Computer Science and Application 计算机科学与应用, 2024, 14(4), 24-32
Published Online April 2024 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2024.144073

Hans汉斯

基于改进型随机振动的电磁泄漏信号检测算法

叶　彬[1,2]

[1]中国科学院大学网安学院，北京
[2]中国科学信息工程研究所，北京

收稿日期：2023年3月3日；录用日期：2024年4月2日；发布日期：2024年4月9日

摘　要

针对当前电子设备电磁泄漏安全检测中，微弱泄漏信号频点易被漏检等问题。本文提出了一种新型随机振动电磁泄漏检测算法，该算法利用随机振动原理，通过迁移原始信号中的噪声信号能量到泄漏信号上，达到增强泄漏信号强度，降低噪声强度，解决泄漏频谱的漏检问题。该算法通过移频，新型遗传算法及分段双稳态等方法，对传统随机振动算法进行优化，克服传统双稳态随机算法中存在的不足。本文通过实验和仿真证明了该方法的在电磁泄漏检测中的有效性。

关键词

电磁泄漏，随机振动，弱信号检测

Electromagnetic Leakage Signal Detection Algorithm Based On Improved Random Vibration

Bin Ye[1,2]

[1]School of Cyber Security, University of Chinese Academy of Sciences, Beijing
[2]Institute of Information Engineering, Chinese Academy of Sciences, Beijing

Received: Mar. 3rd, 2023; accepted: Apr. 2nd, 2024; published: Apr. 9th, 2024

Abstract

In view of the current electronic equipment electromagnetic leakage safety detection, the weak leakage signal frequency point is easy to be detected and so on. In this paper, a new electromagnetic leakage detection algorithm based on random vibration is proposed. The algorithm uses the principle of random vibration to transfer the energy of noise signal from the original signal to the leakage signal, so as to enhance the leakage signal strength and reduce the noise strength, solve

文章引用: 叶彬. 基于改进型随机振动的电磁泄漏信号检测算法[J]. 计算机科学与应用, 2024, 14(4): 24-32.
DOI: 10.12677/csa.2024.144073

the problem of leak detection of leakage spectrum. This algorithm optimizes the traditional random vibration algorithm by frequency shift, new genetic algorithm and subsection bistable method, and overcomes the shortcomings of the traditional bistable random vibration algorithm. The effectiveness of this method in electromagnetic leakage detection is proved by experiment and simulation.

Keywords

Electromagnetic Leakage, Random Vibration, Weak Signal Detection

1. 简介

随着信息化时代的进步，越来越多的电子设备广泛应用于人类社会的各个领域，在给人类社会带来便利的同时，也带来了巨大的安全隐患。其中这些电子设备产生的无意电磁信号的泄漏，可通过相关信号检测设备，收集，解码复原出设备中运行的文件内容信息，该方法又称为 tempest，各国针对 tempest 制定出相关的电磁泄漏标准[1]。

电磁泄漏的检查研究可追溯到十九世纪八十年代，英国军方的 Nile 和 Suakin 最早注意到了通话的线路旁边的线路也可以获取对应电信号的 TEMPEST 现象[2]。

十九世纪五十年代中期，美国颁布了 TEMPEST 标准：NAG-1A，这是人类历史上第一个关于电磁泄漏的标准。来到六十年代，美国又陆续颁布了关于 tempest 的 FS222 与 FS222A 标准。在同一时期，工商界开始进入该领域，生产出基于物理屏蔽特性的各种屏蔽设备[3]。七十年代，美国又推出 tempest 新的标准 NACSIM5100。同时美国工业届联合政府推出“工业 TEMPEST 规划”，对工业界的电磁泄漏防范产品给出相应标准。从此之后，电磁泄漏防护技术逐渐朝着专业化、标准化和市场化发展。八十年代，美国国家安全局又发布新的电磁泄漏防护标准 NACSIM5200 标准，与此同时，西欧各国对电磁泄漏进行研究，北约推出了 AMSG720 实验室标准，欧洲国家也使用该标准来规范自己国家的电子通信设备。九十年代，美国针对电磁泄漏标准提出 3 级等级制度[4] [5] [6]。同时代，英国剑桥大学的 Markus G. Kuhn 和 Ross J Anderson 提出了电磁泄漏防护软体(Soft-TEMPEST)的概念，他们利用电磁泄漏这一有原理实现信息的攻击窃取信息。

