢复并

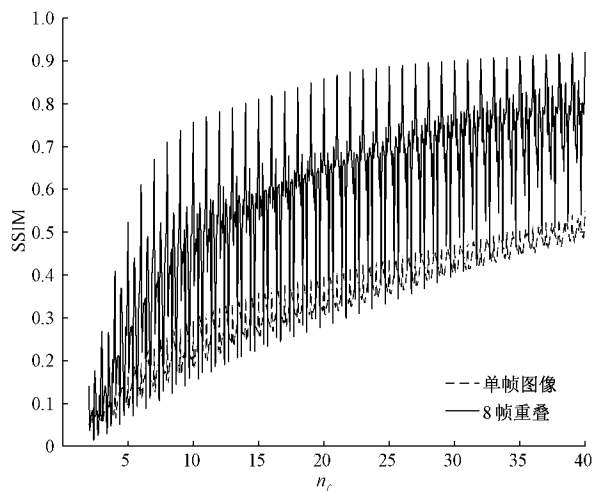


图 8 采样频率与点频的比值 n_f 与恢复图像 SSIM 的关系

重叠 8 帧图像的 n_f - SSIM 关系图。其中 $n_f = f_s / f_p$, 为采样频率与点频的比值;SSIM 为结构相似性,用于评价图像质量。

由图 8 可知,视频图像的恢复质量随着电磁截获采样频率的增加而增加,而经过多帧重叠的图像恢复质量明显高于单帧图像的恢复质量。不考虑噪声干扰,将图 9 通过仿真生成模拟视频信号,再对其进行恢复。取 $n_f = 3.7$ 的恢复结果进行对比,对比结果如图 10 所示。



图 9 用于生成模拟视频信号的图像

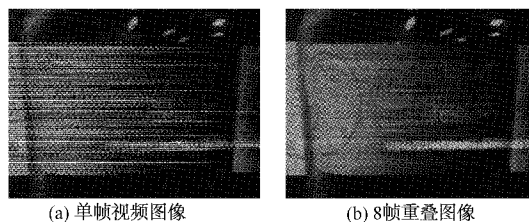


图 10 在相同采样率下对同一视频信号恢复结果的对比

图 10(a) 为恢复的单帧视频图像,图 10(b) 为恢复的 8 帧视频图像的重叠结果。二者对比可知,图 10(b) 中图像信息丢失量较图 10(a) 更少,图像更为清晰完整。

3.2 实际恢复结果验证

为测试以上方法的可用性,于信息产业信息记录及防泄漏产品质量监督检验中心使用电磁截获设备对 VGA 线缆泄露的电磁辐射信号进行截获,并通过以上方式将截获的模拟视频信号进行恢复。图 11 为 VGA 线缆传输的图片,图 12 为 VGA 线缆电磁辐射截获后还原的结果。



图11 VGA线缆传输的图片

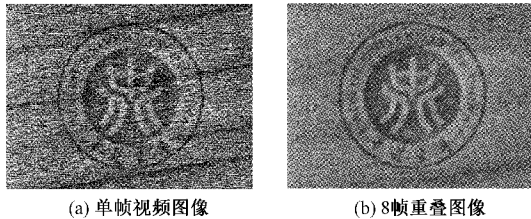


图12 VGA线缆辐射信号还原结果

图11为VGA线缆传输的视频图像,图12(a)为恢复的单帧视频图像,图12(b)为恢复的8帧视频图像重叠结果。将多帧视频图像重叠后,校徽中的文字清晰度大幅提高,并可看见由图像边缘形成的方框。因此可认为视频信号的恢复质量得到了显著提升。

采集的模拟视频信号点频 f_p 、行频 f_w 、场频 f_s 分别为65 MHz、48.36 kHz、60 Hz,采样频率 f_s 为250 MHz,此时 n_f 的值为3.84。

由于采样频率低且存在环境噪声,同时VGA线缆中的视频图像仅含黑白两种颜色。结合图4中采样信号与视频信号的关系,在恢复信息时简化了重抽样的步骤,即在恢复视频图像时仅根据各像素对应信号区间内含冲激的方向将像素值设为0或255。该方式仅适用于颜色构成简单的视频图像,在还原颜色构成复杂的视频图像时会将图像二值化,致使图像信息丢失。

