Electromagnetic eavesdropping on computers

Markus Kuhn

2002-06-12

UNIVERSITY OF CAMBRIDGE

Computer Laboratory

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

The rôle of hardware security

Protection of confidential information becomes easier:

⟶ availability of strong crypto primitives

⟶ CPU power (eliminates crypto performance penalty)

⟶ communication/storage cryptography now basic OS service

⟶ renaissance of mandatory access control

Professions depending on unauthorized information access such as

⟶ law enforcement / intelligence community

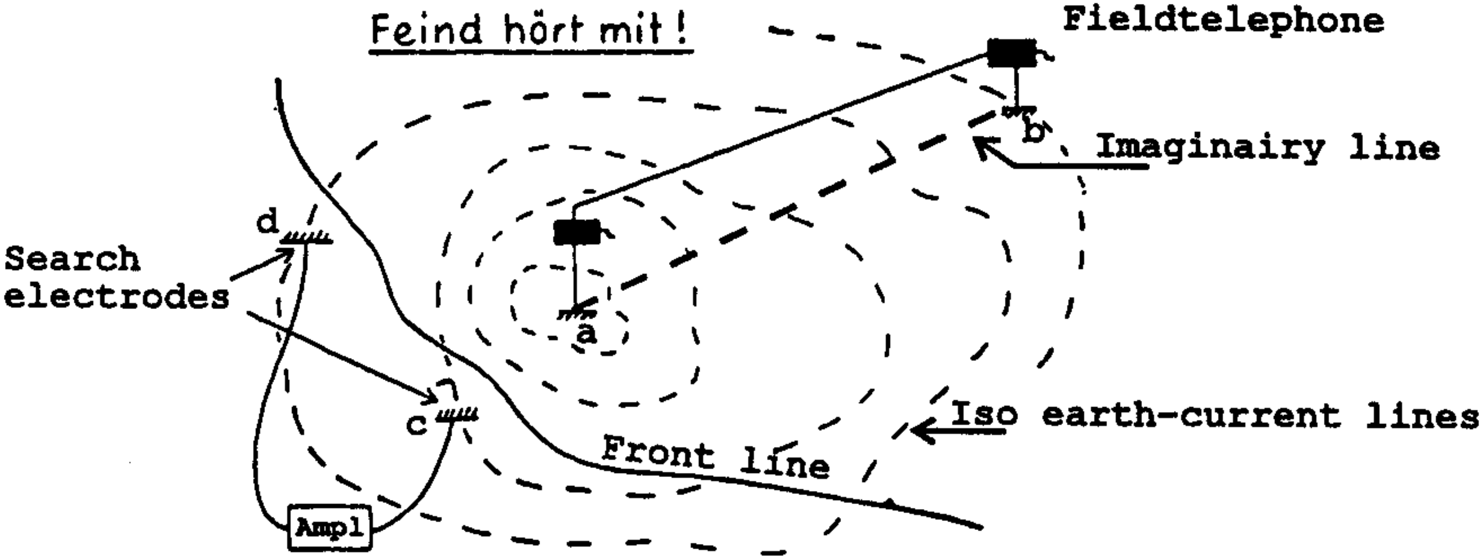
⟶ criminals

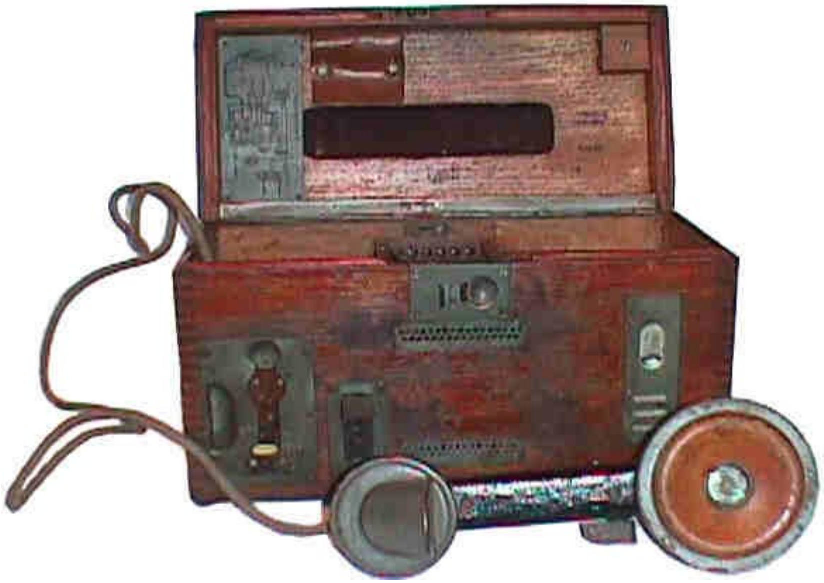
⟶ copyright license monitoring

⟶ market research

are increasingly interested in new/unorthodox access techniques.

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.

Open Literature on Compromising Emanations

⟶ 1985: Wim van Eck demonstrates eavesdropping on video displays with a modified TV set in BBC's "Tomorrow's World".

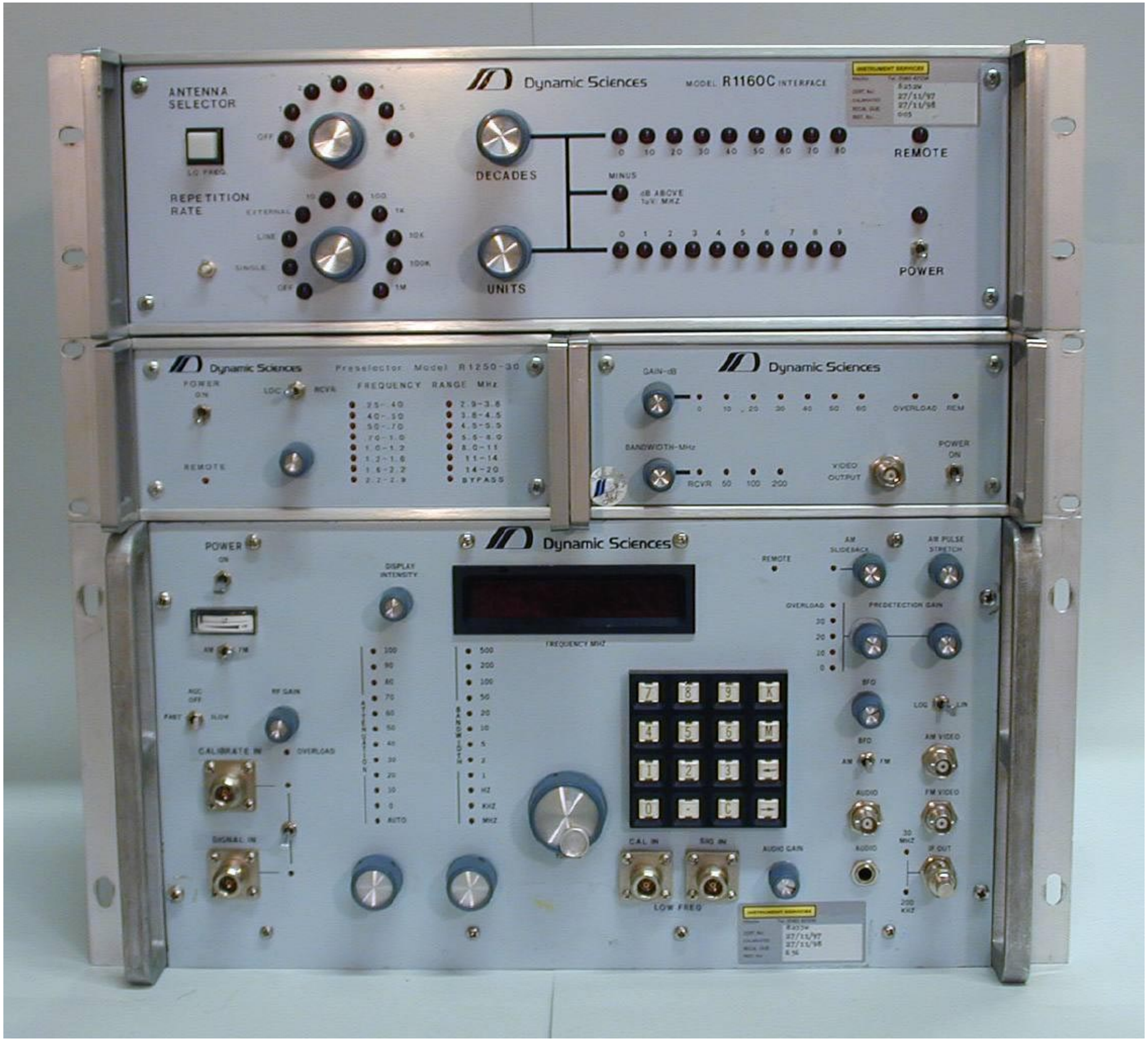
⟶ 1990: Peter Smulders investigates electromagnetic eavesdropping on RS-232 cables.

⟶ 1988/1991: Two Italian conferences on electromagnetic security for information protection.

⟶ 1998: We demonstrate steganographic forms of compromising video emanations.

⟶ 1999: Paul Kocher et al. demonstrate reconstruction of DES keys from power supply fluctuations in smartcard microcontrollers.

R1250 Wideband Tempest Receiver



Wideband Tempest Measurement Receivers

→ Can be tuned continuously from 100 Hz to 1 GHz.

→ Offers 21 bandwidths from 50 Hz to 200 MHz (1-2-5 steps).

For comparison:

- AM radio: 2–10 kHz
- FM radio: 200 kHz
- TV set: 6 MHz

→ Especially robust antenna input (for listening on power lines).