我国电磁泄漏技术研究的发展，起步相对国外较晚。北京邮电大学，长春光机所在 2004 年各自搭建计算机电磁泄漏信号的仿真平台，可实现视频图片的复原[7]。2008 年至今，北京邮电大学，西安电子科技大学和中国科学院信息工程研究所在 TEMPEST 方面做出了深入的研究，并陆续在图形复原，文字复原，音视频复原方面取得一定成果，并培养一批相关人才[8]。

目前针电子设备电磁泄漏信号检测方法，是把采集到的信号通过：时域分析法，频域分析法，时频分析法，混沌振子法，随机共振法，差分振子法等信号处理方法进行信号处理，找出泄漏设备的泄漏特征如周期，振幅，频率，熵等信号特征，以此来判断设备是否存在电磁泄漏。

然而在上述检测方法中存在原始信号中噪声信号强，某些频点电磁泄漏信号弱，同时有强噪声干扰使得信噪比极低。该泄漏频点在信号去噪过程中易被去除，从而造成泄漏频点的漏检。为解决上述弱信号频点漏检问题，关键是提高系统的输出信噪比，将微弱的有用信息从复杂的强电磁噪声中提取出来。随机共振天然具有的将噪声能量转化为信号能量的优势，这为检测微弱的电磁泄漏信号提供新的途径[9]。

现采用的传统随机共振算法是双稳态系统随机共振，但该方法受绝热逼近理论的限制，只能使用低频信号，不适合高频信号；还存在输出饱和，限制对弱信号的增强和系统的抗干扰能力；以及算法最优参数不易获取等问题，本文首先采用移频算法，把高频信号转移到低频信号，再用改进后的 k-遗传算法优化随机振子，使信号增强。

2. 基于改进型随机振动的电磁检测算法

本文采用的方法首先采用移频法，使原始信号中的高频信号转变为低频信号，使其满足随机振动算法使用条件，再通过 k-遗传算法[10]与分段随机算法[11]，自适应地使信号、噪声和系统达到最佳匹配程度，最大程度削弱信号中的噪声，提高目标信号的能量。具体流程图如下图 1 所示。

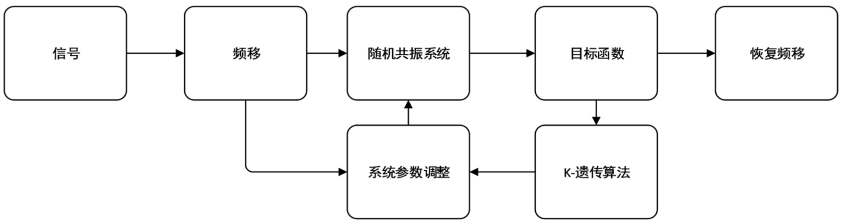

Figure 1. Flow chart of k-genetic vibration algorithm
图 1. k-遗传振动算法流程图

针对传统遗传算法在大规模寻优时容易陷入局部最优，本文通过加入种群择优算子加大了遗传算法的寻优力度；改进的选择算子在选择出优秀个体的同时，也保证了父代规模；提供运行速度的同时避免出现局部最优[12]。

本算法采用分段双稳态系统替代经典随机振动中使用的双稳态系统，解决了传统随机振动中过饱和，对弱信号的增强限制和系统的抗干扰能力弱等问题。

算法的流程如下图 2 所示，综合 k-遗传算法与双稳态随机共振实现参数联合优化的具体步骤如下。

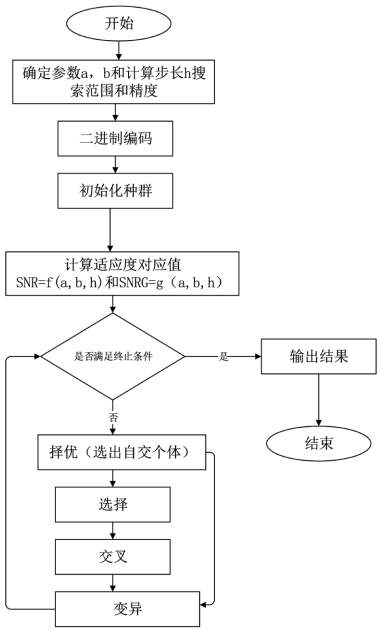

Figure 2. K-genetic algorithm and random vibration algorithm optimize flow chart
图 2. k-遗传算法与随机振动算法优化流程图

