Electromagnetic eavesdropping on computers

Markus Kuhn

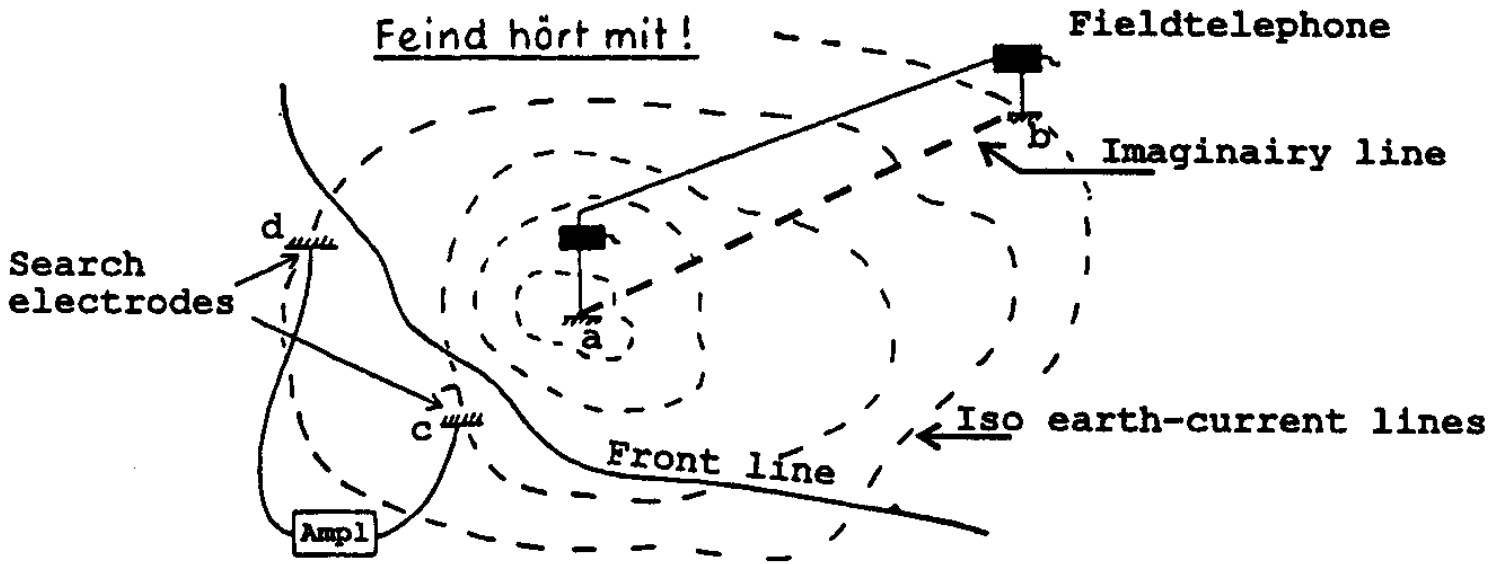
2002-06-12

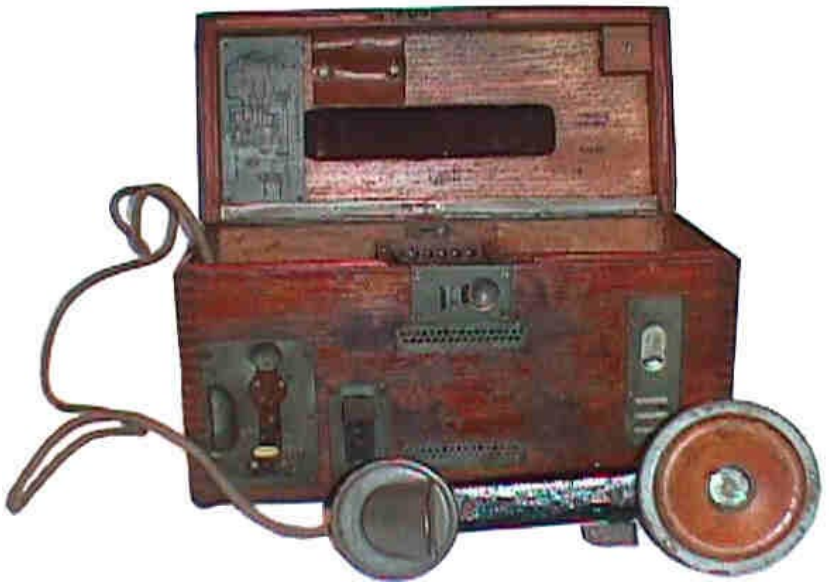
UNIVERSITY OF CAMBRIDGE

Computer Laboratory

http://www.cl.cam.ac.uk/~mgk25/

Early use of compromising emanations



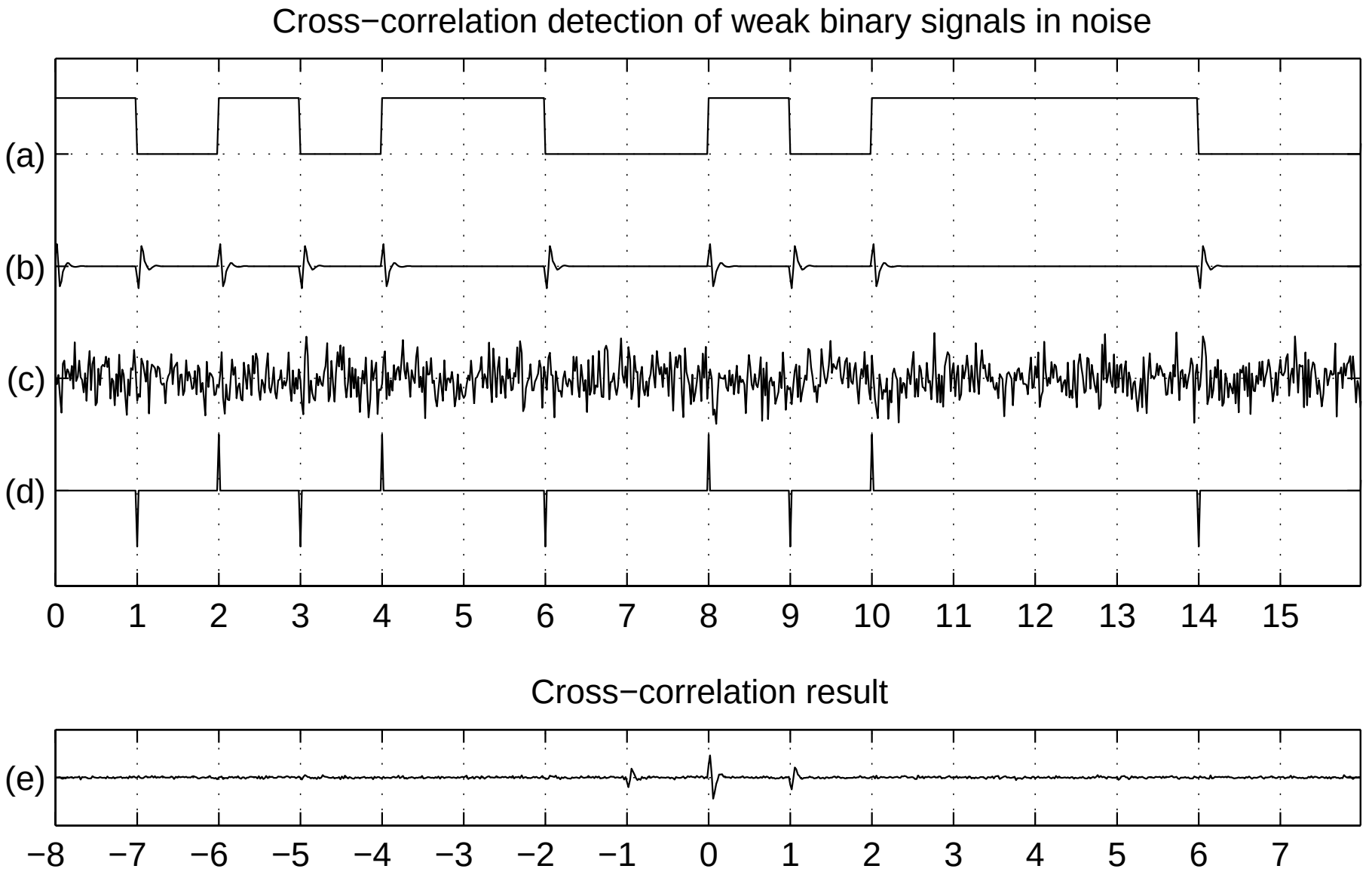


The German army started in 1914 to use valve amplifiers for listening into ground return signals of distant British, French and Russian field telephones across front lines.

Military History of Side-Channel Attacks

- → 1915: WW1 ground-return current tapping of field telephones.
- → 1960: MI5/GCHQ find high-frequency plaintext crosstalk on encrypted telex cable of French embassy in London.
- → Since 1960s: Secret US government "TEMPEST" programme investigates electromagnetic eavesdropping on computer and communications equipment and defines "Compromising Emanations Laboratory Test Standards" (NACSIM 5100A, AMSG 720B, etc. still classified today).