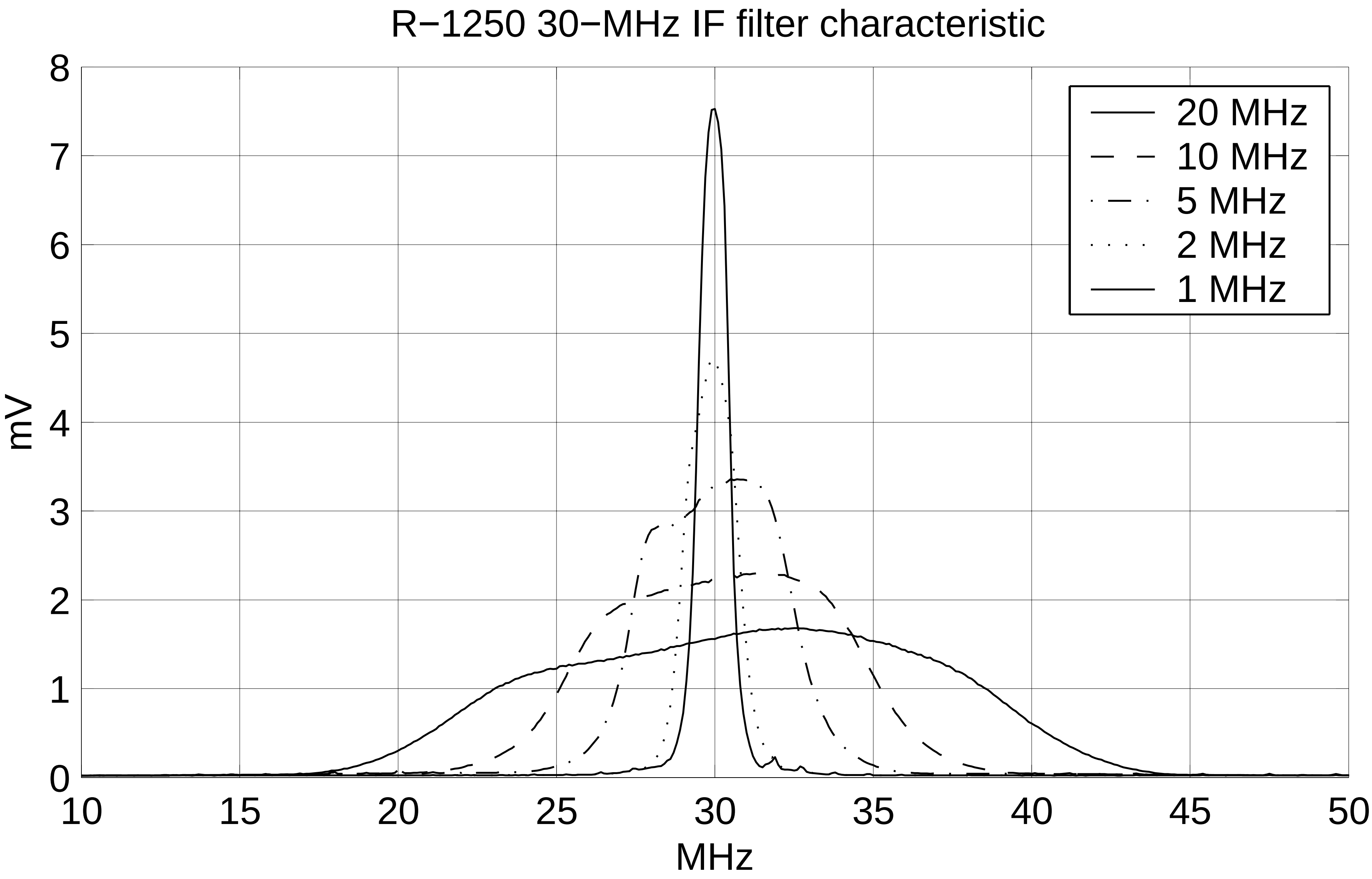
→ Gain adjustable by a factor of 10^9.

→ Automatic gain control circuit can be deactivated.

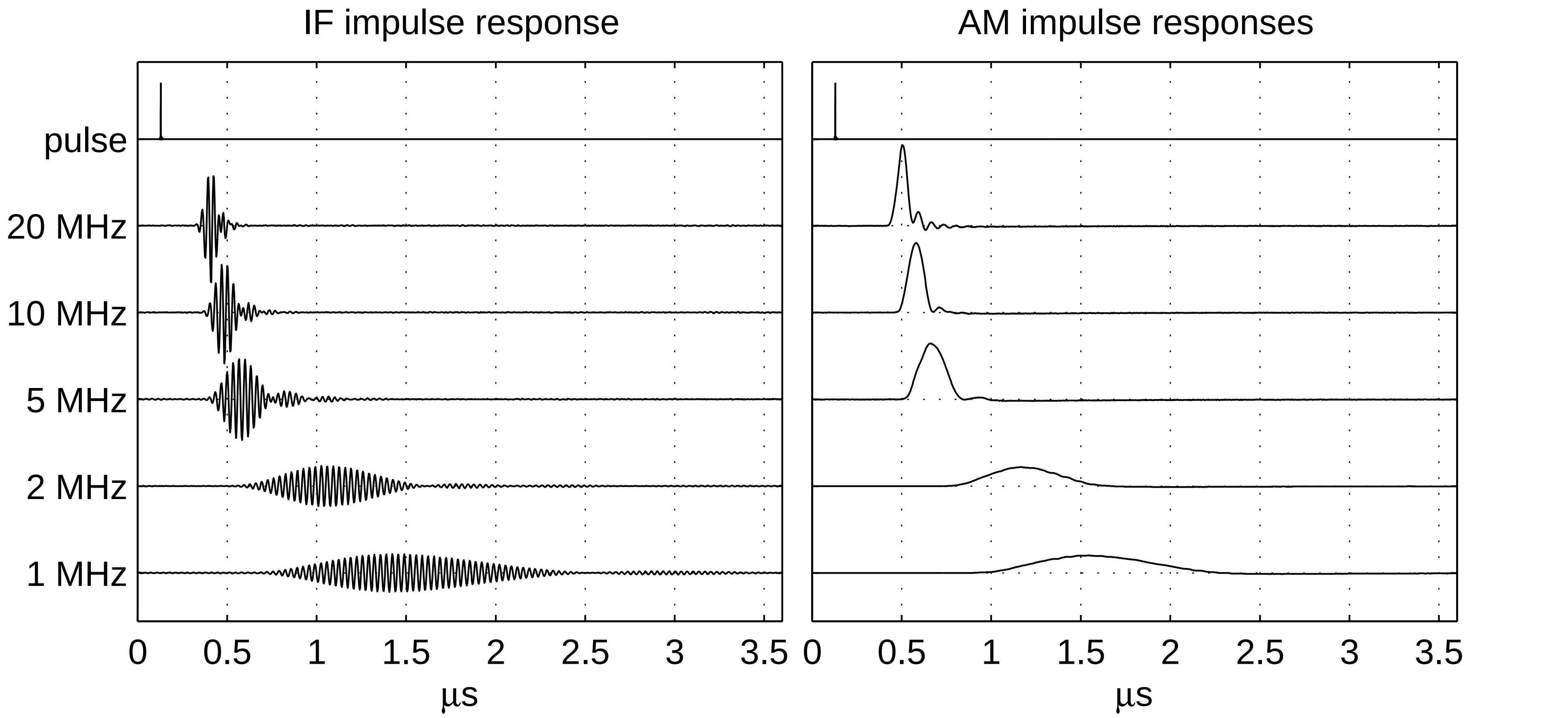
→ Demodulators: AM linear, AM logarithmic, FM, BFO.

→ Export controlled products, ≈ 30–100 k£.