在对仅含黑白两种颜色的图像还原时,除按照以上方式简化重抽样的步骤外,还可在重叠不同帧图像后,使用Otsu算法对图像进行二值化处理以增加恢复图像清晰度,并使用中值滤波将图像中孤立噪声点滤除^[15]。为增加去噪程度,可将中值滤波计算窗口范围内的图像区域置入SVM中,并将中值滤波后的结果结合SVM进行归一化处理,使噪声区域最大程度平滑^[16]。通过图像降噪技术处理恢复结果,可使图像具备更好的可读性。

4 结 论

本文结合模拟视频信号的时频特性以及模拟视频恢复规则,详细介绍了VGA线缆辐射视频信号的恢复步骤。为解决低采样率下视频信号恢复质量差的问题,结合连续帧视频图像差异极小的性质,提出将连续多帧视频图像重叠的方式以提高视频信号恢复质量的方法。经数据仿真可知,该方法显著提升了视频信号的恢复质量,并通过实际

采集的VGA线缆辐射信息的恢复验证了该方法的可行性。

参考文献

- [1] 何庶民. 电场辐射敏感度测试系统的维修方法[J]. 国外电子测量技术, 2019, 38(12): 120-124.
- [2] HAYASHI Y I, HOMMA N, WATANABE T, et al. Introduction to the special section on electromagnetic information security [J]. IEEE Transactions on Electromagnetic Compatibility, 2013, 55(3): 539-546.
- [3] 周源. 基于USRP平台的新型计算机视频信息电磁泄漏截获系统研究[D]. 北京: 北京邮电大学, 2017.
- [4] 苗春卫. 电磁信息安全技术研究现状与发展趋势[J]. 保密科学技术, 2019(2): 5-11.
- [5] SONG T, JEONG Y, YOON J. Modeling of leaked digital video signal and information recovery rate as a function of SNR [J]. IEEE Transactions on Electromagnetic Compatibility, 2015, 57(2): 164-172.
- [6] KUHN M G. Compromising emanations of LCD TV sets [J]. IEEE Transactions on Electromagnetic Compatibility, 2013, 55(3): 564-570.
- [7] KUBIAK I. Influence of the method of colors on levels of electromagnetic emissions from video standards[J]. IEEE Transactions on Electromagnetic Compatibility, 2018: 1-9.
- [8] LEE H S, YOON J G, SIM K. An information recovery technique from radiated electromagnetic fields from display devices [C]. Asia-pacific International Symposium on Electromagnetic Compatibility, IEEE, 2016: 473-475.
- [9] 张南. 计算机电磁信息泄漏与视频信息认知研究[D]. 北京: 北京邮电大学, 2019.
- [10] LEE H S, YOON J G, SIM K. Measurement and analysis of the electromagnetic emanations from video display interface [C]. 2015 IEEE Electrical Design of Advanced Packaging and Systems Symposium, IEEE, 2015.
- [11] 何雯, 董威, 苟辉. 基于FPGA的高速视频采集系统的设计[J]. 国外电子测量技术, 2016, 35(5): 83-87.
- [12] 王森, 邱扬, 田锦, 等. 数字接口视频传输线的电磁泄漏特性[J]. 西安电子科技大学学报, 2017, 44(5): 81-86.
- [13] 钱志升. 基于电源线传导的LCD电磁信息泄漏分析与重建[D]. 郑州: 战略支援部队信息工程大学, 2018.
- [14] 陈映竹. 电磁泄漏测试系统的设计与实现[D]. 成都: 电子科技大学, 2018.
- [15] 徐艳云, 郭佳, 李怡伟, 等. 信息设备电磁泄漏还原图像的文本识别研究[J]. 信息安全研究, 2016, 2(2): 137-142.
- [16] 净亮, 邵党国, 相艳, 等. 基于支持向量机的自适应均值

滤波超声图像降噪[J]. 电子测量与仪器学报, 2020, 34(3):1-8.

作者简介

杨旺霖, 硕士研究生, 主要研究方向为信号处理技术与图像处理技术等。

E-mail: 1814198426@qq.com

苏新彦, 博士, 副教授, 主要研究方向为目标信息获取和处理技术与电磁兼容等。

E-mail: 869921695@qq.com

姚金杰, 博士, 副教授, 主要研究方向为毫米波测试技术与北斗导航定位技术应用等。

E-mail: 1910382988@qq.com