- → Military and diplomatic computer and communication facilities in NATO countries are today protected by
  - "red/black separation"
  - shielding of devices, rooms, or entire buildings.

  US market for "TEMPEST" certified equipment in 1990: over one billion dollars annually.



$$b(t) = (r * h)(t) + n(t) = \int_0^\infty r(t - t')\, h(t)\, dt + n(t)$$

Video Timing

The electron beam position on a raster-scan CRT is predictable:

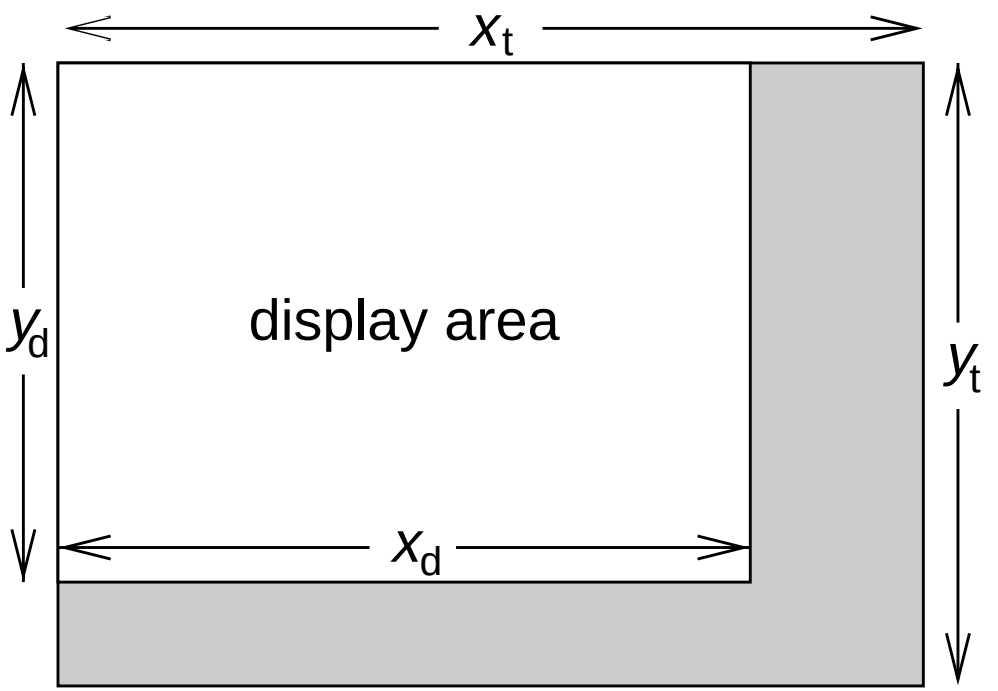
Pixel frequency: f_p

Deflection frequencies:

$$f_\mathrm{h} = \frac{f_\mathrm{p}}{x_\mathrm{t}}, \qquad f_\mathrm{v} = \frac{f_\mathrm{p}}{x_\mathrm{t} \cdot y_\mathrm{t}}$$

Pixel refresh time:

$$t = \frac{x}{f_\mathrm{p}} + \frac{y}{f_\mathrm{h}} + \frac{n}{f_\mathrm{v}}$$



The 43 VESA standard modes specify f_p with a tolerance of $\pm 0.5\%$.