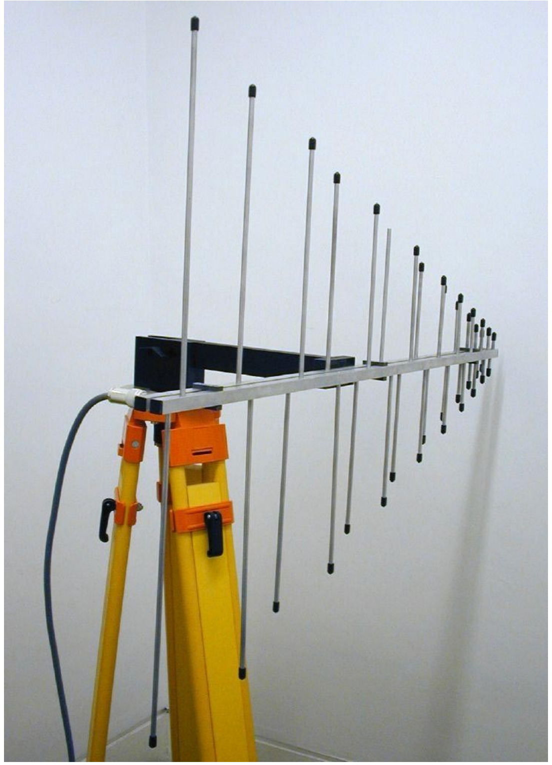
Intermediate frequency bandwidth



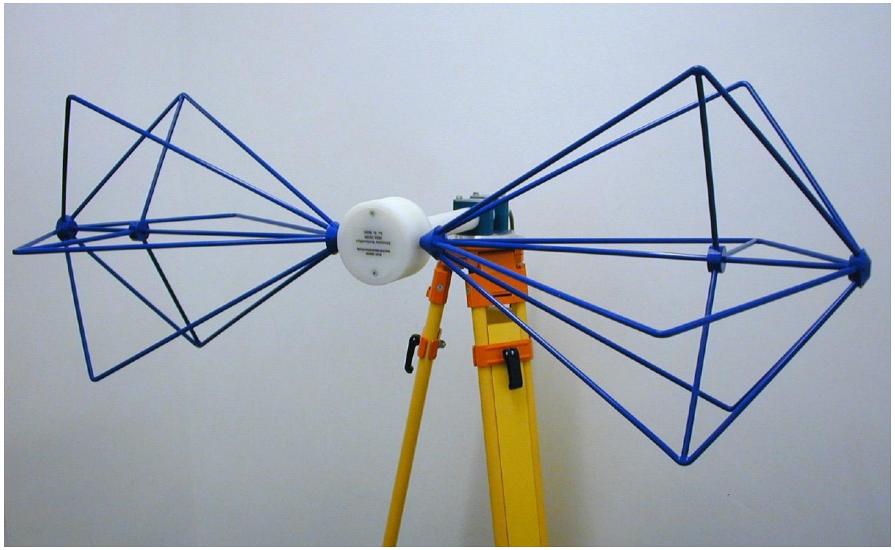
Receiving impulse signals



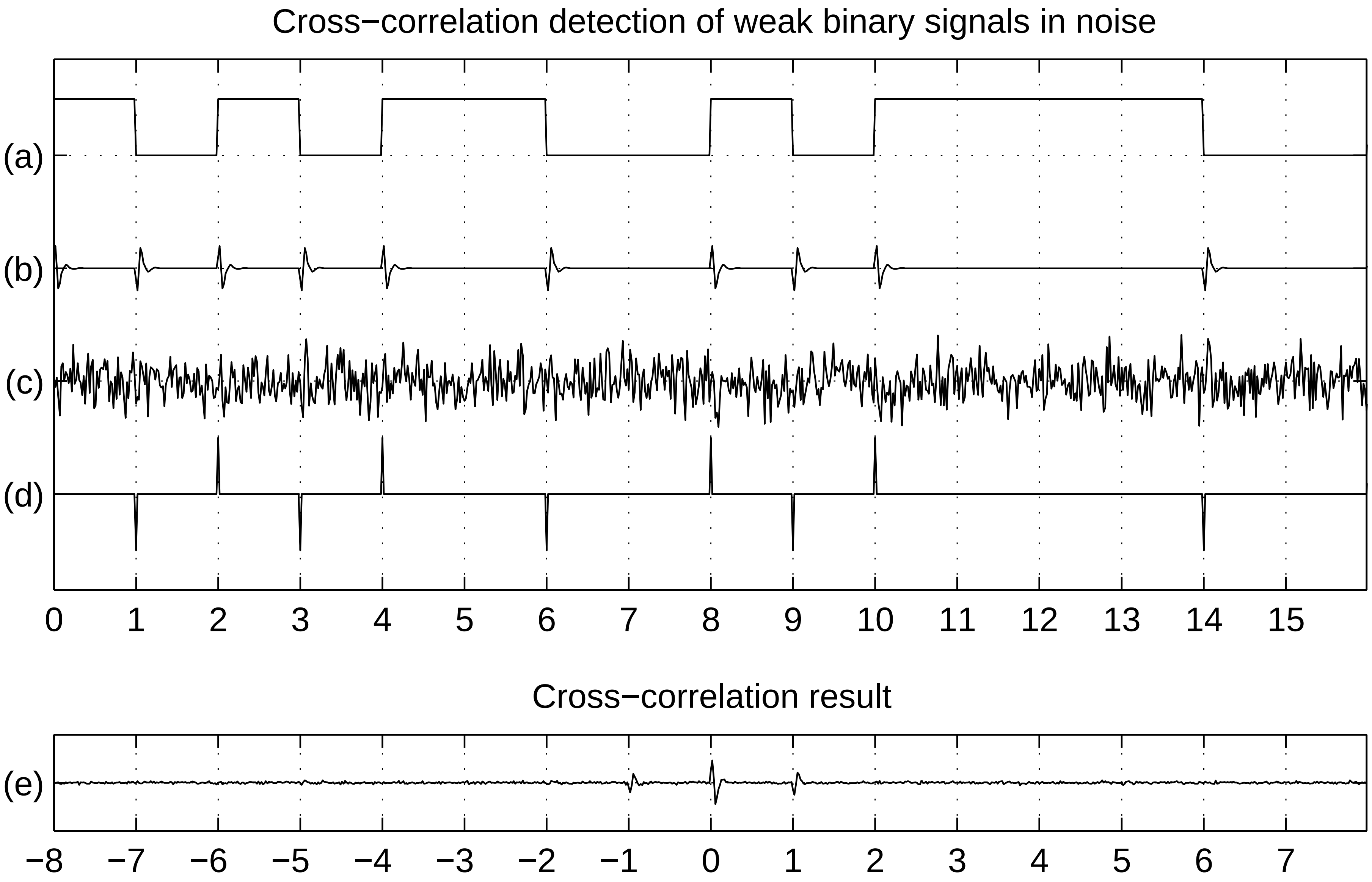
$$\text{impulse width} = \frac{1}{\text{bandwidth}}$$



FIELD SELECTOR
POWER
Dynamic Sciences



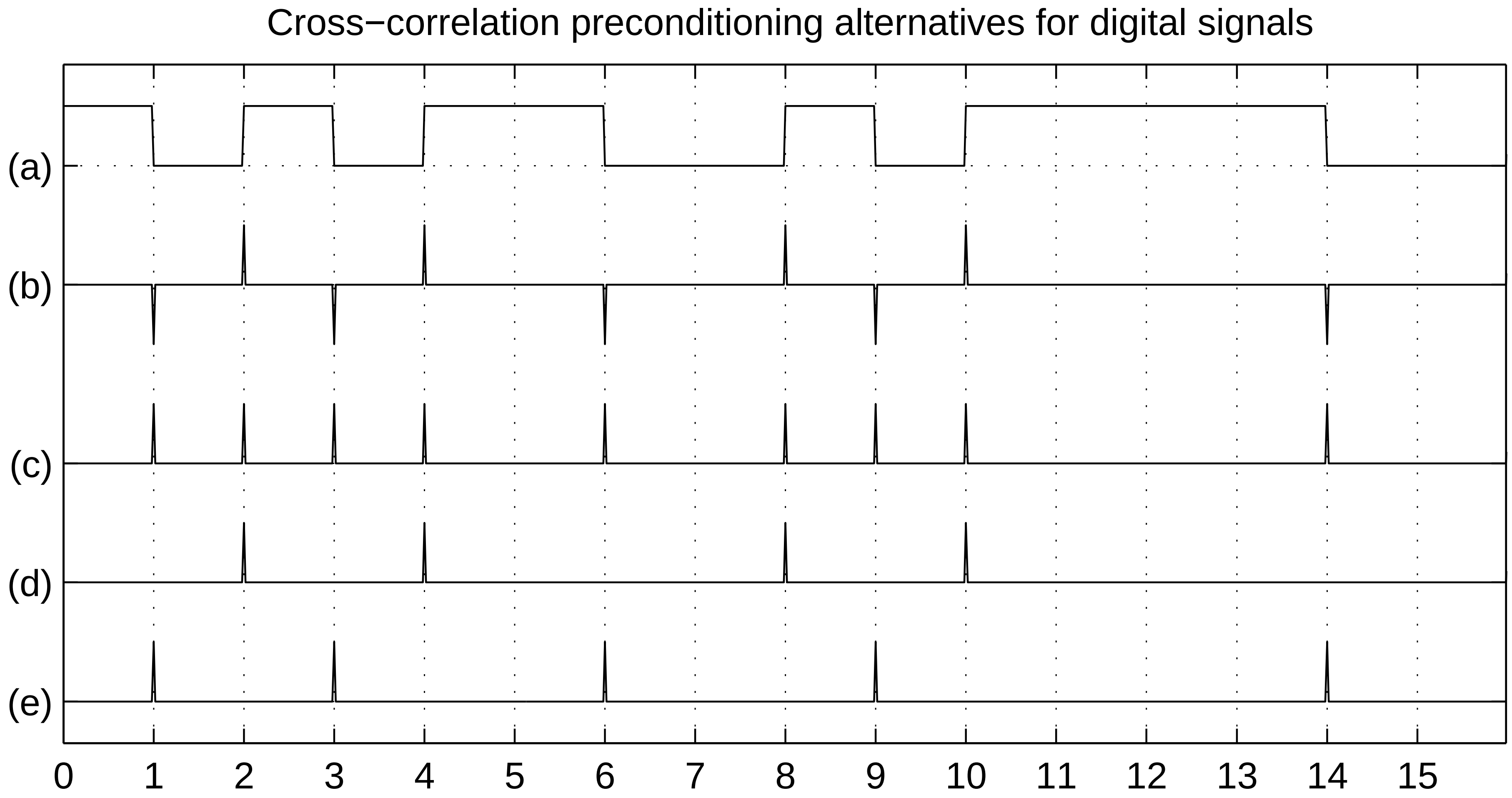
H
E
FIELD SELECTOR
ON
OFF
POWER
Dynamic Sciences



Cross−correlation detection of weak binary signals in noise

Cross−correlation result

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


Cross−correlation preconditioning alternatives for digital signals
(a)
(b)
(c)
(d)
(e)
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

