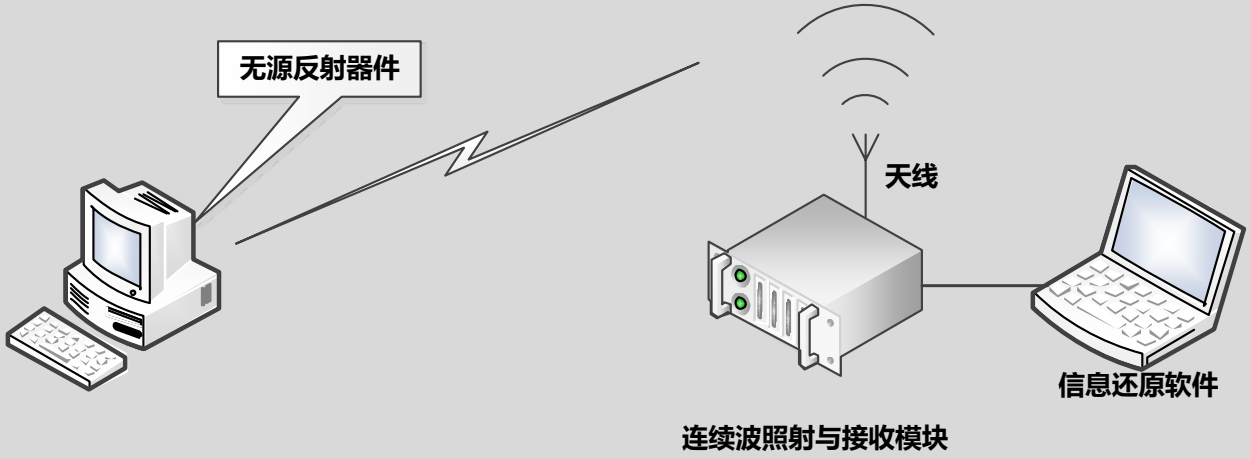
安全应用实例-无线信息获取技术

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

目录

1基于连续波照射的视频线信息获取——功能与组成



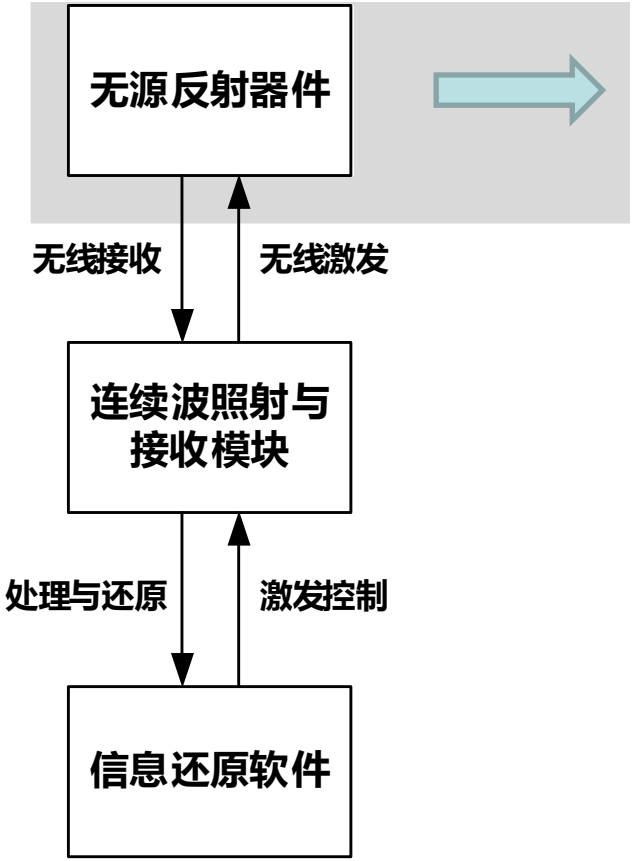
功能：

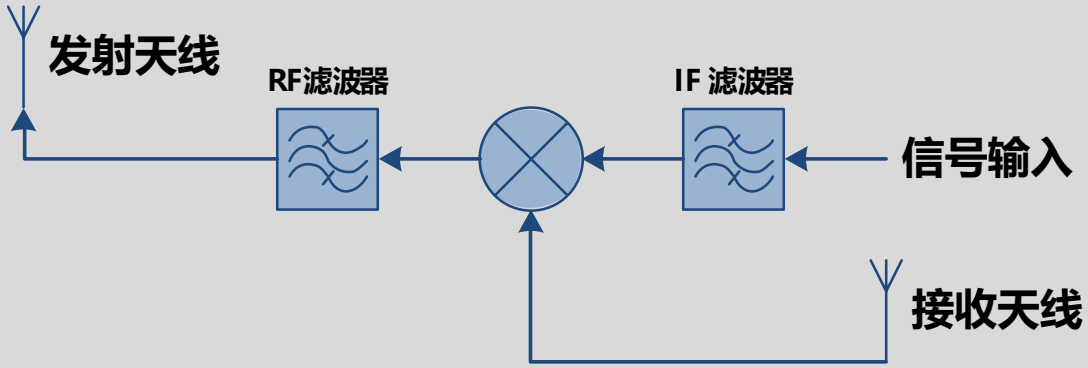
通过预先植入到计算机视频线缆的硬件获取计算机信息

组成：

- 无源反射器件：截取和无线发射视频线信号
- 连续波照射与接收模块：激发无源反射器件和接收视频线信号
- 信息还原软件：信号处理和信息还原

1基于连续波照射的视频线信息获取——工作原理

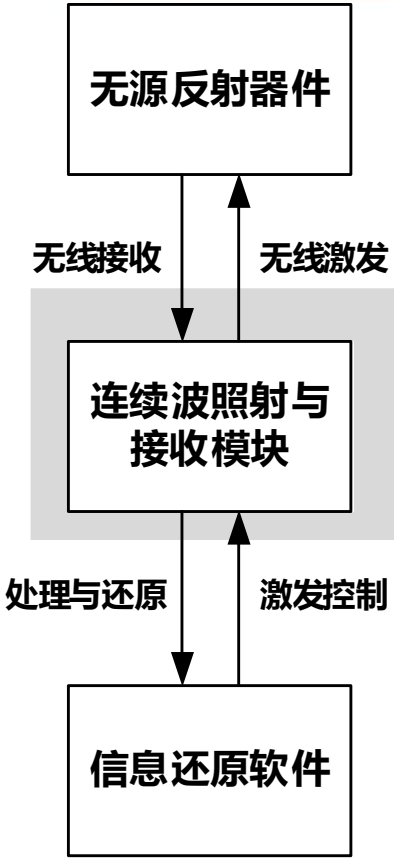


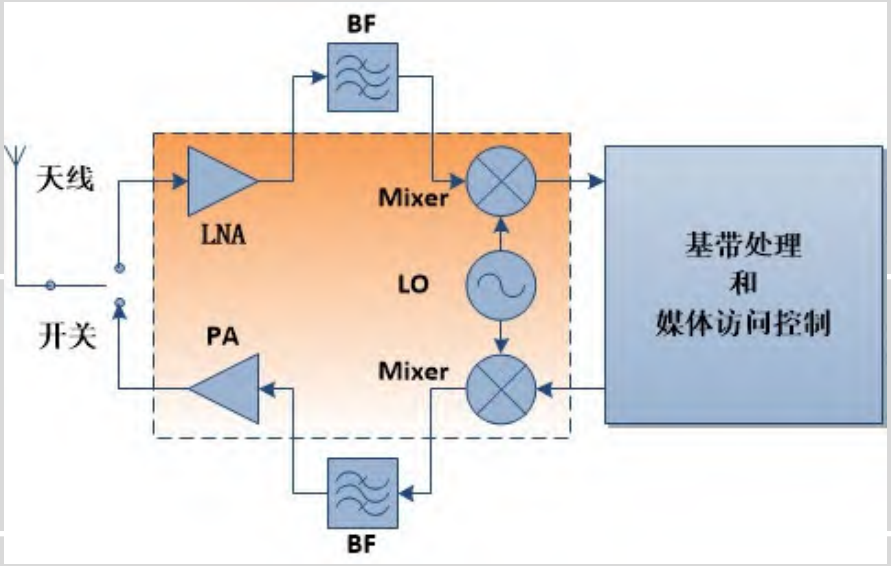


—种简化的射频发射结构

- 结构简单，可隐藏在视频线缆里
- 平时处于静默状态，无线激发后开始工作

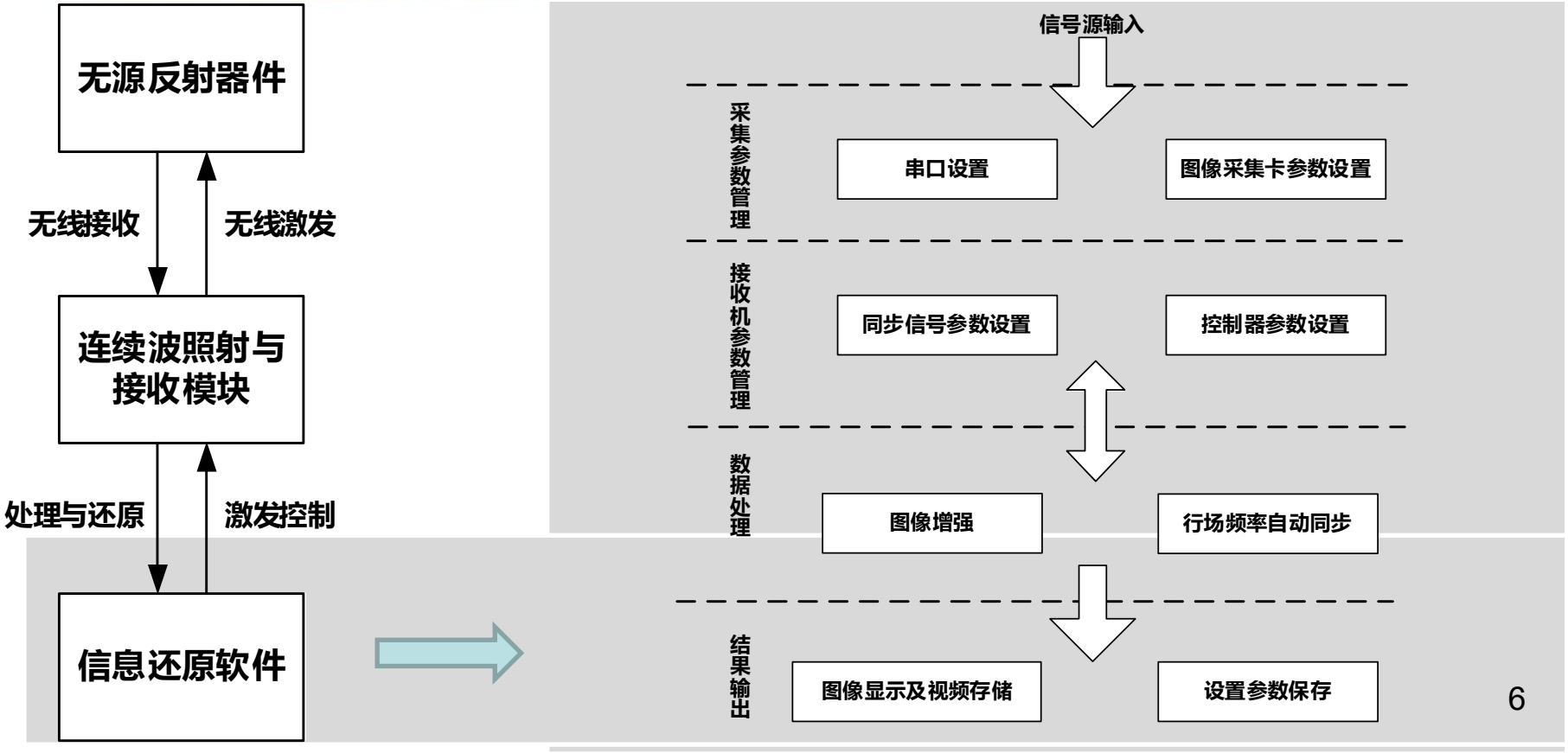
1基于连续波照射的视频线信息获取——工作原理



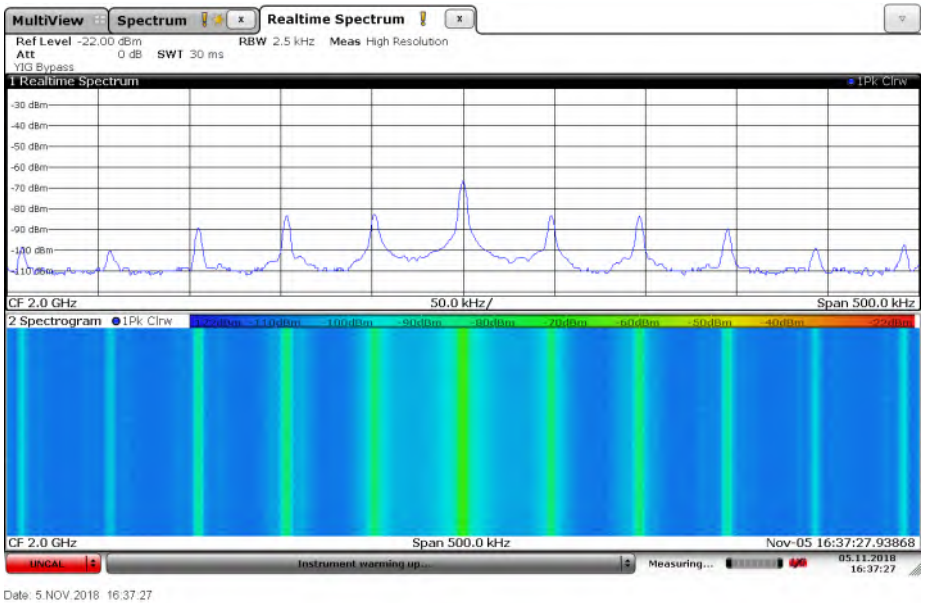


- 该模块主要包括天线、射频发射芯片、射频接收芯片、基带处理芯片等

1基于连续波照射的视频线信息获取——工作原理



1基于连续波照射的视频线信息获取——频谱瀑布图



调制方式：AM调制

中心频率：2GHz

1基于连续波照射的视频线信息获取——参考文献

TOP SECRET//COMINT//REL TO USA, FVEY

RAGEMASTER

ANT Product Data

(TS//SI//REL TO USA,FVEY) RF retro-reflector that provides an enhanced radar cross-section for VAGRANT collection. It's concealed in a standard computer video graphics array (VGA) cable between the video card and video monitor. It's typically installed in the ferrite on the video cable.

24 Jul 2008

(U) Capabilities