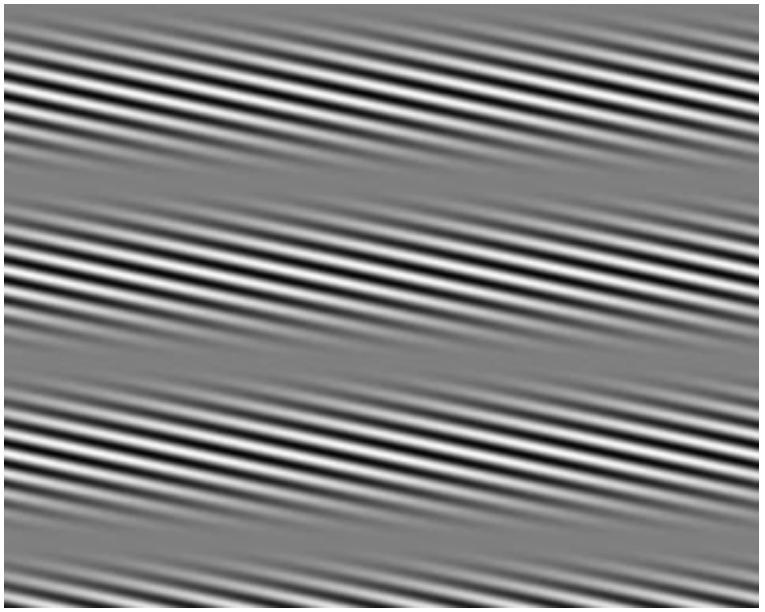
```
ModeLine "1280x1024@85"  157.5  1280 1344 1504 1728  1024 1025 1028 1072
```

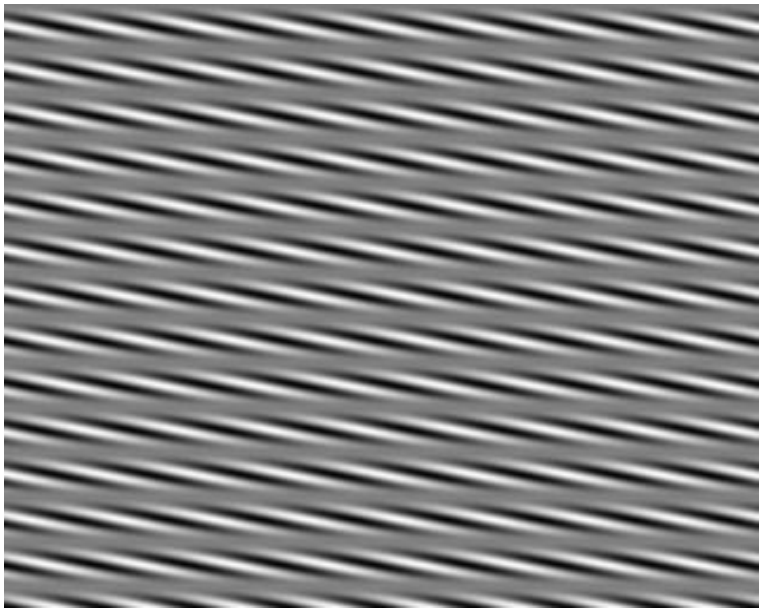
Image mostly stable if relative error of f_h below $\approx 10^{-7}$.

AM audio broadcast from CRT displays

$$s(t) = A \cdot \cos(2\pi f_{\mathrm{c}} t) \cdot [1 + m \cdot \cos(2\pi f_{\mathrm{t}} t)]$$

300 and 1200 Hz tones at $f_{\mathrm{c}} = 1.0$ MHz:





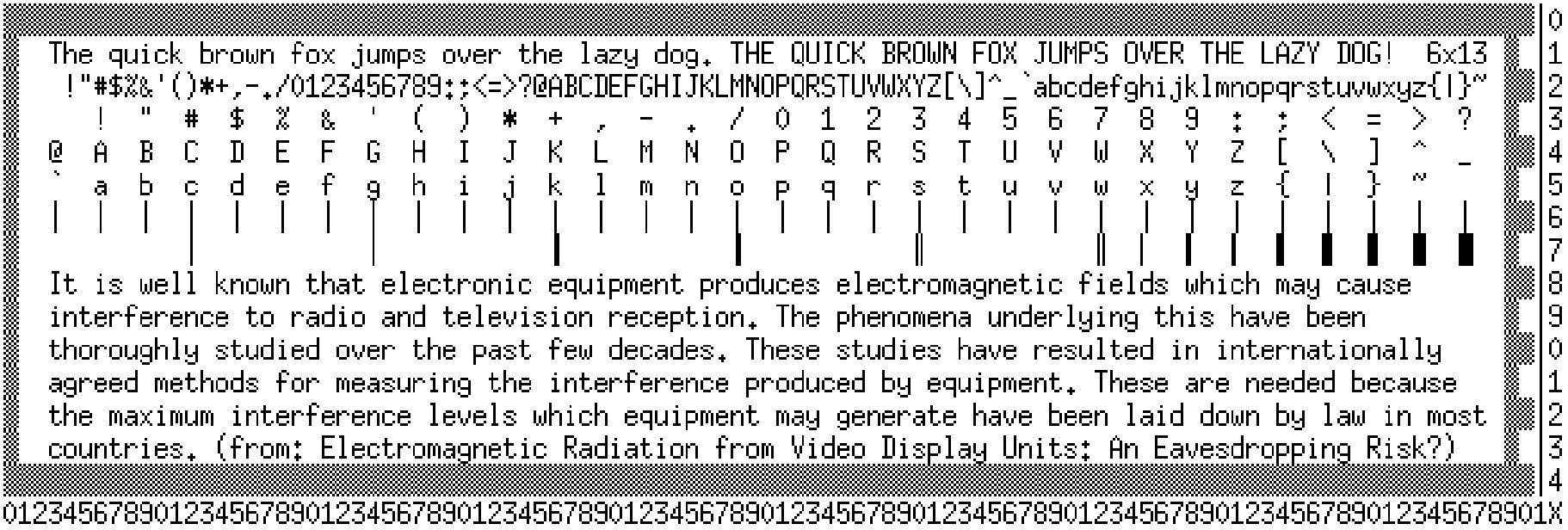
Play your MP3 music at home via CRT emanations in your AM radio:

`http://www.erikyyy.de/tempest/`

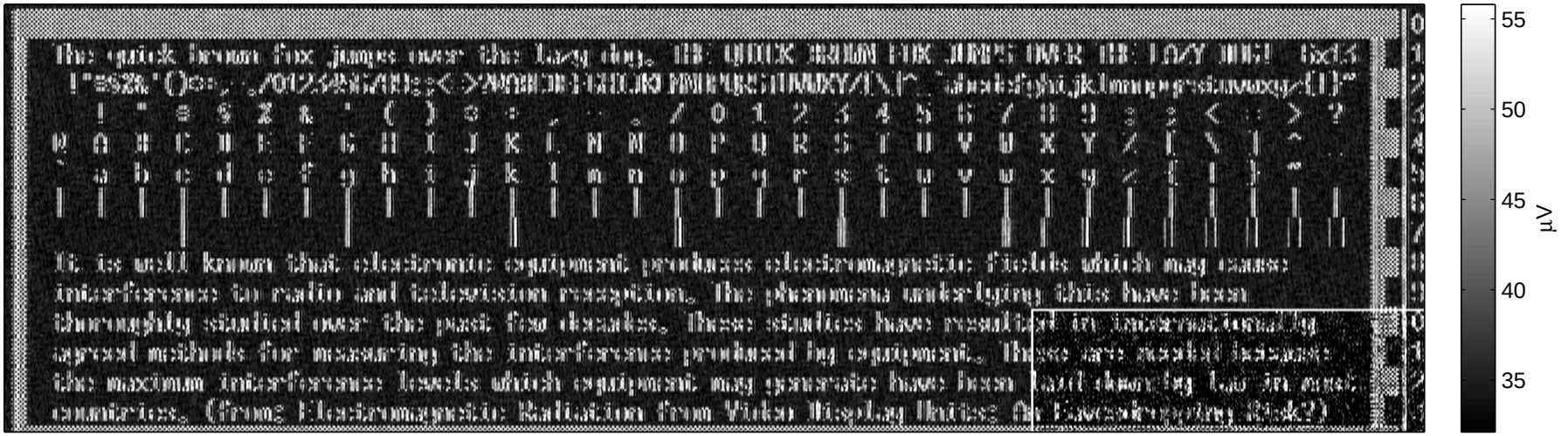
Eavesdropping of CRT Displays

CRT Monitor amplifies with $\gg 100$ MHz bandwidth the video signal to $\approx 100\ V$ and applies it to the screen grid in front of the cathode to modulate the e-beam current. All this acts together with the video cable as a (bad) transmission antenna.

Test text used in the following experiments:



480 MHz center frequency, 50 MHz bandwidth, 256 (16) frames averaged, 3 m distance



480 MHz center frequency, 50 MHz bandwidth, magnified image section

Automatic Radio Character Recognition

Example Results (256 frames averaged):

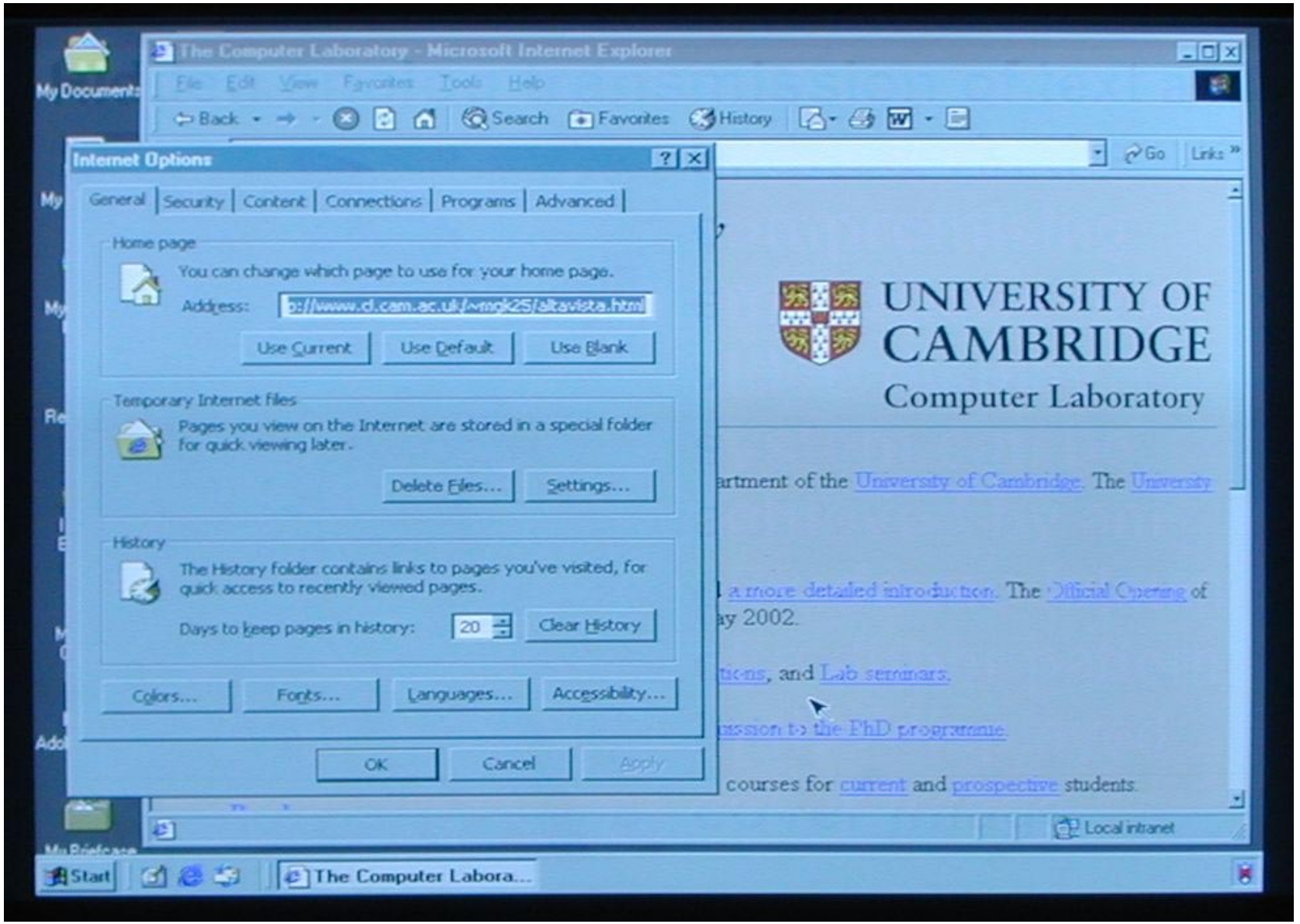
```
  The quick brown fox jumps over the lazy dog. THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG!  6x13
   !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_‘abcdefghijklmnopqrstuvwxyz{|}~
  It is well known that electronic equipment produces electromagoetic fields which may cause
  interference to radio and television reception. The phenomena underlying this have been
  thoroughly studied over the past few decades. These studies have resulted in internationally
  agreed methods for measuring the interference produced by equipment. These are needed because
  the maximum interference levels which equipment may generate have been laid down by law in most
  countries. (from: Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?)
```