Video Timing

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

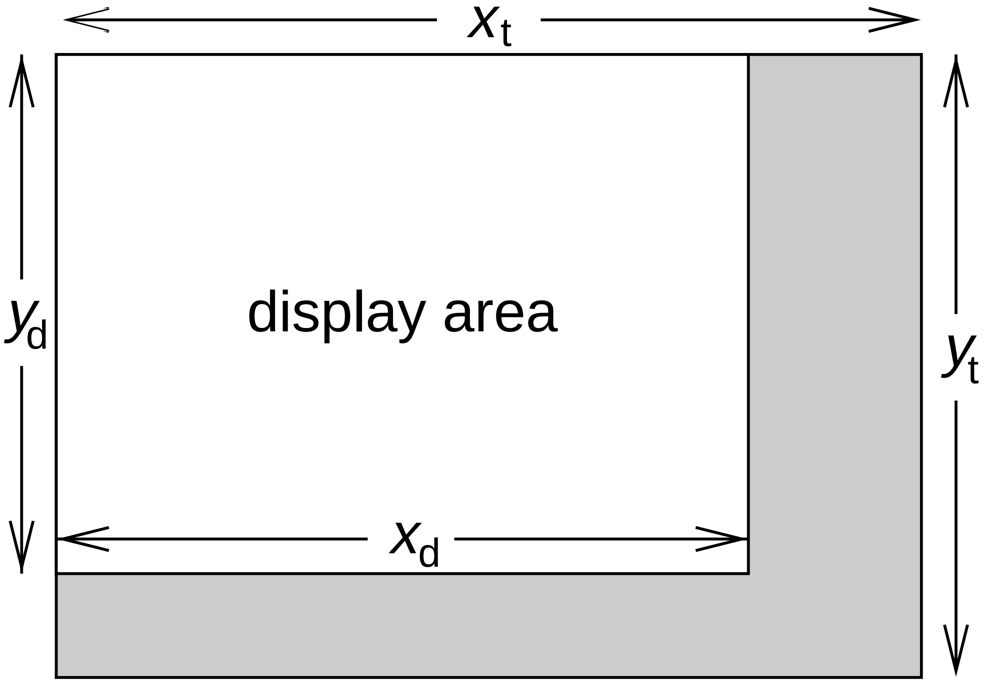
Pixel frequency: f_p

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 ±0.5%.

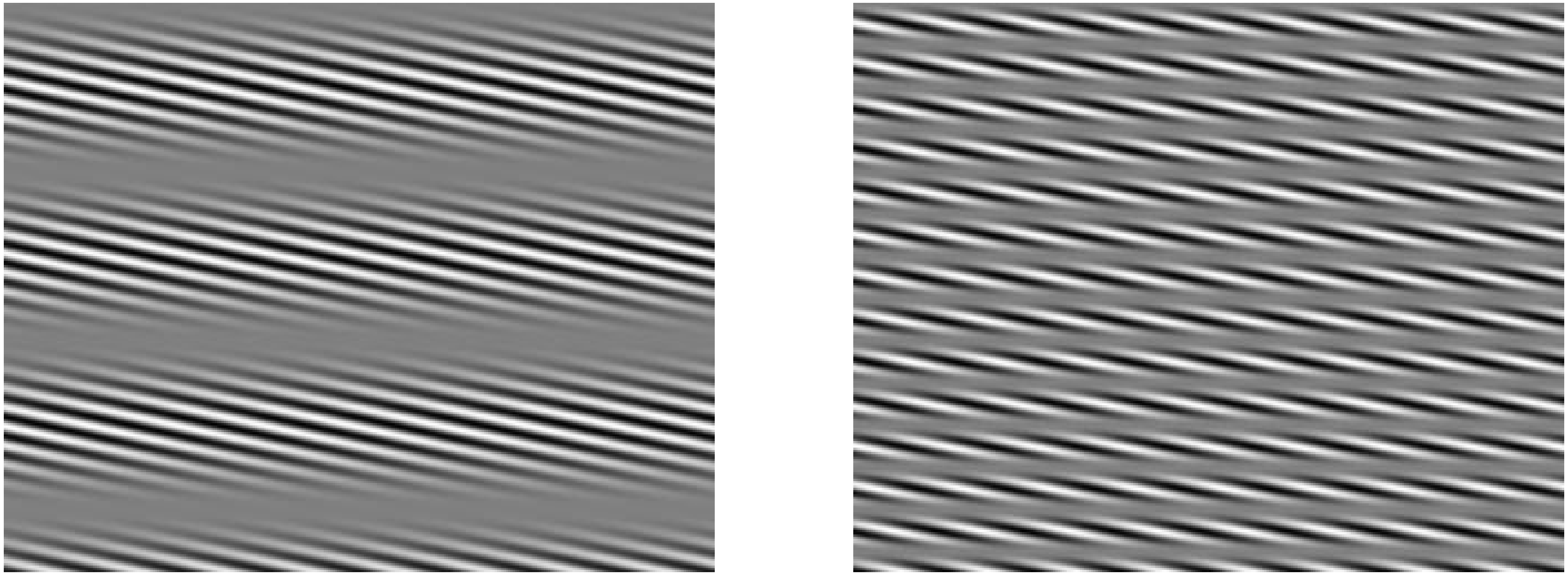
```
ModeLine "1280x1024@85"  157.5  1280 1344 1504 1728  1024 1025 1028 1072
```

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

AM audio broadcast from CRT displays

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

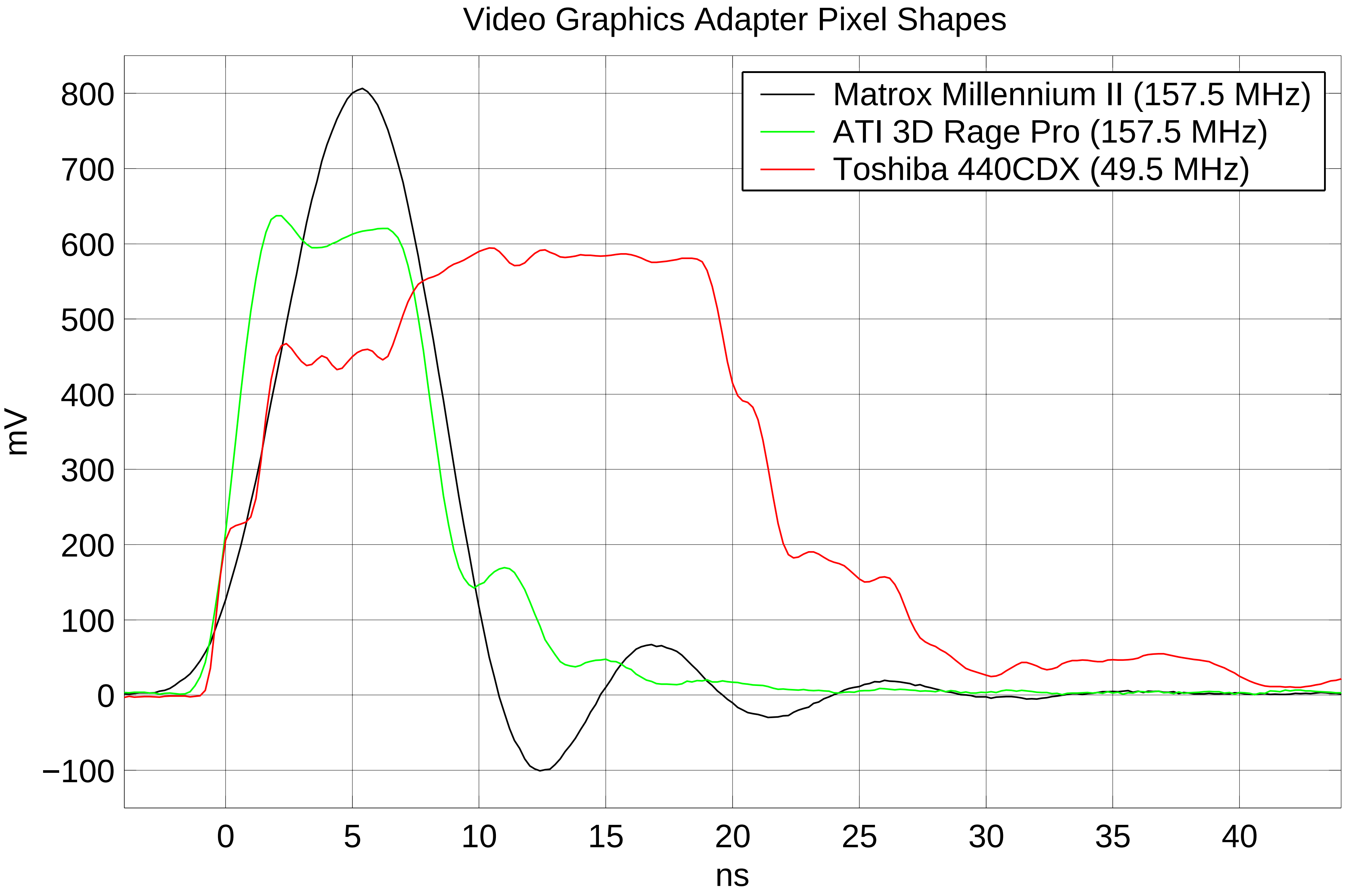
300 and 1200 Hz tones at $f_{\mathrm{c}} = 1.0$ MHz:



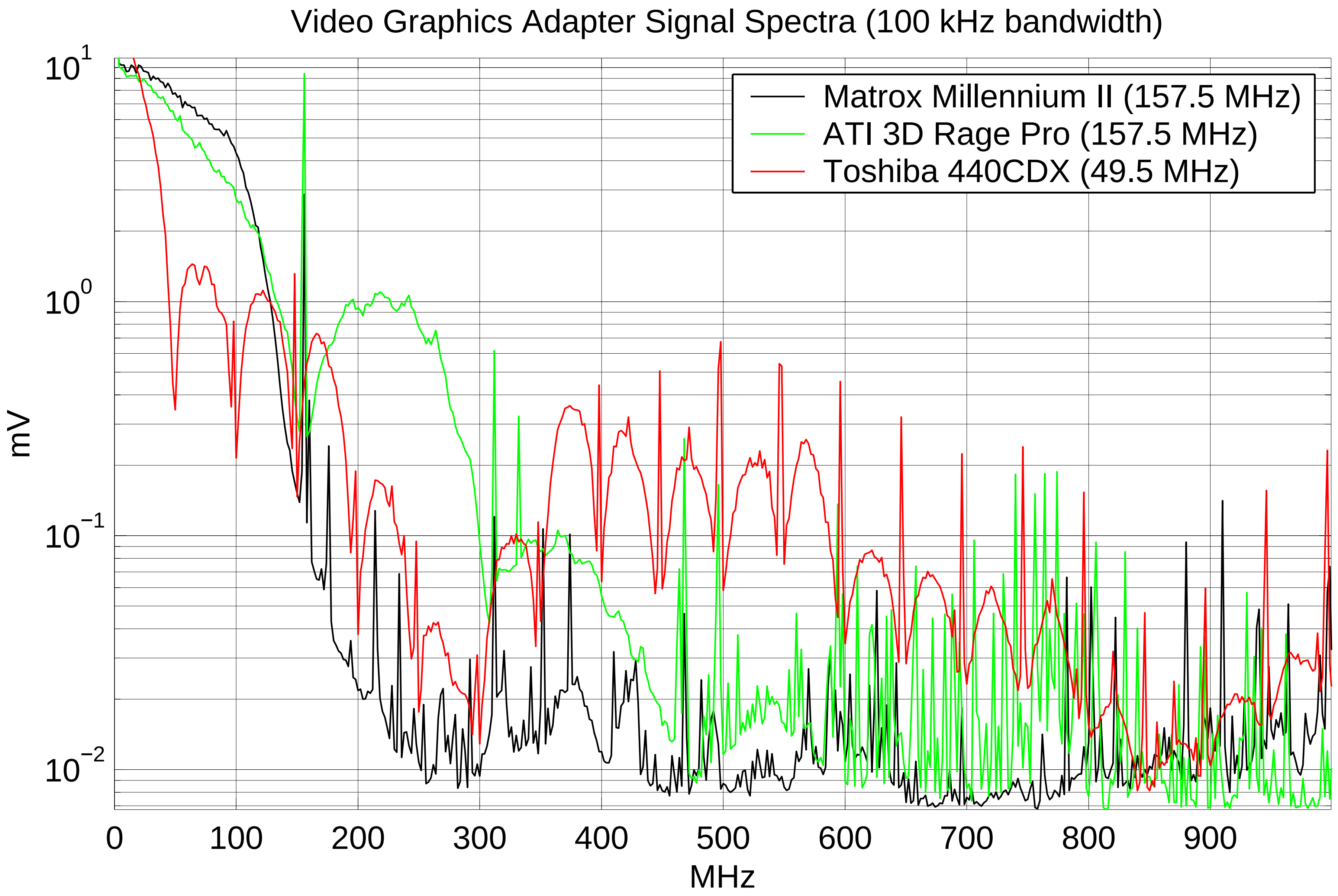
Play your MP3 music at home via CRT emanations in your AM radio:

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

Real-world VGA card pixel shapes



Real-world VGA card frequency spectrum



Analog video signal spectra

Fourier transform

$$
\begin{aligned}
\mathcal{F}[h](f) &= \int_{-\infty}^{\infty} h(t)\,\mathrm{e}^{2\pi \mathrm{j} f t}\,\mathrm{d}t \\
\mathcal{F}^{-1}[H](t) &= \int_{-\infty}^{\infty} H(f)\,\mathrm{e}^{-2\pi \mathrm{j} f t}\,\mathrm{d}f
\end{aligned}
$$

Convolution theorem

$$
\begin{aligned}
(g * h)(x) &= \int\limits_{-\infty}^{\infty} g(y)\,h(x-y)\,\mathrm{d}y \\
\mathcal{F}[g \cdot h] &= \mathcal{F}(g) * \mathcal{F}(h) \\
\mathcal{F}[g * h] &= \mathcal{F}(g) \cdot \mathcal{F}(h)
\end{aligned}
$$

Sampling theorem

Sequence of pixel values $v_0, v_1, v_2, \ldots$ produced with pixel frequency f_p can be represented as continuous waveform

$$v(t) = \sum_i v_i \cdot \frac{\sin \pi(f_\mathrm{p}t - i)}{\pi(f_\mathrm{p}t - i)}$$

which contains no spectral energy in frequencies $|f| > f_p/2$.

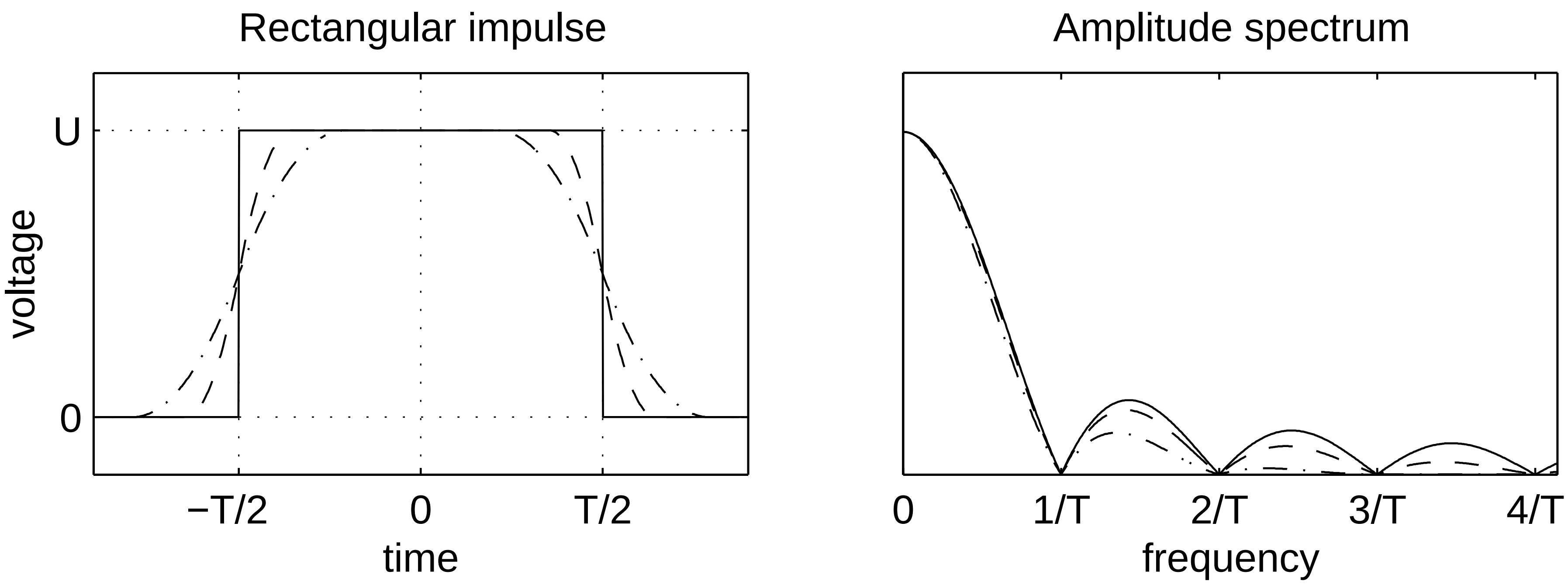
Impulse sequences

The Fourier transform of a pulse sequence is again a pulse sequence, but with reciprocal spacing:

$$\mathcal{F}\left[\sum_{i=-\infty}^{\infty} \delta(t - ik)\right](f) = \frac{1}{k} \sum_{i=-\infty}^{\infty} \delta\left(f - \frac{i}{k}\right).$$

$\Longrightarrow$ These concepts together describe every video-signal spectrum.

Amplitude spectrum of an idealised pixel

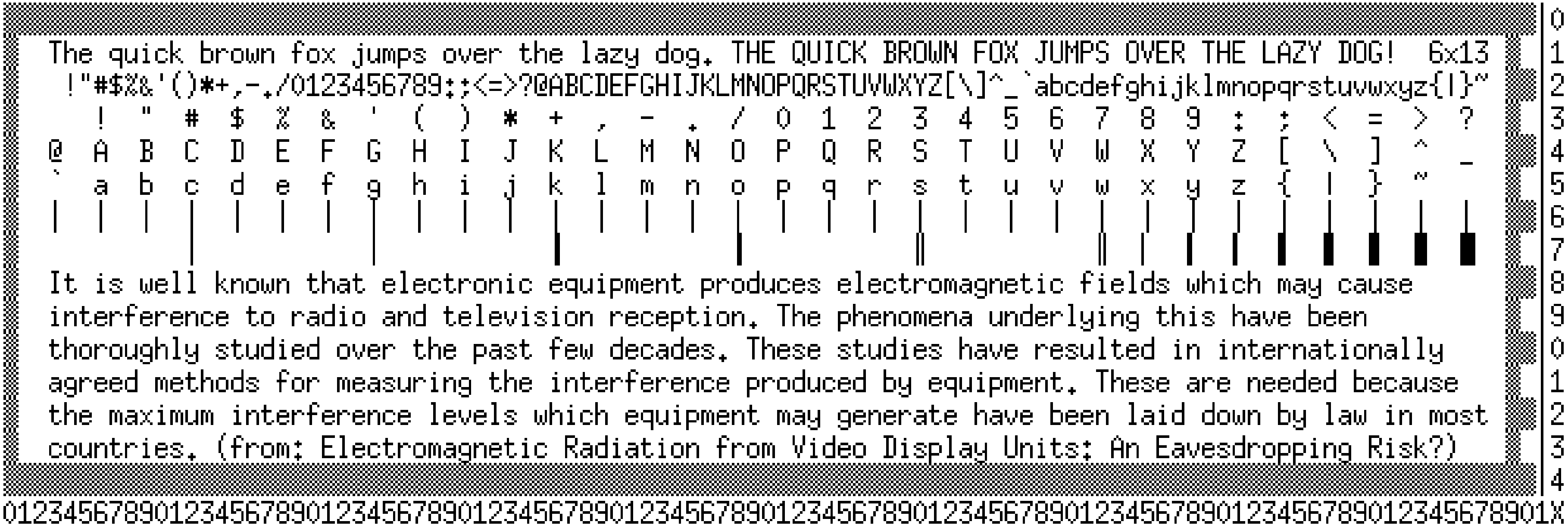


$$\mathcal{F}\left[A \cdot \Pi\left(\frac{t}{T}\right)\right](f) = AT \cdot \frac{\sin \pi T f}{\pi T f}$$

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.