(TS//SI//REL TO USA,FVEY) RAGEMASTER provides a target for RF flooding and allows for easier collection of the VAGRANT video signal. The current RAGEMASTER unit taps the red video line on the VGA cable. It was found that, empirically, this provides the best video return and cleanest readout of the monitor contents.

(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The RAGEMASTER taps the red video line between the video card within the desktop unit and the computer monitor, typically an LCD. When the RAGEMASTER is illuminated by a radar unit, the illuminating signal is modulated with the red video information. This information is re-radiated, where it is picked up at the radar, demodulated, and passed onto the processing unit, such as a LFS-2 and an external monitor, NIGHTWATCH, GOTHAM, or (in the future) VIEWPLATE. The processor recreates the horizontal and vertical sync of the targeted monitor, thus allowing TAO personnel to see what is displayed on the targeted monitor.

Unit Cost: $ 30

Status: Operational. Manufactured on an as-needed basis. Contact POC for availability information.

POC: [redacted], S32243, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY

CTX4000

ANT Product Data

(TS//SI//REL TO USA,FVEY) The CTX4000 is a portable continuous wave (CW) radar unit. It can be used to illuminate a target system to recover different off net information. Primary uses include VAGRANT and DROPMIRE collection.

8 Jul 2008

(TS//SI//REL TO USA,FVEY) The CTX4000 provides the means to collect signals that otherwise would not be collectable, or would be extremely difficult to collect and process. It provides the following features:

- Frequency Range: 1 - 2 GHz.
- Bandwidth: Up to 45 MHz
- Output Power: User adjustable up to 2 W using the internal amplifier; external amplifiers make it possible to go up to 1 kW.
- Phase adjustment with front panel knob
- User-selectable high- and low-pass filters.
- Remote controllable
- Outputs:
- Transmit antenna
- I & Q video outputs
- DC bias for an external pre-amp on the Receive input connector
- Inputs:
  - External oscillator
  - Receive antenna

Unit Cost: N/A

Status: unit is operational. However, it is reaching the end of its service life. It is scheduled to be replaced by PHOTOANGLO starting in September 2008.