With only 16 frames averaged:

```
  Ihc quick bcown fox_jumps-evec-toe Iazg dsg_=TOE_QHICK-DROWM-EHX JUHPS Q?ER iUE LOZY DH6! -6zi3=
   !"#$%&'()* ,-=Z0!?3‘5670 9:;< >?@ADcDEFCHIJKLHNcPQRHTHVQ%YZ[\]^=‘abedcBg6Ijkimndpqcstuvw:yz{|}"
  it Ic weII=kocwn=tHat-clectroric=cguipmcnt e_dduces-electrpmugmctic_fidlde_whico-may euuse  _-.
= icce-feceaee tc-radic-and teIcvisicn ceccpticc=-|6e phcncmcna uedcrlyigg tcic=have=bcec_=    -=
_-tncceughIy ctuHicd=dvcc the eust few=decudes, ihcsc stvdics‘have =ecuItcd io_inteceutiocu_iy   -
_ ugrceH=mct6edc=foc meacuciny t6c icterfcsesce pcoduccd_bg eeuipmcnt. Tbese are-nccded bccouse
  toc=meximum intcrfercncc ievcls which-eguipmcnt may gesc-atc-6ave oecn la7d=dewc=by law in mcsc
  ceuntricc=-(fcem: FIectromegnctic-Radiatibn f_om Video Dispiey_Hsitc:=Hn Eavcsdcc=pimg-Risk?)-
```

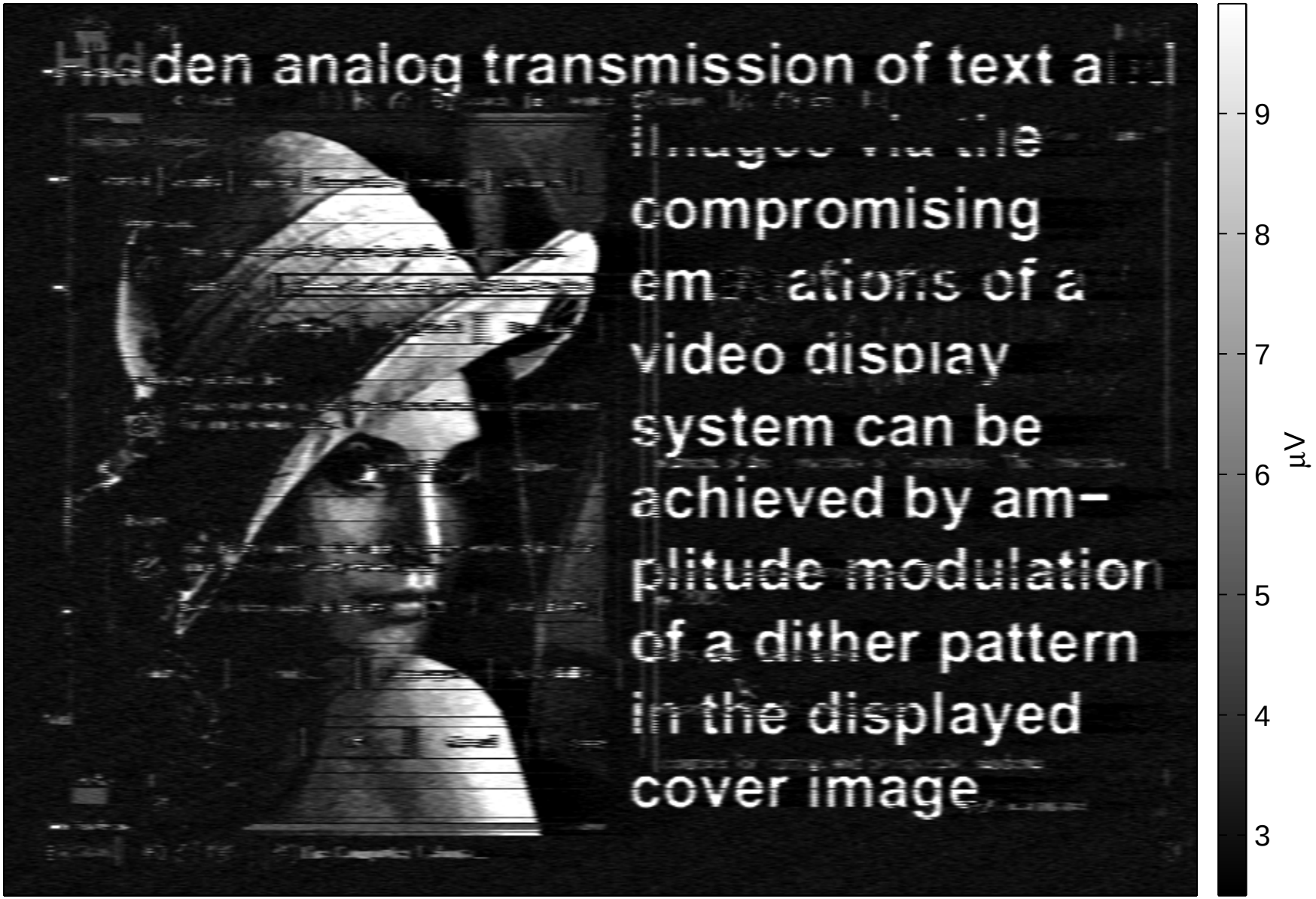
Steganographic transmission of images

The user sees on her screen:

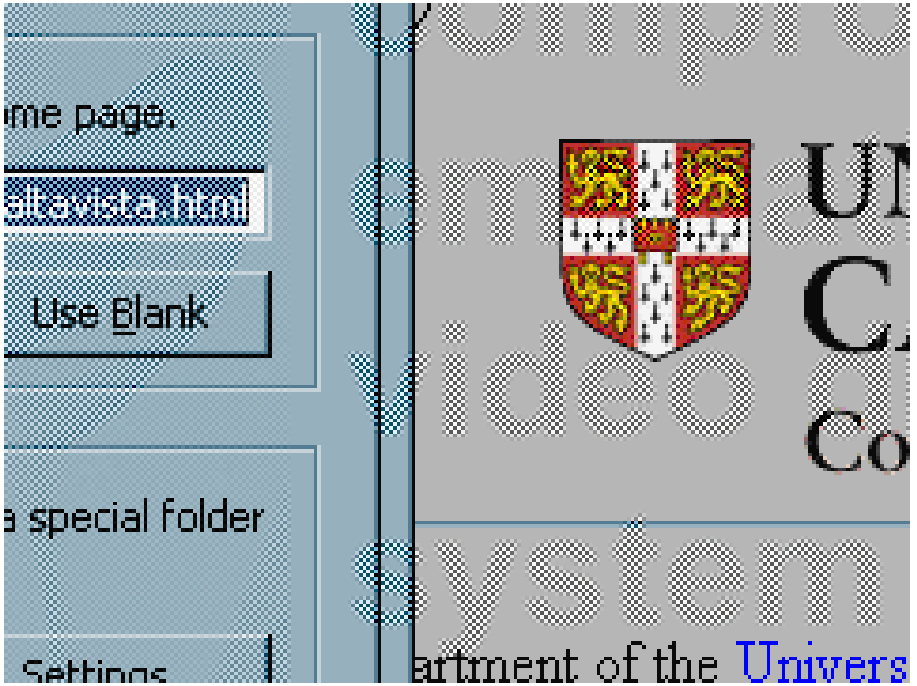


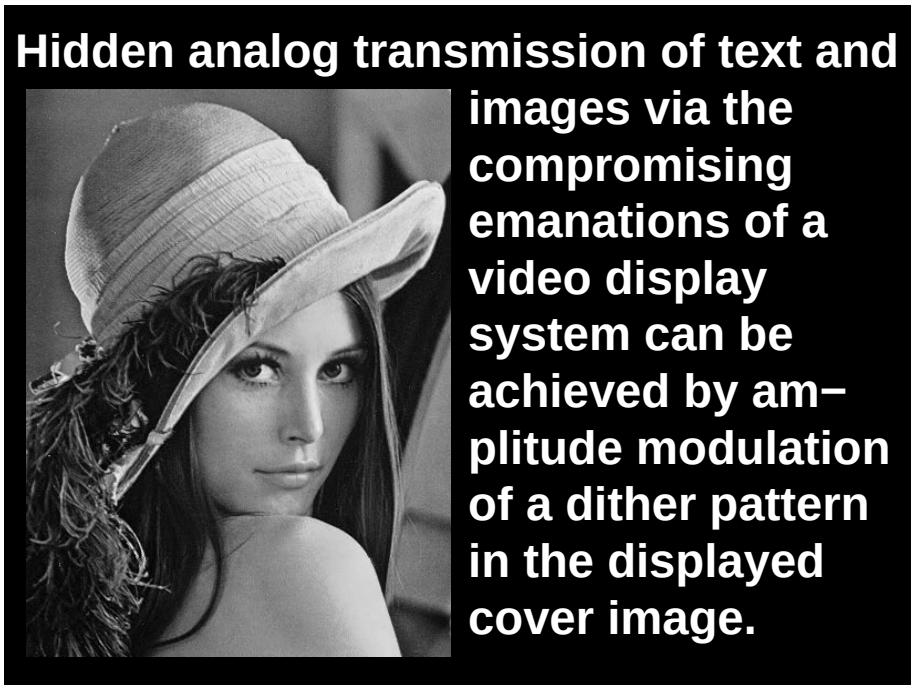
The radio frequency eavesdropper receives instead:

445 MHz center frequency, 10 MHz bandwidth, 1024 frames averaged, 3 m distance



Amplitude modulation of dither patterns



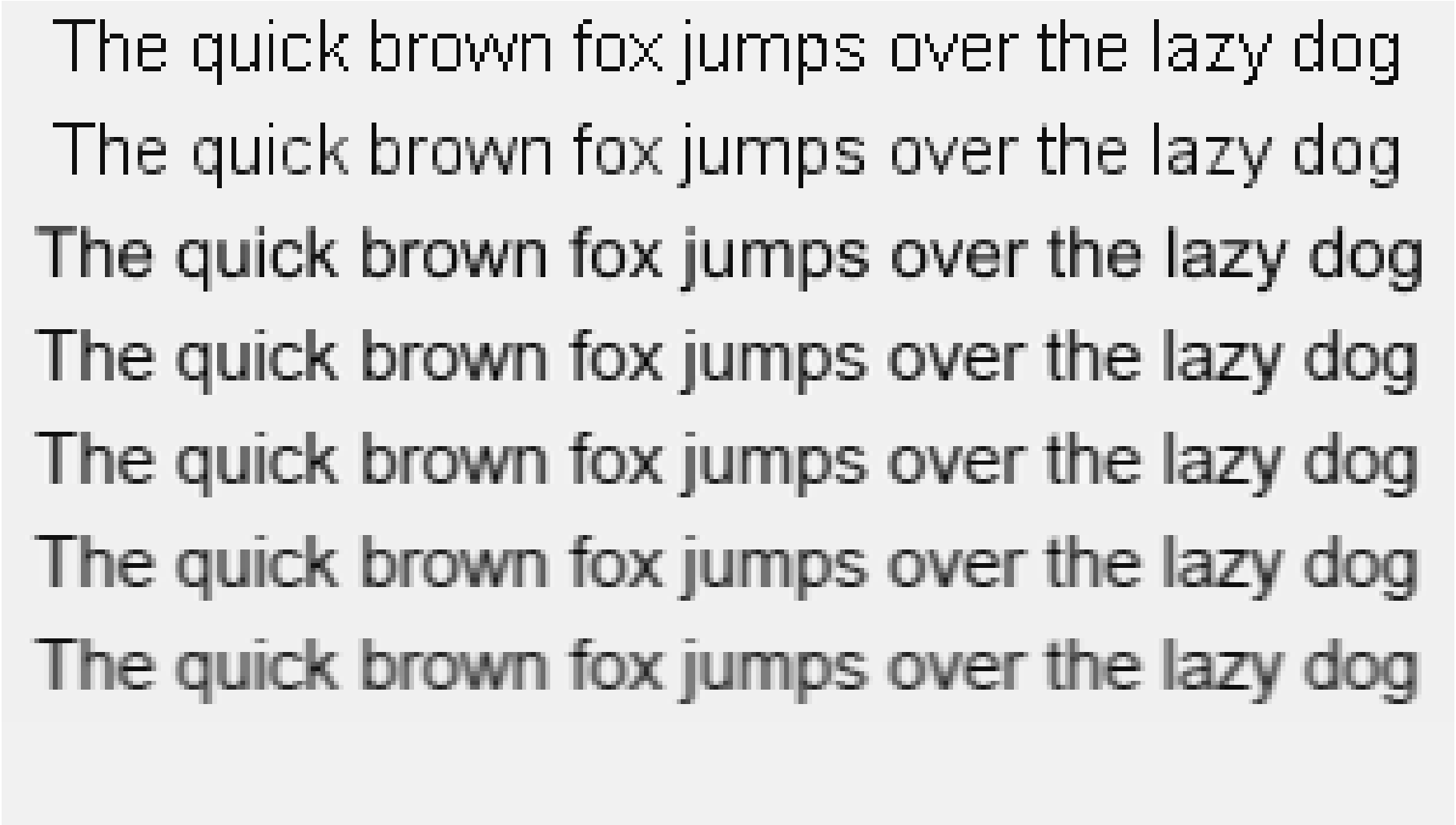


Cover image $C_{x,y,c}$, embedded image $E_{x,y}$, all normalized to [0,1]. Then screen display is