步骤 1：个体编码。设置 k-遗传算法参数 a、b 和双稳态系统中龙格库塔法的步长参数 h 和搜索精度 δ，设置各参数的取值范围为 $a\in[A_{\min}, A_{\max}]$，$b\in[B_{\min}, B_{\max}]$，$h\in[H_{\min}, H_{\max}]$，根据 k-遗传算法的二进制编码方式，确定 a、b 和 h 对应的编码长度 l、k 和 j：

$$\begin{cases} 2^l-1=\left(A_{\max}-A_{\min}\right)/\delta \\ 2^k-1=\left(B_{\max}-B_{\min}\right)/\delta \\ 2^j-1=\left(H_{\max}-H_{\min}\right)/\delta \end{cases} \tag{2-1}$$

步骤 2：参数初始化。针对遗传种群规模大小，种群包含个体数目，设置选择、交叉和变异的概率，迭代的最大次数以及满足最小误差标准等参数进行初始化处理；

步骤 3：个体解码。对群体中的个体进行解码，由步骤 2 可知 k-遗传算法参数 a、b 和龙格库塔法的计算步长 h 的编码方案，根据遗传算法的解码公式得到其对应的系统参数为：

$$\begin{cases} a=A_{\min}+\left(\sum_{i=1}^{l}c_i2^i-1\right)\dfrac{A_{\max}-A_{\min}}{2^l-1} \\ b=B_{\min}+\left(\sum_{j=1}^{k}d_j2^j-1\right)\dfrac{B_{\max}-B_{\min}}{2^k-1} \\ h=H_{\min}+\left(\sum_{g=1}^{j}e_g2^j-1\right)\dfrac{H_{\max}-H_{\min}}{2^j-1} \end{cases} \tag{2-2}$$

步骤 4：适应度估计。通过把个体对应参数带入双稳态随机共振系统，计算输出信噪比和信噪比增益，即 $SNR(a, b, h)$，$SNRG(a, b, h)$。

步骤 5：通过选择、交叉和变异等算子对当前 t 代群体中个体之间进行运算，得到新的群体第 t + 1 代。

步骤 6：若运算达到设置的最大迭代次数，则中止循环。否则重复步骤 3 至步骤 5。

综上所述，本算法利用遗传算法中的交叉、选择和变异等算子自适应调整遗传算法参数 a、b 和双稳态系统里的龙格库塔法的计算步长 h 参数，使输出信噪比最大，使微弱信号增强，提高了微弱信号的检测能力。