POC: [redacted], S32243, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

参考文献：斯诺登曝光文档

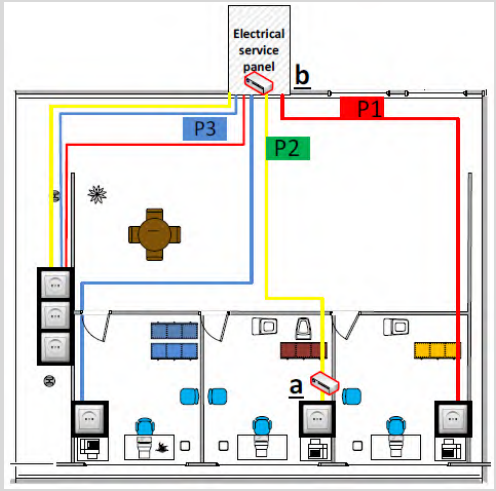
关键指标：

- 工作距离（15m）
- 工作速率（实时传输）

应用场景：

- 处于物理隔离的计算机

2基于电力线的信息获取——功能与步骤



功能：

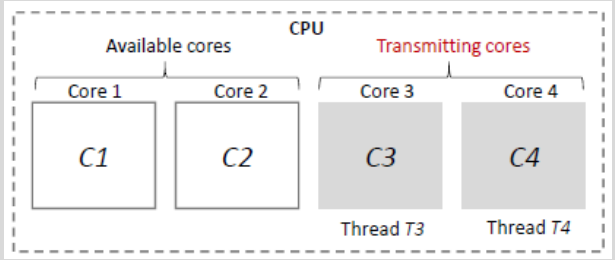
通过预先植入到计算机的软件获取计算机信息并通过电力线传输该信息

步骤：

- 系统感染
- 接收器植入
- 数据收集
- 数据泄漏

2基于电力线的信息获取——工作原理

- 信号生成
  - 控制CPU是否满载

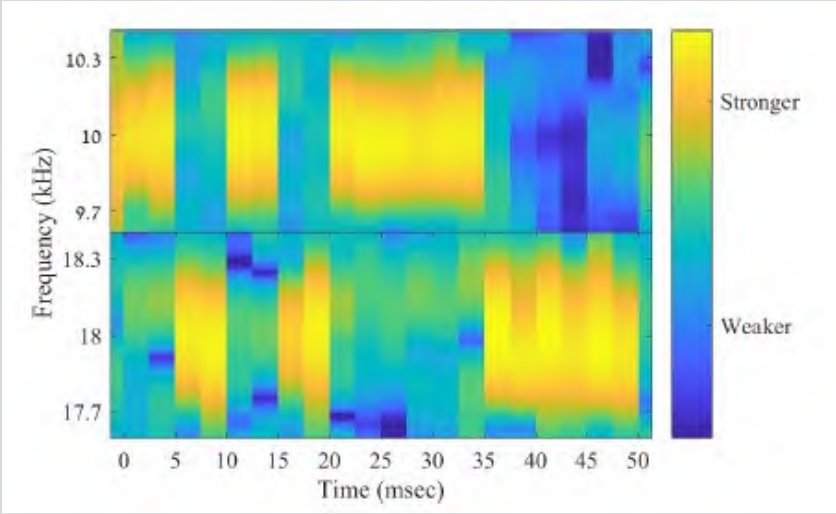


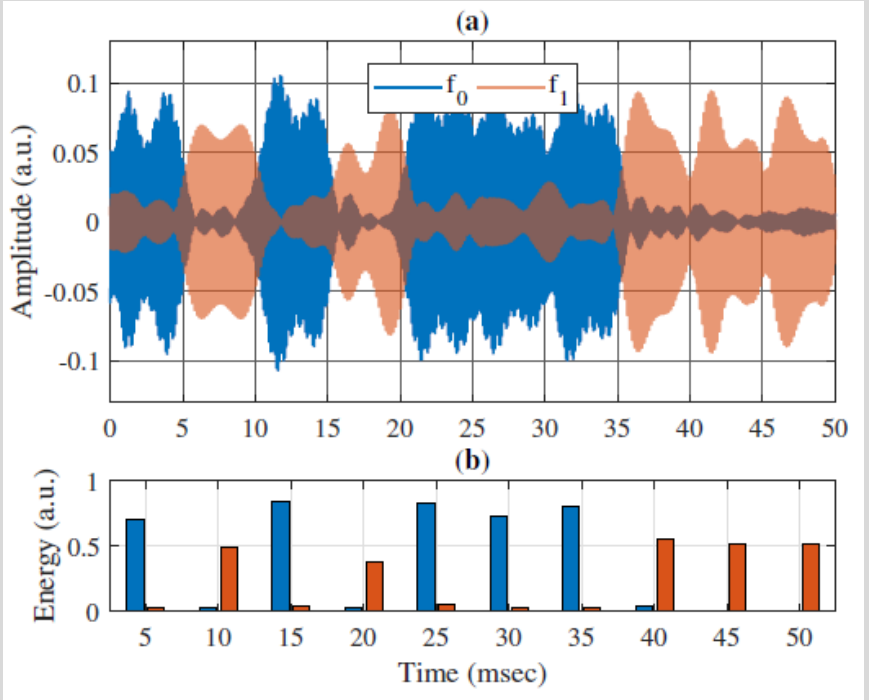
Algorithm 1 WorkerThread ($iCore$, $freq$, $nCycles0$, $nCycles1$)

```
1: bindThreadToCore(iCore)
2: half_cycle_ms ← 0.5 * 1000/freq
3: while (!endTransmission()) do
4:     if (data[i] = 0) then
5:         sleep(nCycles0*half_cycle_ms*2)
6:     else
7:         for j ← 0 to nCycles1 do
8:             T1 ← getCurrentTime()
9:             while (getCurrentTime() − T1 < half_cycle_ms) do ;
10:            end while
11:            sleep(half_cycle_ms)
12:        end for
13:    end if
14: end while
```