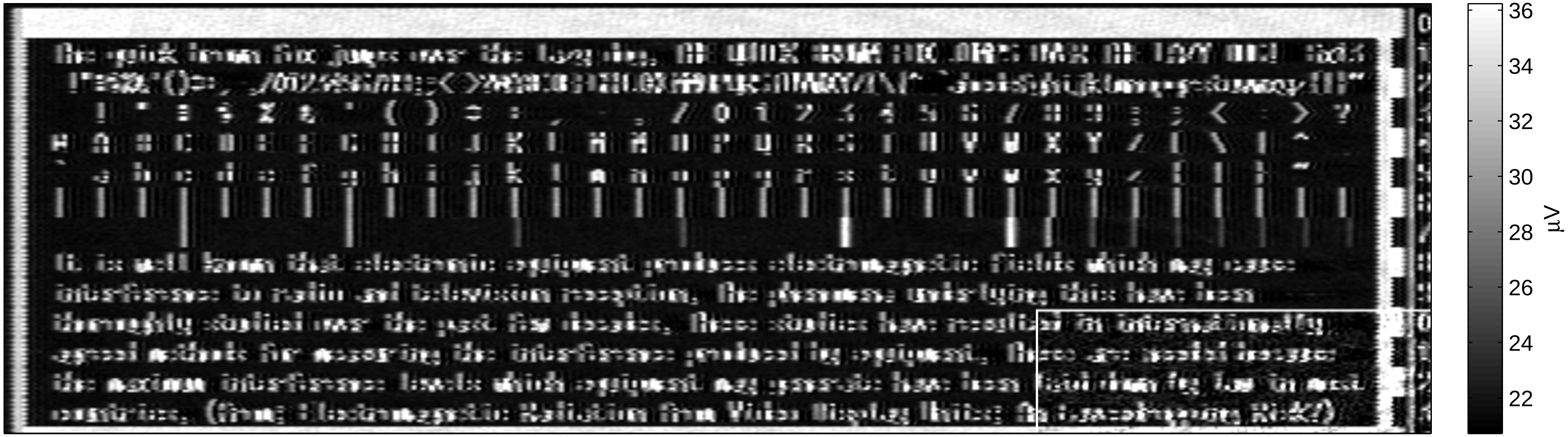
Test text used in the following experiments:



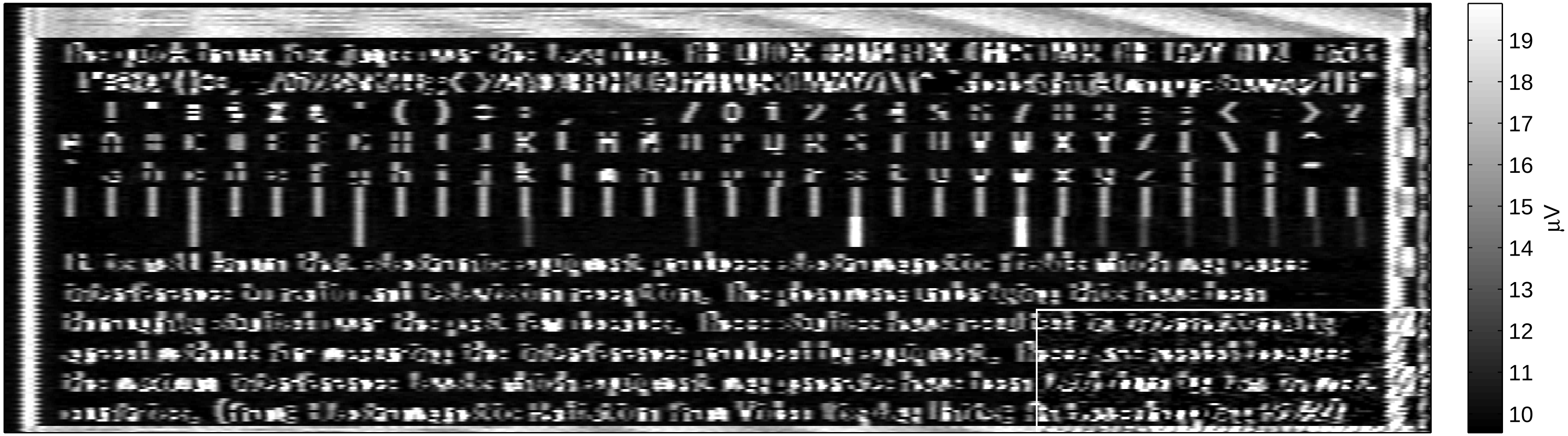
```
The quick brown fox jumps over the lazy dog. THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG!  6x13
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
   !  "  #  $  %  &  '  (  )  *  +  ,  -  .  /  0  1  2  3  4  5  6  7  8  9  :  ;  <  =  >  ?
@  A  B  C  D  E  F  G  H  I  J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z  [  \  ]  ^  _
`  a  b  c  d  e  f  g  h  i  j  k  l  m  n  o  p  q  r  s  t  u  v  w  x  y  z  {  |  }  ~

It is well known that electronic equipment produces electromagnetic 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?)
```

0
1
2
3
4
5
6
7
8
9
0
1
2
3
4
012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901X

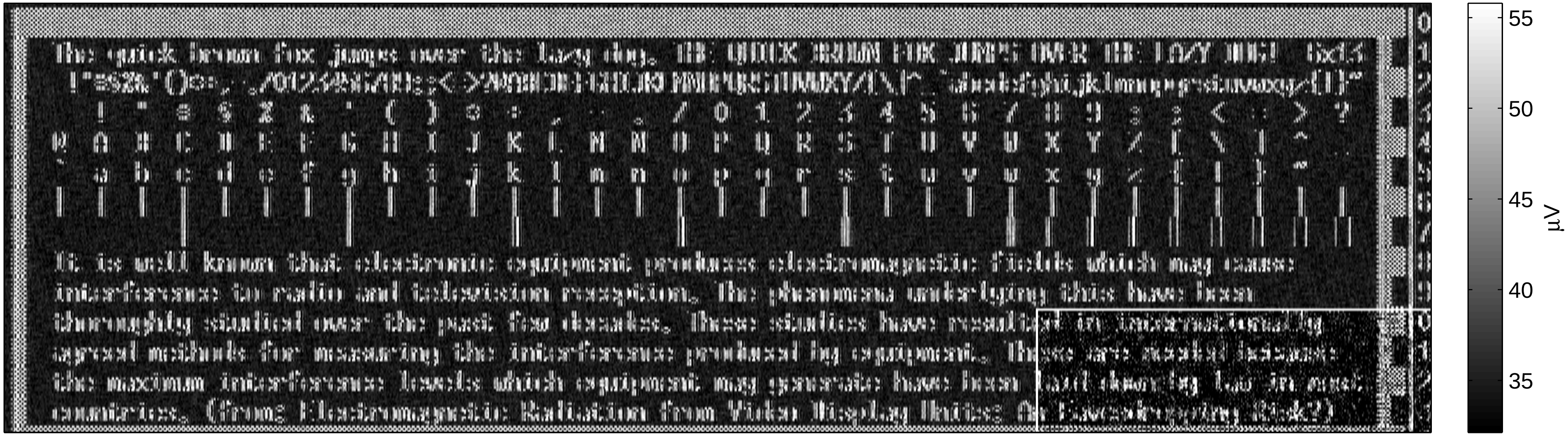
292 MHz center frequency, 20 MHz bandwidth, 256 (16) frames averaged, 3 m distance