仿真实验

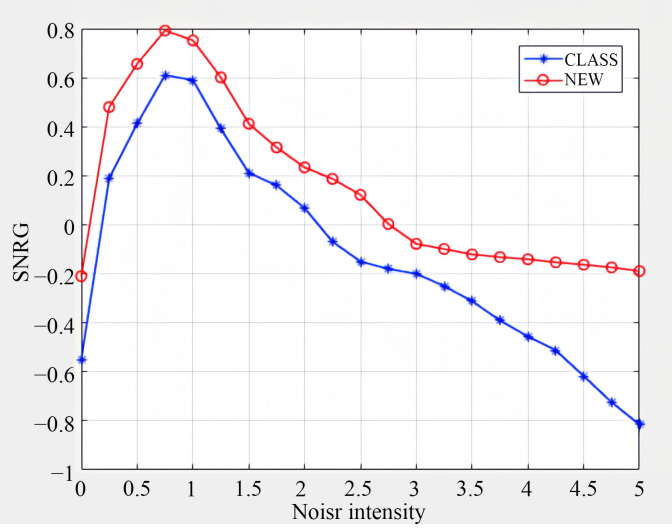

Figure 3. SNR performance comparison
图 3. SNR 性能比较

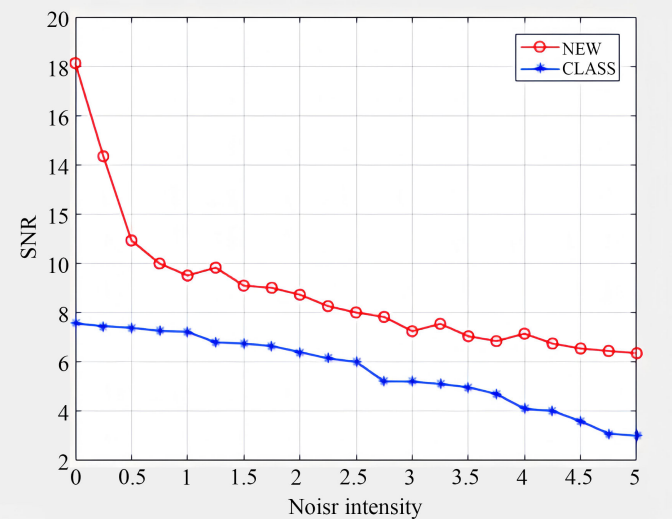

Figure 4. SNRG performance comparison
图 4. SNRG 性能比较

为验证算法性能，本文特别采用在相同噪声强度下，改进型随机振动算法与传统随机振动算法，在信噪比(*SNR*)和信噪比增益(*SNRG*)性能来做仿真比较。该仿真中，设置改进随机振动算法参数 *a*、*b* 取[1~5]，*h* 取值[0~1]，择优概率为 0.15，选择，交叉，变异概率为 0.2，最大迭代次数为 100，个体数量为 50；设置传统遗传算法的 *a*、*b* 取 1，其他参数不变。

通过上图(图 3、图 4)仿真结果可知，改进后的算法相对旧的算法，信噪比得到 2~6 db 范围内的提升，信噪比增益也有所提升，证明了改进型算法的有效性。

3. 检测电磁辐射

3.1. 基于 VGA 线泄漏信号的实验

图 5 是显示器 VGA 线上的电磁信息泄漏频谱，频段 8 MHz~16 MHz。显示器的参数为：分辨率 1280 × 1024，刷新率 60 HZ，采样频率为 1.25 GHZ。通过随机共振增强，通过随机共振方法强化，发现信号强度得到增强。通过随机共振增强，发现了 8 MHz~10 MHz 频段存在等间隔的谐波峰值，如图 6 所示。此案例中的非线性系统参数为 $a = 7.5 \times 10^{-4}$，$b = 6.25 \times 10^{-4}$，$h = 0.1$。根据 SNR 计算公式说明信号增强 6.782 dB。图 7 是 14 MHz~16 MHz 频段的增强结果，通过随机共振方法强化，能够对频域中的信号增强 5.671 dB。

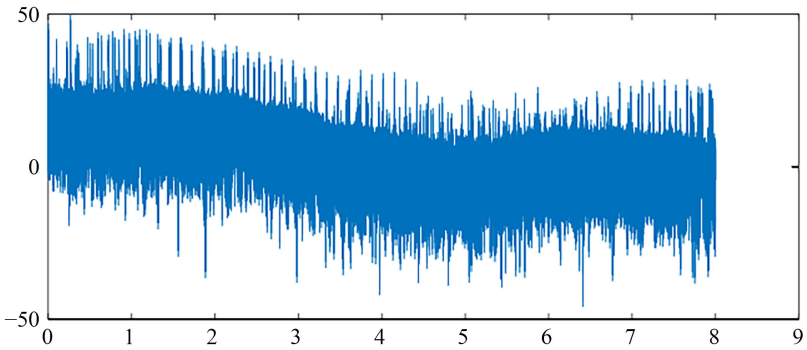

Figure 5. Electromagnetic information leakage spectrum of measured display data line (8 MHz~16 MHz)
图 5. 实测显示器数据线电磁信息泄漏频谱(8 MHz~16 MHz)

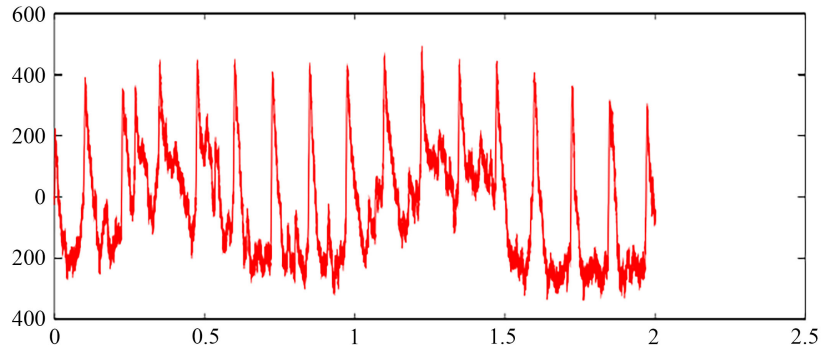

Figure 6. Random resonance enhancement results of data line leakage spectrum (8 MHz~10 MHz)
图 6. 数据线泄漏频谱的随机共振增强结果(8 MHz~10 MHz)