2基于电力线的信息获取——工作原理

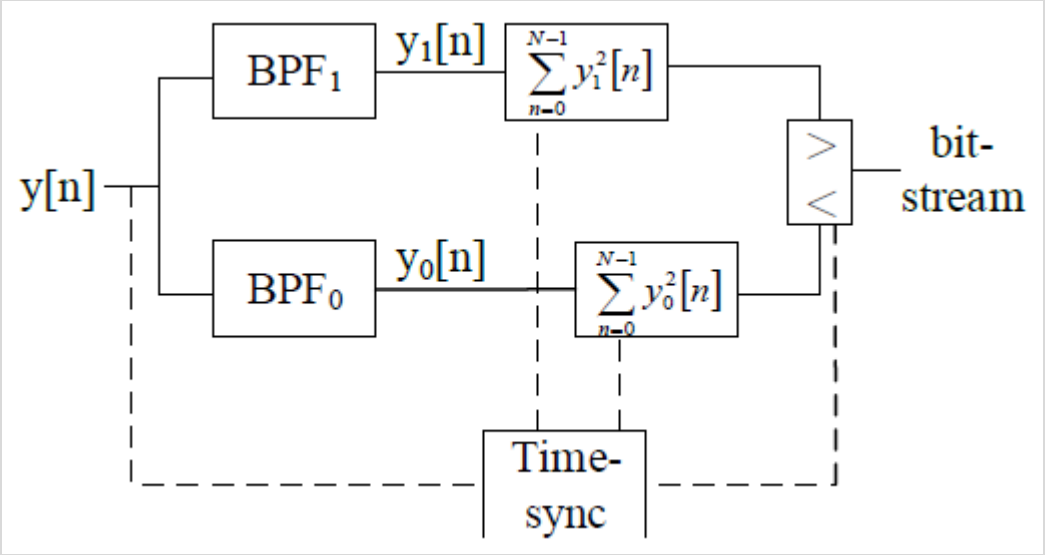
- 调制
  - BFSK





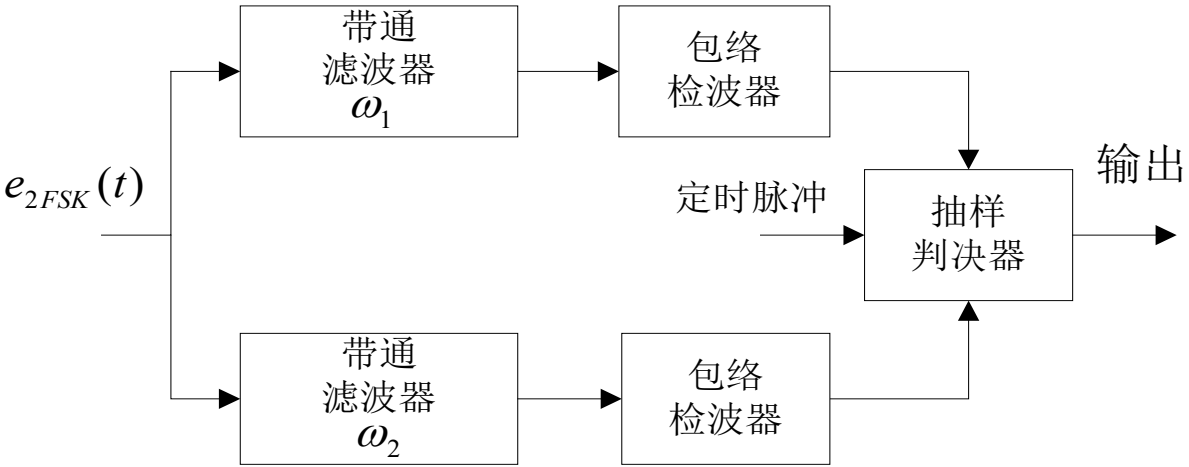
2基于电力线的信息获取——工作原理

- 接收端架构



第7章 数字带通传输系统

- 2FSK信号的解调方法★（复习）
  - 非相干解调



2基于电力线的信息获取——参考文献

PowerHammer: Exfiltrating Data from Air-Gapped Computers through Power Lines

Mordechai Guri, Boris Zadov, Dima Bykhovsky, Yuval Elovici‡
Ben-Gurion University of the Negev, Israel
Cyber-Security Research Center
‡Department of Software and Information Systems Engineering
Email: gurim@post.bgu.ac.il, borisza@gmail.com, bykhov@post.bgu.ac.il, elovici@bgu.ac.il

应用场景：

- 处于物理隔离的计算机

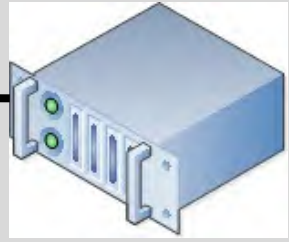
性能参数：比特率和误码率

#	bit rate (bit error rate)
PC	333 bit/sec (0%) 500 bit/sec (0%) 1000 bit/sec (0%)
Server	100 bit/sec (0%) 200 bit/sec (0.96%) 333 bit/sec (4.8%) 500 bit/sec (26%)
IoT	5 bit/sec (1.9%) 10 bit/sec (4.8%) 20 bit/sec (18.2%)

3电磁木马——功能与组成

植入电磁木马后

电磁波



网络隔离的目标计算机

信息还原模块

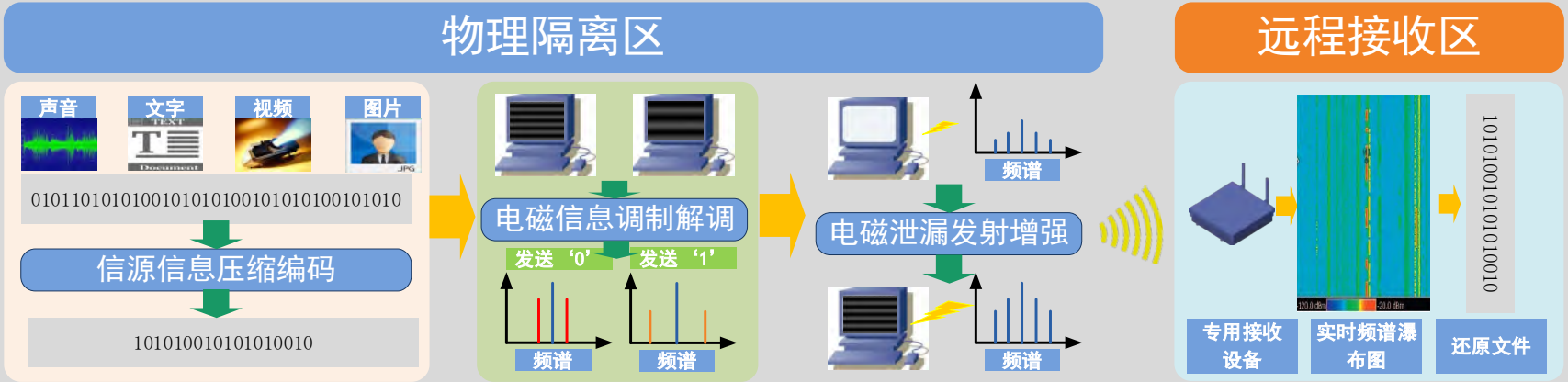
功能：

通过预先植入到计算机的软件获取计算机信息并通过视频接口传输该信息

组成：

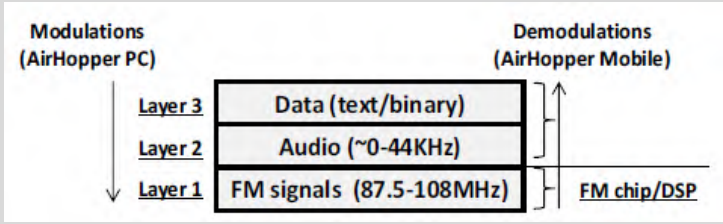
- **电磁木马：获取计算机数据，利用视频接口无线发射该数据**
- **信息还原模块：信号接收和信息还原**

3电磁木马——工作原理


物理隔离区
远程接收区
声音
文字
视频
图片
0101101010100101010100101010100101010
信源信息压缩编码
101010010101010010
电磁信息调制解调
发送 ‘0’
发送 ‘1’
频谱
频谱
电磁泄漏发射增强
频谱
频谱
专用接收设备
实时频谱瀑布图
还原文件
101010010101010010