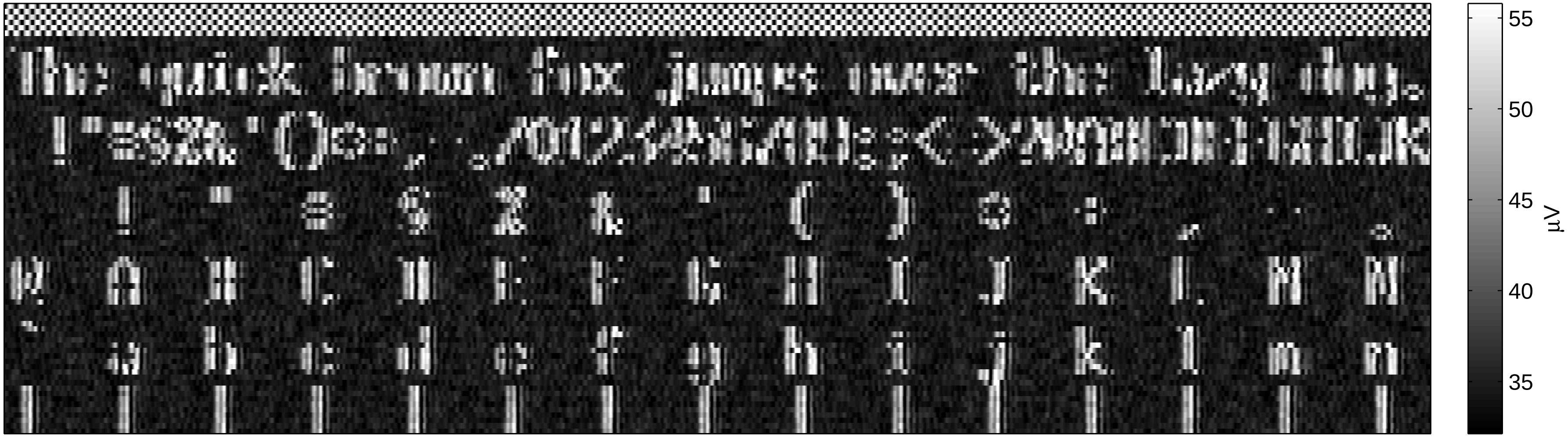
292 MHz center frequency, 10 MHz bandwidth, 256 (16) frames averaged, 3 m distance

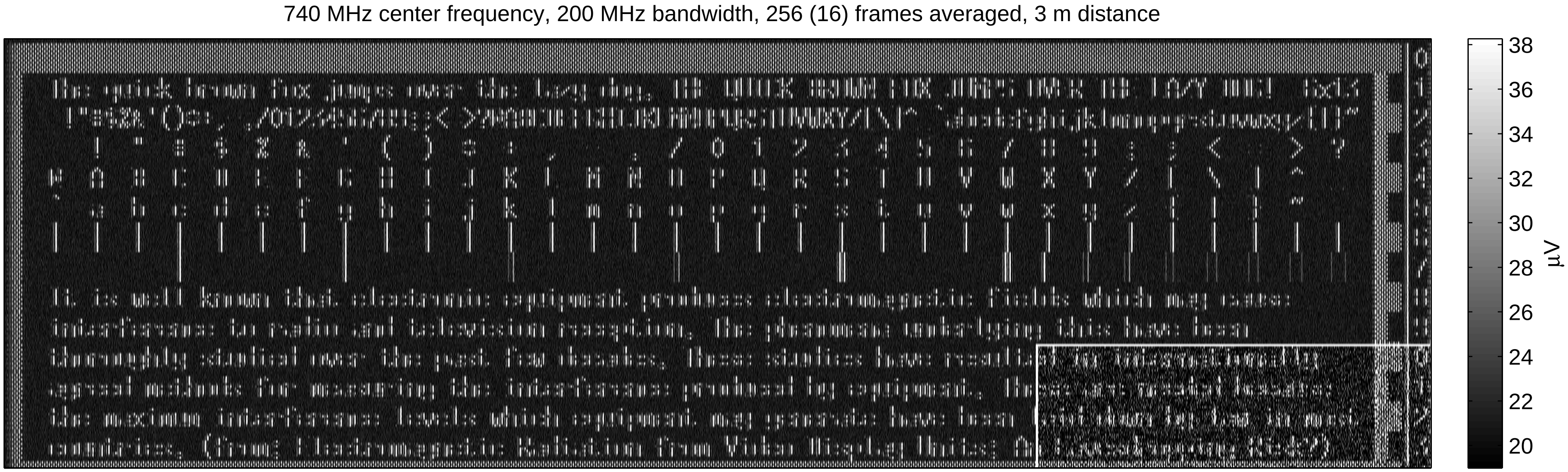


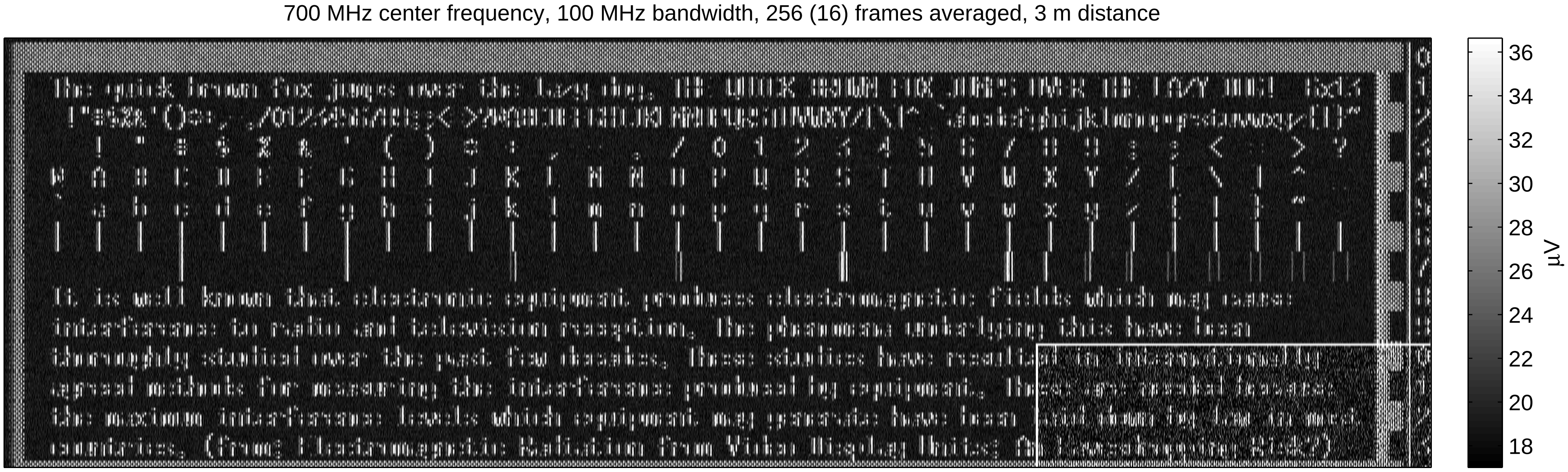
480 MHz center frequency, 50 MHz bandwidth, 256 (16) frames averaged, 3 m distance


The quick brown fox jumps over the lazy dog. THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG! 6x13
It is well known that electronic equipment produces electromagnetic 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?)
55
50
45
40
35
µV

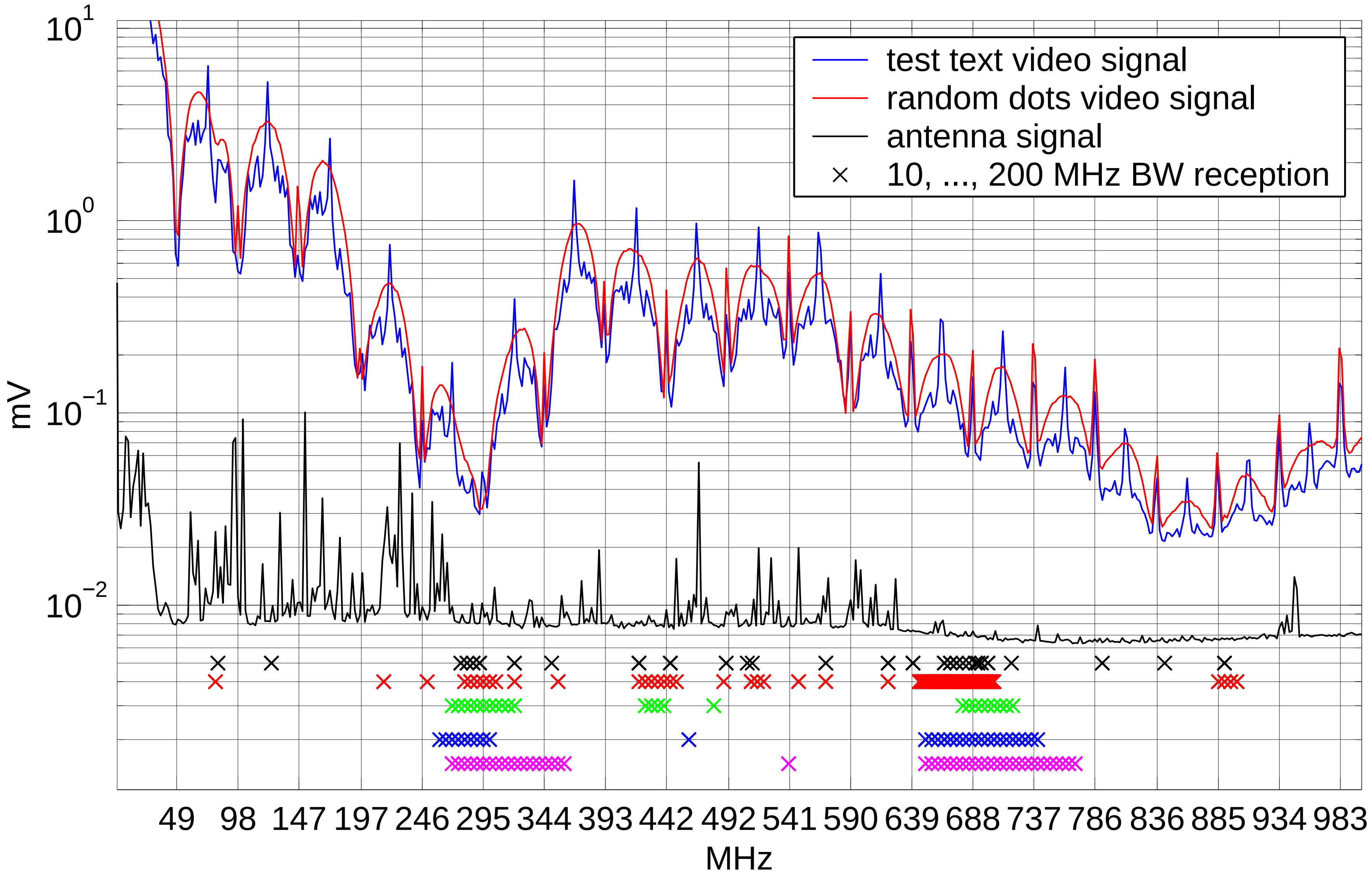
480 MHz center frequency, 50 MHz bandwidth, magnified image section