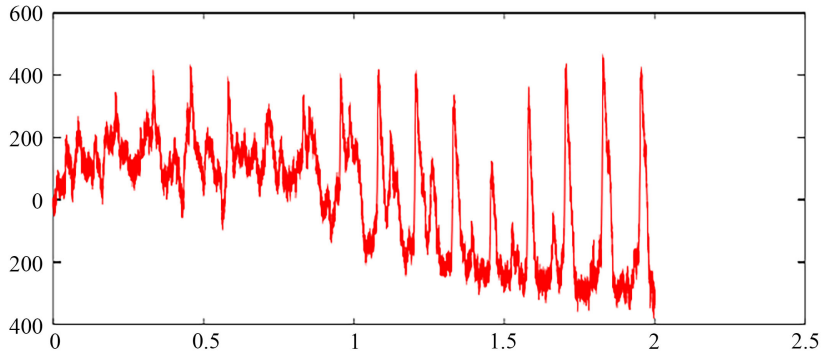

Figure 7. Random resonance enhancement results of data line leakage spectrum (14 MHz~16 MHz)
图 7. 数据线泄漏频谱的随机共振增强结果(14 MHz~16 MHz)

3.2. 基于电源线电磁泄漏信号的实验

显示器的电源线上同样存在显示器的电磁信息泄漏。虽然，电源模块加了滤波，电源线线上还增加了磁环，但这些措施依然无法将电磁信息泄漏彻底屏蔽。图 8 是在计算机显示器电源线上测得的电磁辐射频谱，显示器分辨率为 1280 × 768，刷新频率 60 Hz，通过卡钳和电磁数据采集卡获取，所显示的频段 15 MHz~20 MHz。图 9 和图 10 是随机共振信号增强的结果。等间隔泄漏频点非常明显，间距约为 124.4 kHz。图 3~5 中信号增强了 6.312 dB。图 3~6 中信号增强了 5.652 dB。此处，参数 $a = 7.5\times 10^{-4}$，$b = 6.25\times 10^{-4}$，$h = 0.1$。

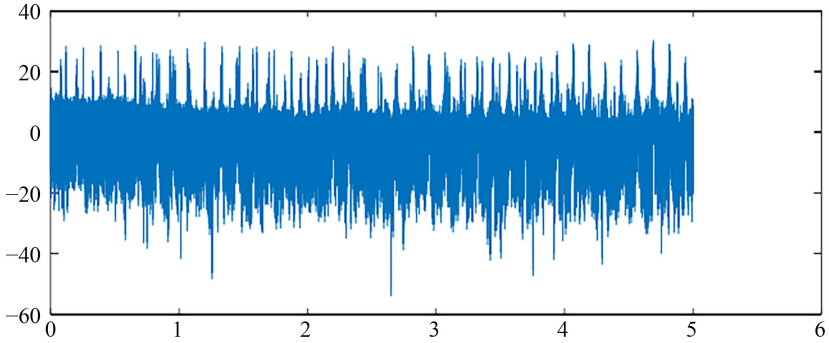

Figure 8. Measured electromagnetic information leakage spectrum of monitor power line (15 MHz~20 MHz)
图 8. 实测显示器电源线电磁信息泄漏频谱(15 MHz~20 MHz)

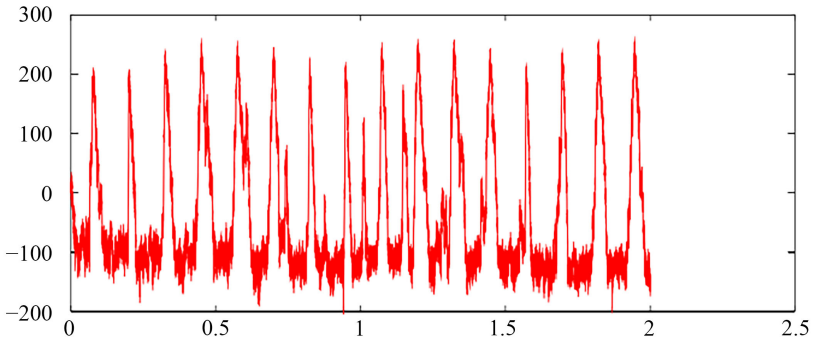

Figure 9. Random resonance enhancement results of power line leakage spectrum (16 MHz~18 MHz)
图 9. 电源线泄漏频谱的随机共振增强结果(16 MHz~18 MHz)