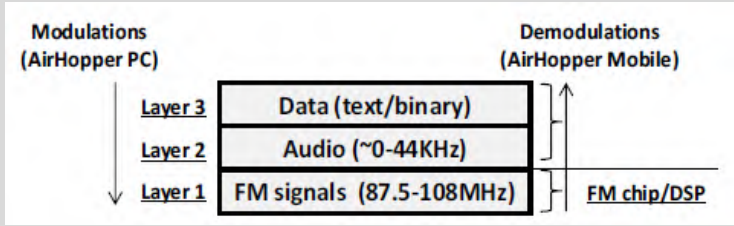
3电磁木马——工作原理

- 数据调制
  - A-FSK：受干扰小、距离远
  - DTMF：传输速率快
    - 双音多频，由高频群和低频群组成，高低频群各包含4个频率。一个高频信号和一个低频信号叠加组成一个组合信号，代表一个数字。DTMF信号有16个编码



3电磁木马——工作原理

- FM声音信号生成
  - 通过显卡：
    http://bk.gnarf.org/creativity/vgasig/vgasig.pdf

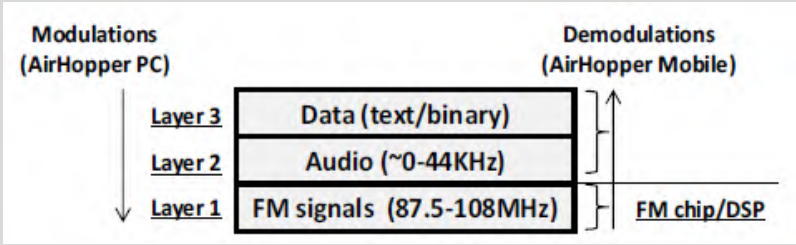


$$(Y_1 - Y_0)\frac{(H_{pixel} + H_{sync})}{P_c} \approx \frac{1}{F_d}$$

```
01 k ← 2 * Fd / PC , t ← 0
02 all pixels ← BLACK
03   For i ← 0 to Vp
04     IF floor(t*k)is odd
05       For j ← 0 to Hp
06         IF floor(t*k) is odd
07           pixel[j][i] ← WHITE
08         t←t+1
09     Else
10       t←t+Hp
```

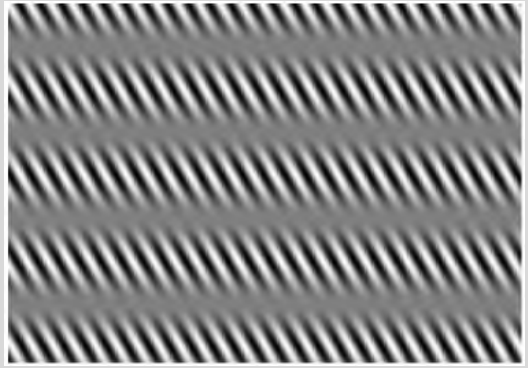
3电磁木马——工作原理

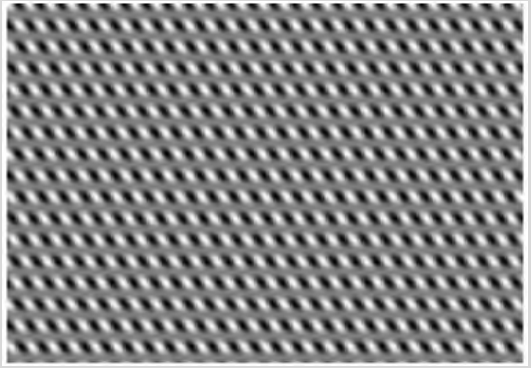
- 数据解调
  - FM音频输出重定向
  - 音频采样
  - 信号处理



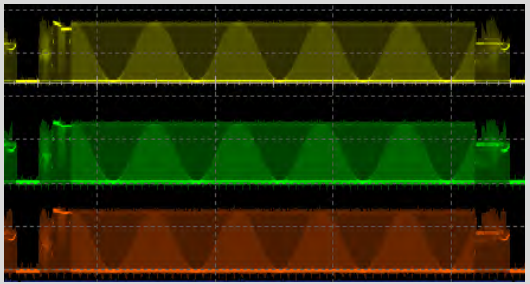
3电磁木马——测试数据

计算机屏显

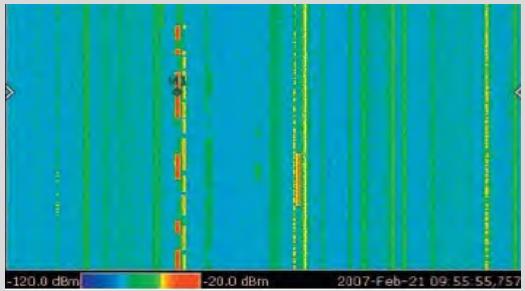




视频信号时域波形



视频信号频谱瀑布图



3电磁木马——参考文献

AirHopper: Bridging the Air-Gap between Isolated Networks and Mobile Phones using Radio Frequencies

Mordechai Guri[1], Gabi Kedma[1], Assaf Kachlon[1], Yuval Elovici[1,2]
[1]*Department of Information Systems Engineering, Ben-Gurion University*
[2]*Telekom Innovation Laboratories at Ben-Gurion University*
{gurim, gabik, assafka}@post.bgu.ac.il, elovici@bgu.ac.il