$$S_{x,y,c} = \left(C_{x,y,c}^{\tilde{\gamma}} + \min\{\alpha E_{x,y}, C_{x,y,c}^{\tilde{\gamma}}, 1 - C_{x,y,c}^{\tilde{\gamma}}\} \cdot d_{x,y}\right)^{1/\tilde{\gamma}}$$

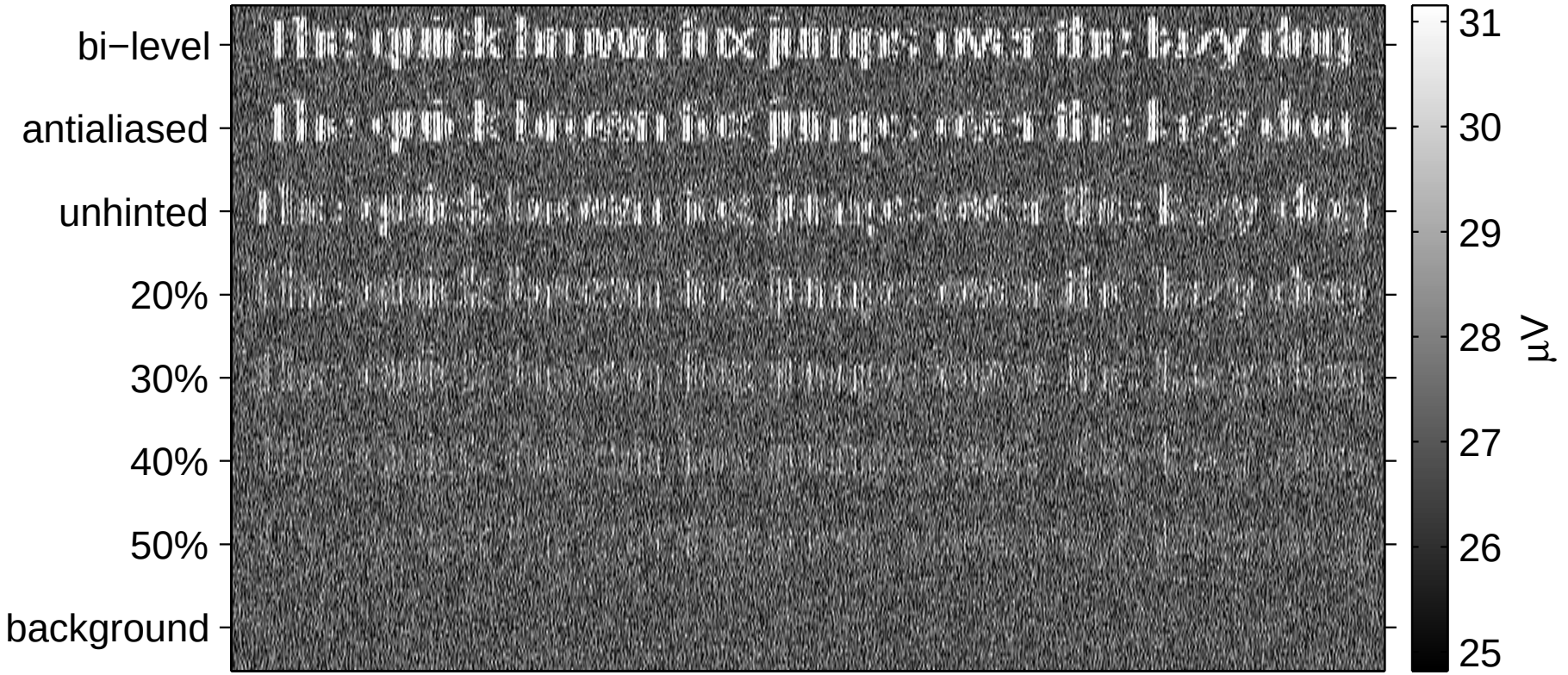
with dither function $d_{x,y} = 2[(x+y) \bmod 2] - 1 \in \{-1, 1\}$ and $0 < \alpha \leq 0.5$.