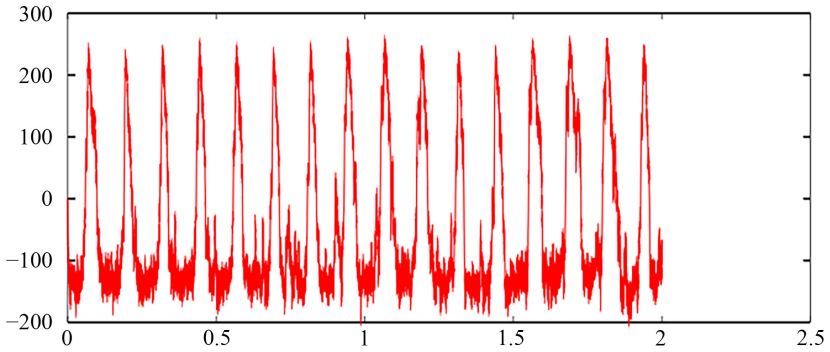

Figure 10. Random resonance enhancement results of power line leakage spectrum (18 MHz~20 MHz)
图 10. 电源线泄漏频谱的随机共振增强结果(18 MHz~20 MHz)

3.3. 基于显示器泄漏图像信号的实验

图 11 是对数天线实测到计算机显示器电磁泄漏的时域波形，显示器分辨率为 1920 × 1280，刷新率 60 hz，采样率为 250 MHz。由于是各种信号和噪声混叠在一起，无法清楚识别出是否存在泄漏信号。经过 N-遗传随机共振处理之后提取出的信号如图 12 所示，信号的周期为 15.884 us，对应于显示器行频。经过随机共振强化后，信号增益 SNRI = 5.6113，即信号增强了 17.2478 dB。此处，非线性系统的结构参数为 $a = 6.66667 \times 10^{-4}$，$b = 4.38957 \times 10^{-7}$。

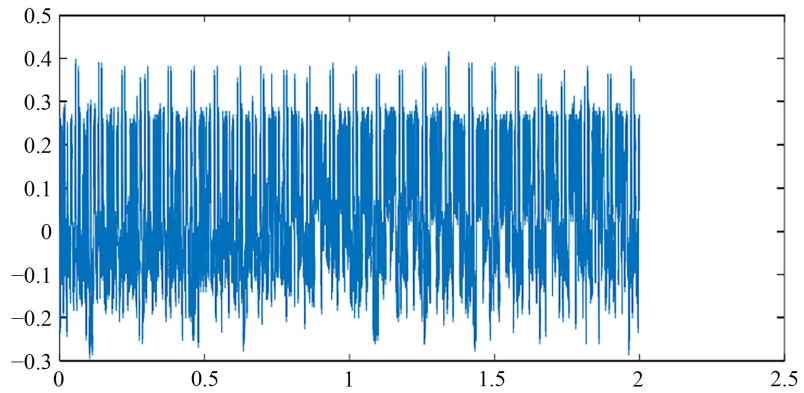

Figure 11. Time domain waveform
图 11. 电磁泄漏的时域波形

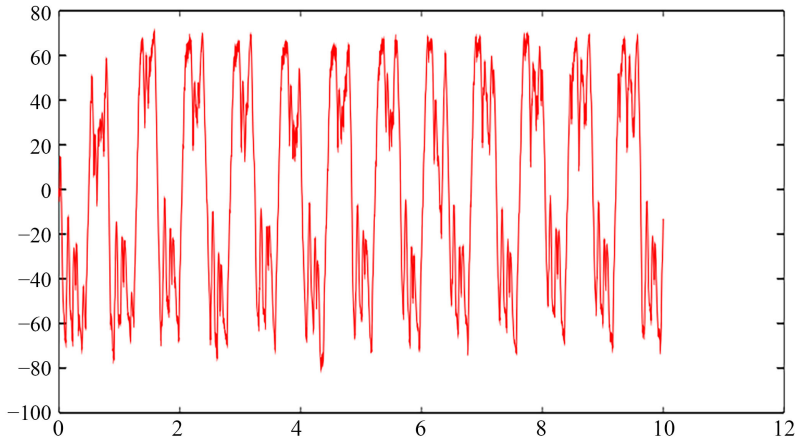

Figure 12. Remove the leak signal of electromagnetic leakage
图 12. 取出的泄漏信号

Figure 13. Directly demodulated out
图 13. 直接解调出的泄漏图形

Figure 14. The new algorithm demodulated of the leak pattern the leak pattern
图 14. 使用新算法后解调出泄漏图形