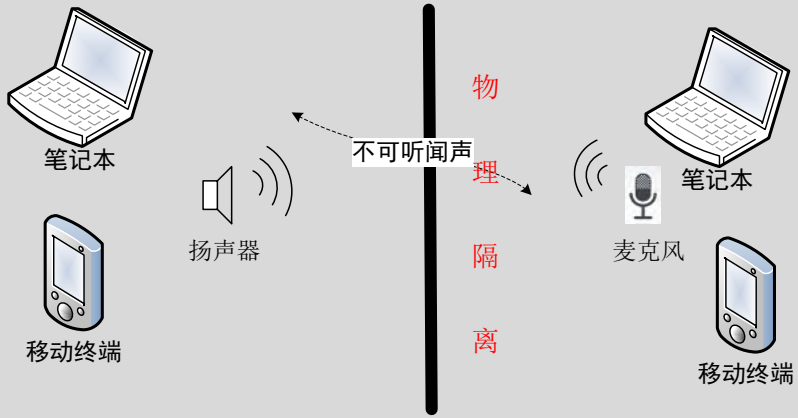
应用场景：

- 处于物理隔离的计算机

性能参数：

- 工作距离（7m）
- 工作速率（104-480bit/s）

4基于超声波的信息获取——功能与组成



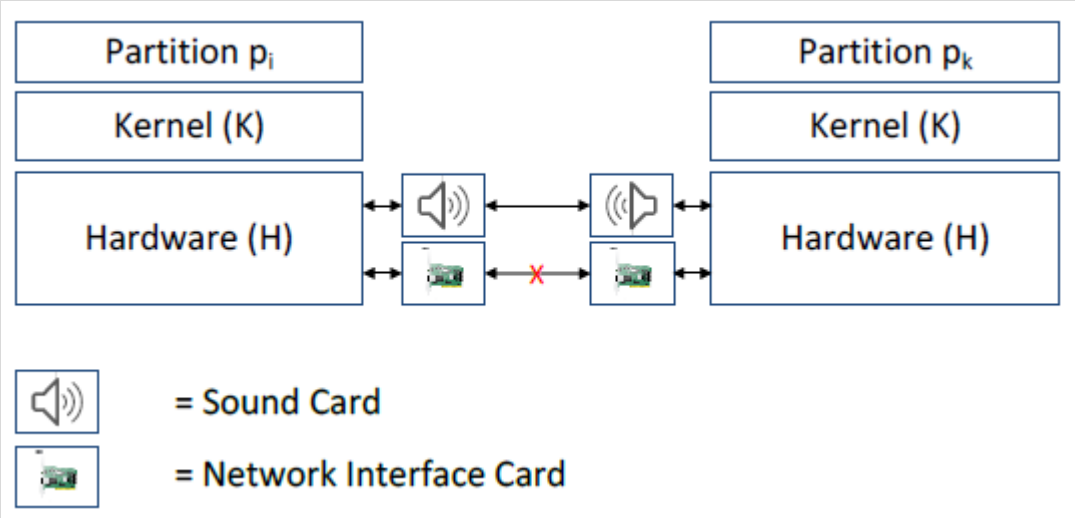
功能：

通过预先植入到计算机的软件获取计算机信息并通过人耳不可听闻声传输该信息

组成：

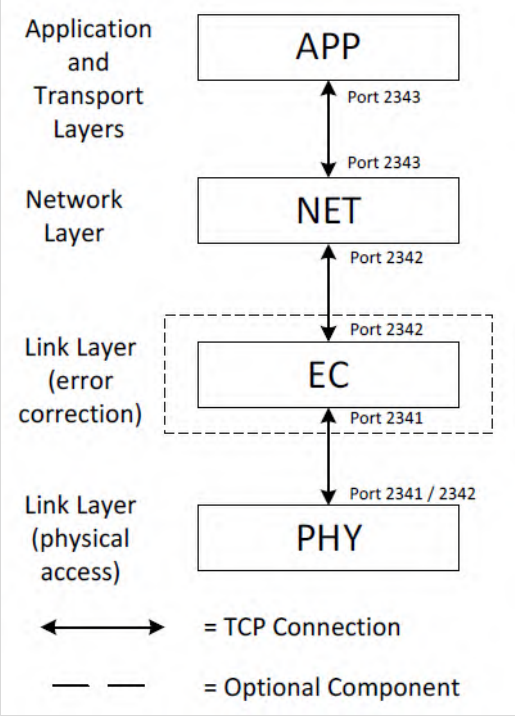
- **声木马：获取计算机数据，利用扬声器发射该数据**
- **信息还原模块：信号接收和信息还原（带有麦克风的手机或计算机）**

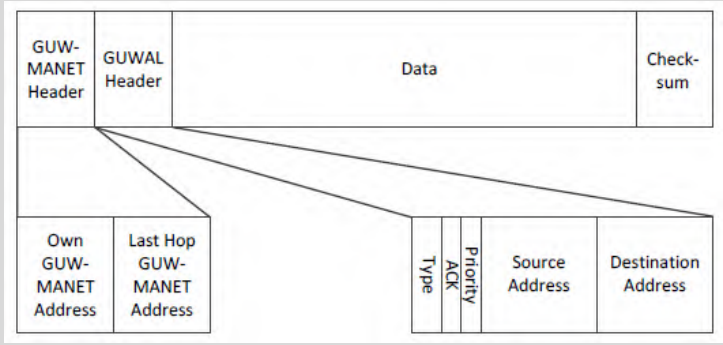
4基于超声波的信息获取——工作原理



4基于超声波的信息获取——工作原理

- 通信系统架构





4基于超声波的信息获取——参考文献

Journal of Communications Vol. 8, No. 11, November 2013

On Covert Acoustical Mesh Networks in Air

Michael Hanspach and Michael Goetz
Fraunhofer FKIE, Wachtberg, Germany
Email: {michael.hanspach, michael.goetz}@fkie.fraunhofer.de