Filtered fonts as a protection measure



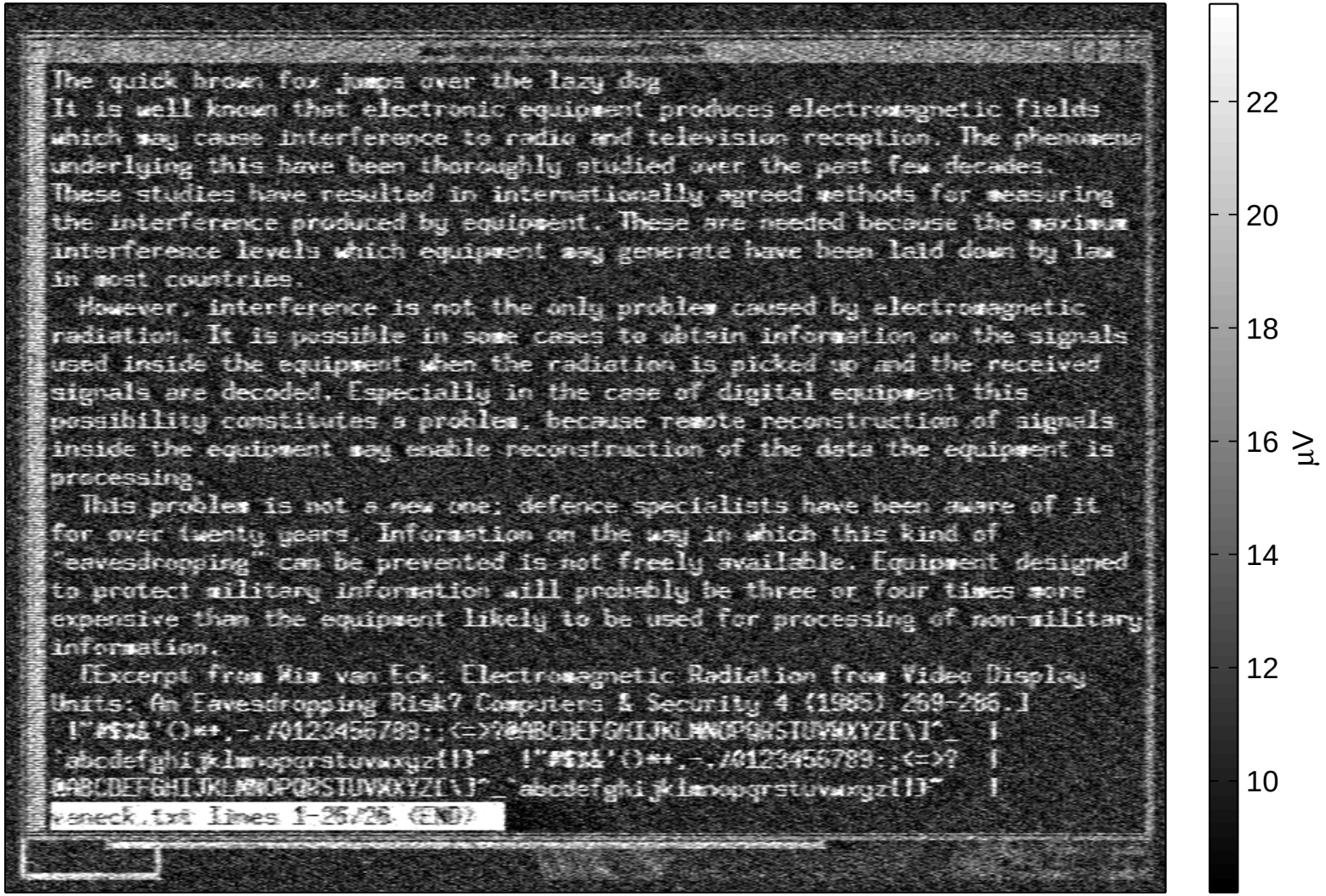
Received radio signal

740 MHz center freq., 200 MHz bandwidth, 256 frames averaged, 3 m distance



Eavesdropping across two office rooms

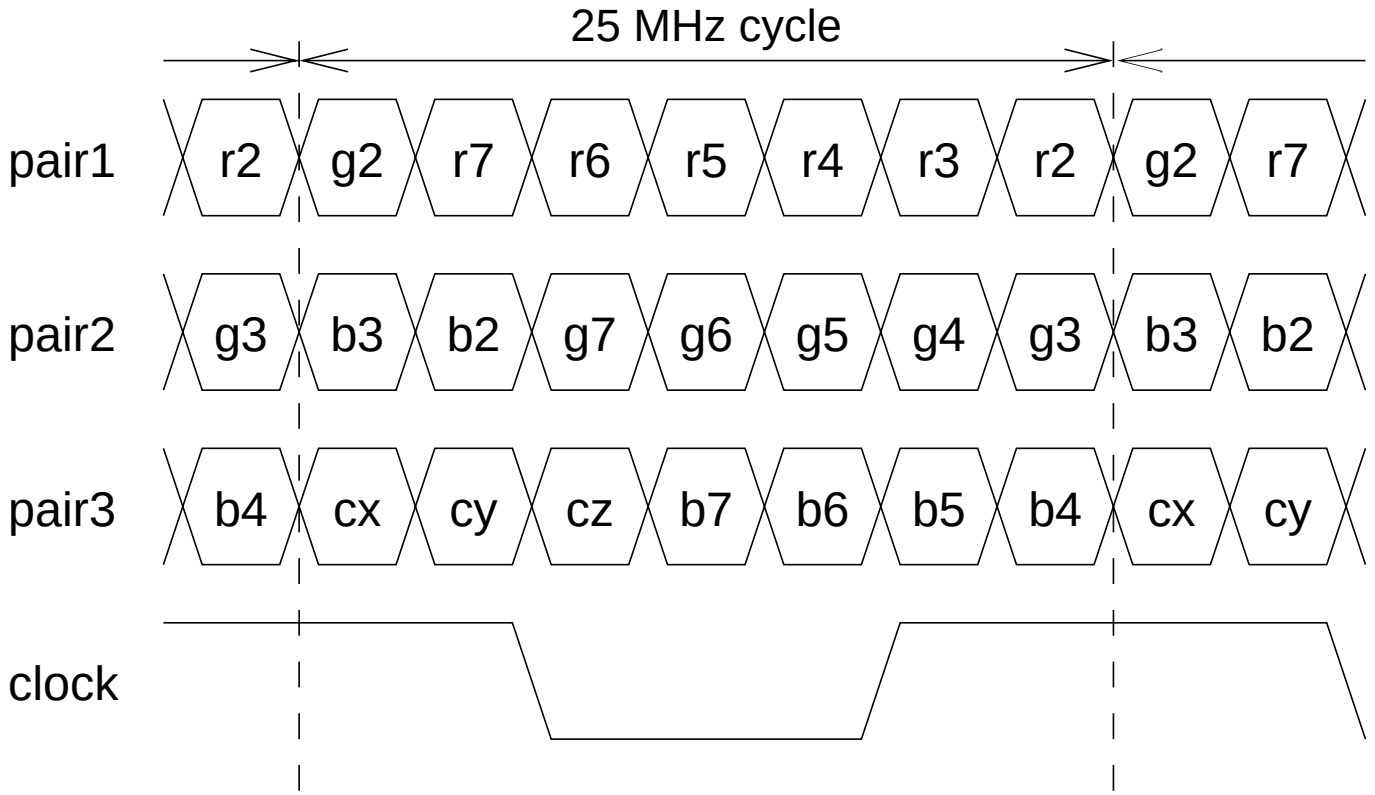
350 MHz, 50 MHz BW, 12 frames (160 ms) averaged



Target in room GE16 and antenna in room GE10 of the William Gates building, with two offices and three plasterboard walls (-2.7 dB each) in between.

FPD-Link – a digital video interface

LCD module and video controller are connected in Toshiba 440CDX laptop by eight twisted pairs (each 30 cm), which feed the 18-bit RGB parallel signal through the hinges via low-voltage differential signaling (LVDS, EIA-644).



Minimal/maximal reception contrast

350 MHz center frequency, 50 MHz bandwidth, 16 frames averaged, 3 m distance