图 13 为泄漏信号直接解调恢复出图像，图 14 为使用改进算法解调后恢复出的图像，通过对比，我

们可以看出新算法对电磁泄漏信号恢复有一定的改善。

4. 结论

本文提出了新型改进型随机共振算法，该算法利用移频法，遗传算法和随机振动算法相结合，有效的提高了计算机设备电磁泄漏信号检测的准确率，解决了传统电磁泄漏检测中弱信号频点漏检问题。经仿真和实验证明，该算法可有效降低噪声信号强度，增强信号的强度，提高了电磁信号的信噪比，可有效提高电磁信息泄漏的检测精度。

参考文献

[1] Van Eck, W. (1985) Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? *Computers & Security*, **4**, 269-286. https://doi.org/10.1016/0167-4048(85)90046-X

[2] Kuhn, M.G. (1998) Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations. *Proceeding 2nd International Workshop on Information Hiding*, Portland, 14-17 April 1998, 124-142. https://doi.org/10.1007/3-540-49380-8_10

[3] Hesseldahl, A. (2013) You Won't Believe All the Crazy Hardware the NSA Uses for Spying. All Things Digital. http://allthingsd.com/20131230/you-wont-believe-all-the-crazy-hardware-the-nsa-uses-for-spying/

[4] Oren, Y. and Shamir, A. (2007) Remote Password Extraction from RFID Tags. *IEEE Transactions on Computers*, **56**, 1292-1296. https://doi.org/10.1109/TC.2007.1050

[5] 王丹琛. 建设国家电磁空间安全体系维护电磁空间安全国家利益——陈鲸院士谈电磁空间安全[J]. 中国信息安全, 2020(12): 24-28.

[6] U.S. Department of Defense (2020) Electromagnetic Spectrum Superiority Strategy Released. https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/ELECTROMAGNETIC_SPECTRUM_SUPERIORITY_STRATEGY.PDF

[7] 崔天舒. 面向天基电磁信号识别的深度学习方法[D]: [博士学位论文]. 北京: 中国科学院大学, 2021.

[8] Liang, L.L., Li, Z., Wang, D.Y., *et al*. (2016) Comparison Results of Stochastic Resonance Effects Realized by Coherent and Non-Coherent Receiver. 2016 *International Conference on Computer, Information and Telecommunication Systems* (*CITS*), Kunming, 6-8 July 2016, 1-5. https://doi.org/10.1109/CITS.2016.7546427

[9] Lai, Z.H., Liu, J.S., Zhang, H.T., Zhang, C.L., Zhang, J.W. and Duan, D.Z. (2019) Multi-Parameter-Adjusting Stochastic Resonance in a Standard Tri-Stable System and Its Application in Incipient Fault Diagnosis. *Nonlinear Dynamics*, **96**, 2069-2085. https://doi.org/10.1007/s11071-019-04906-w

[10] Ma, Q., Huang, D. and Yang, J. (2018) Adaptive Stochastic Resonance in Second-Order System with General Scale Transformation for Weak Feature Extraction and Its Application in Bearing Fault Diagnosis. *Fluctuation and Noise Letters*, **17**, Article No. 1850009. https://doi.org/10.1142/S0219477518500098

[11] Li, Z. and Shi, B. (2017) An Adaptive Stochastic Resonance Method for Weak Fault Characteristic Extraction in Planetary Gearbox. *Journal of Vibroengineering*, **19**, 1782-1792. https://doi.org/10.21595/jve.2016.17652

[12] Zhang, G. and Gao, J.P. (2018) Weak Signal Detection Based on Combination of Power and Exponential Function Model in Tri-Stable Stochastic Resonance. *Journal of Computational and Applied Mathematics*, **38**, 2747-2752.