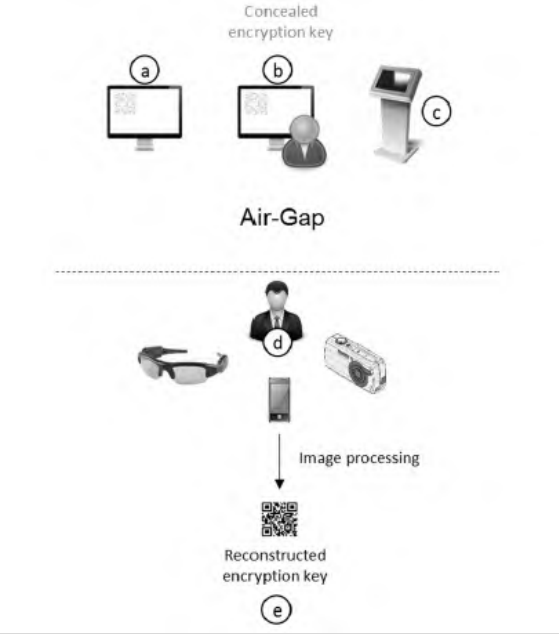
应用场景：

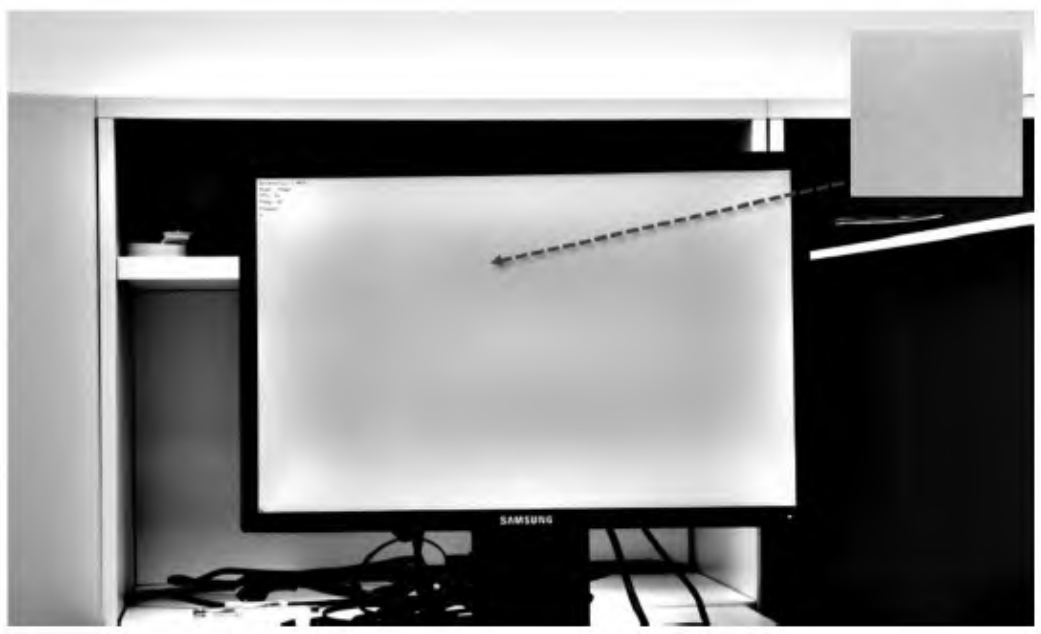
- 处于物理隔离的计算机

性能参数：

- 工作距离（19.7m）
- 工作速率（20bit/s）

5基于光隐藏的信息获取——功能与组成





功能：

通过预先植入到计算机的软件获取计算机信息并通过光传输该信息

组成：

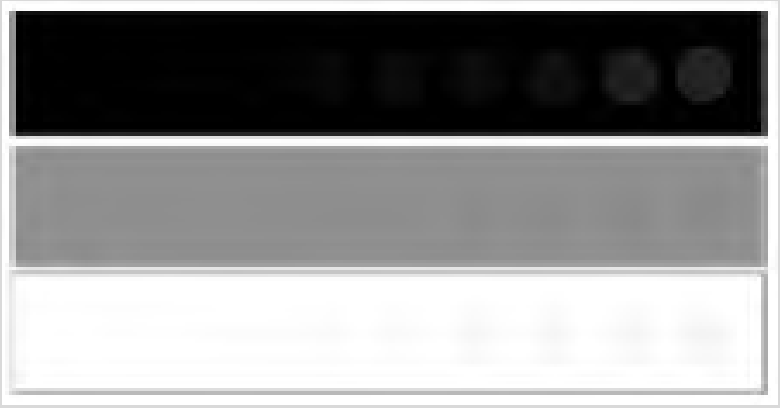
- **光木马：获取计算机数据，利用显示器发射该数据**
- **信息还原模块：信号接收和信息还原**

5基于光隐藏的信息获取——工作原理

- QR code
  - 将信息生成二维码

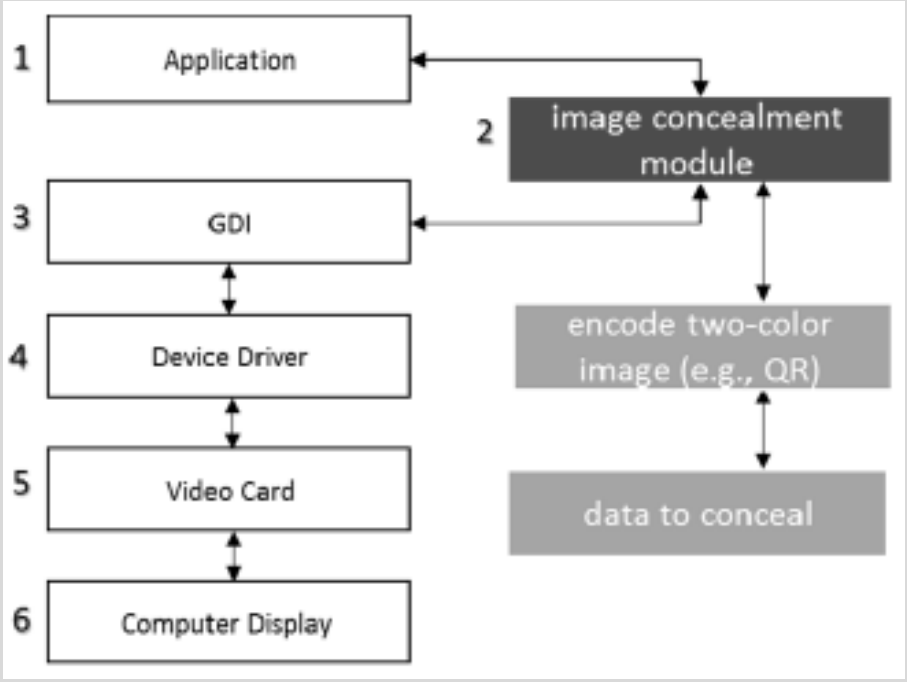
5基于光隐藏的信息获取——工作原理

- 图像隐藏
  - 嵌入式：颜色对比度调试
  - 闪烁式：高频闪烁



5基于光隐藏的信息获取——工作原理

- 隐藏流程



5基于光隐藏的信息获取——工作原理

- 图像重组流程
  - 图像去饱和度：去除背景噪声
  - 动态范围扩展：增强对比度
  - 图像锐化：还原图像

5基于光隐藏的信息获取——参考文献

VisiSploit: **An Optical Covert-Channel to Leak Data through an Air-Gap**

Mordechai Guri, Ofer Hasson, Gabi Kedma, Yuval Elovici
Ben-Gurion University of the Negev
{gurim, hassonofer, gabik, elovici}@post.bgu.ac.il

应用场景：

- 处于物理隔离的计算机

性能参数：

- 工作距离（8m）

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

谢谢！