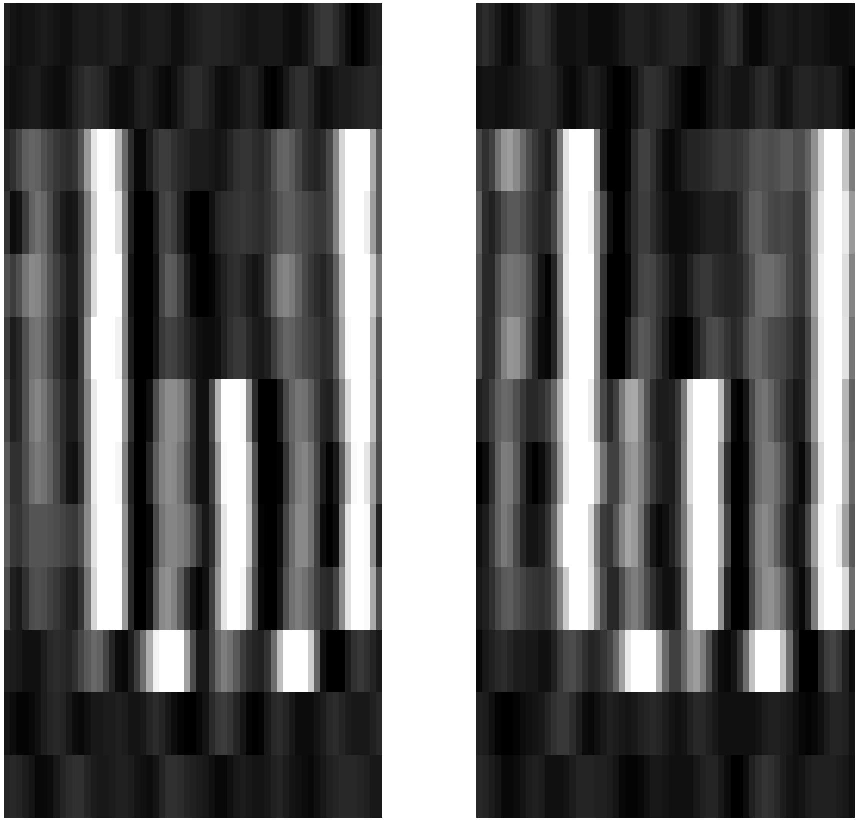

740 MHz center frequency, 200 MHz bandwidth, 256 (16) frames averaged, 3 m distance


700 MHz center frequency, 100 MHz bandwidth, 256 (16) frames averaged, 3 m distance

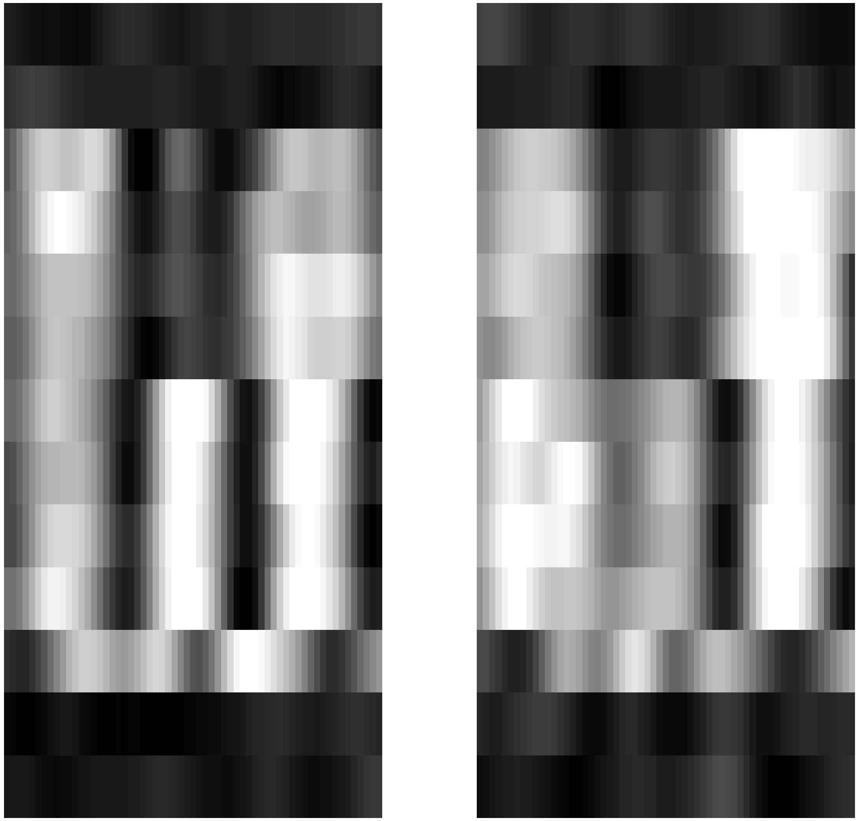
Background noise and reception frequency



Bandwidth and inter-character interference



200 MHz BW



50 MHz BW

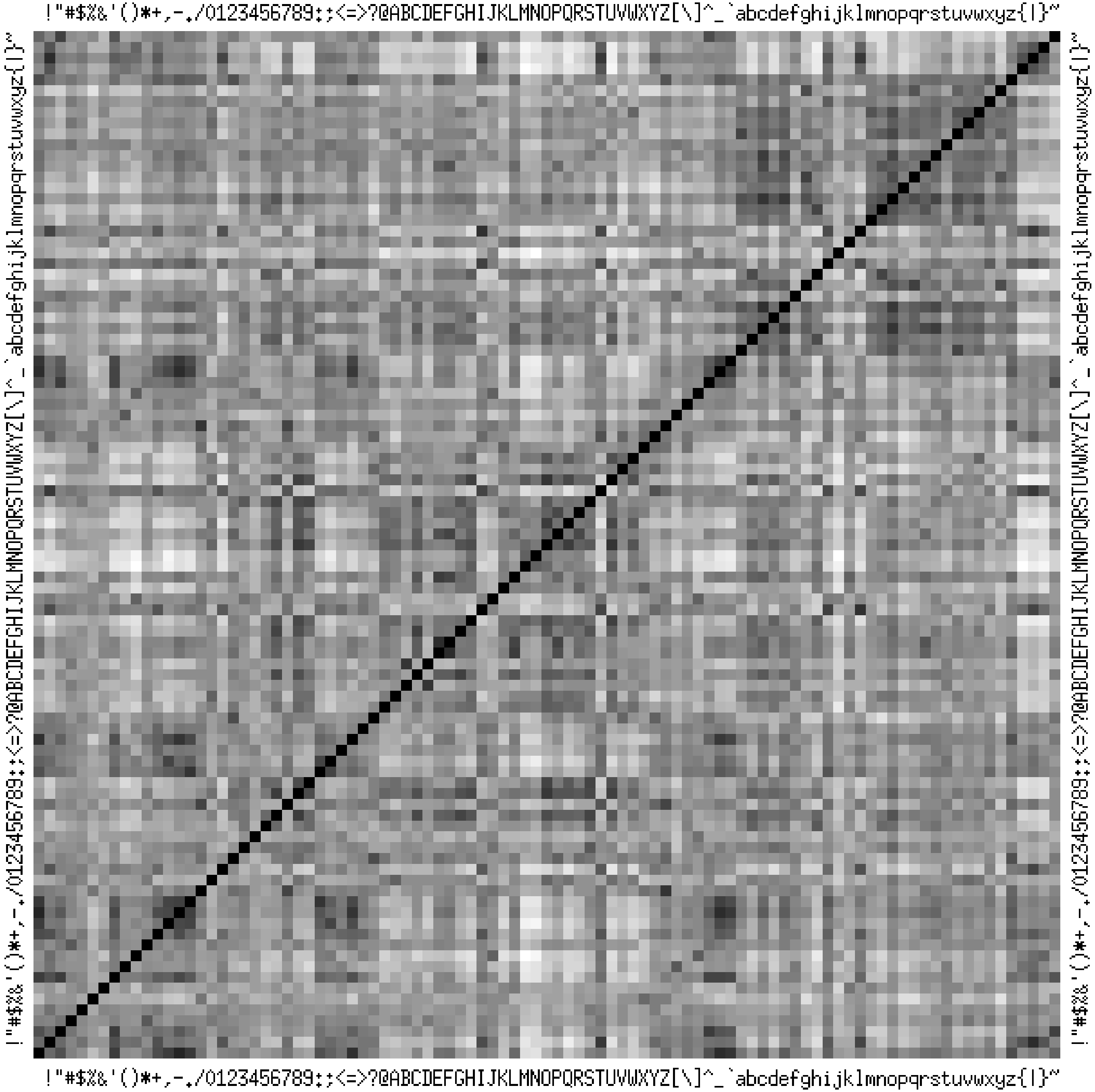
Automatic Radio Character Recognition

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?)
```

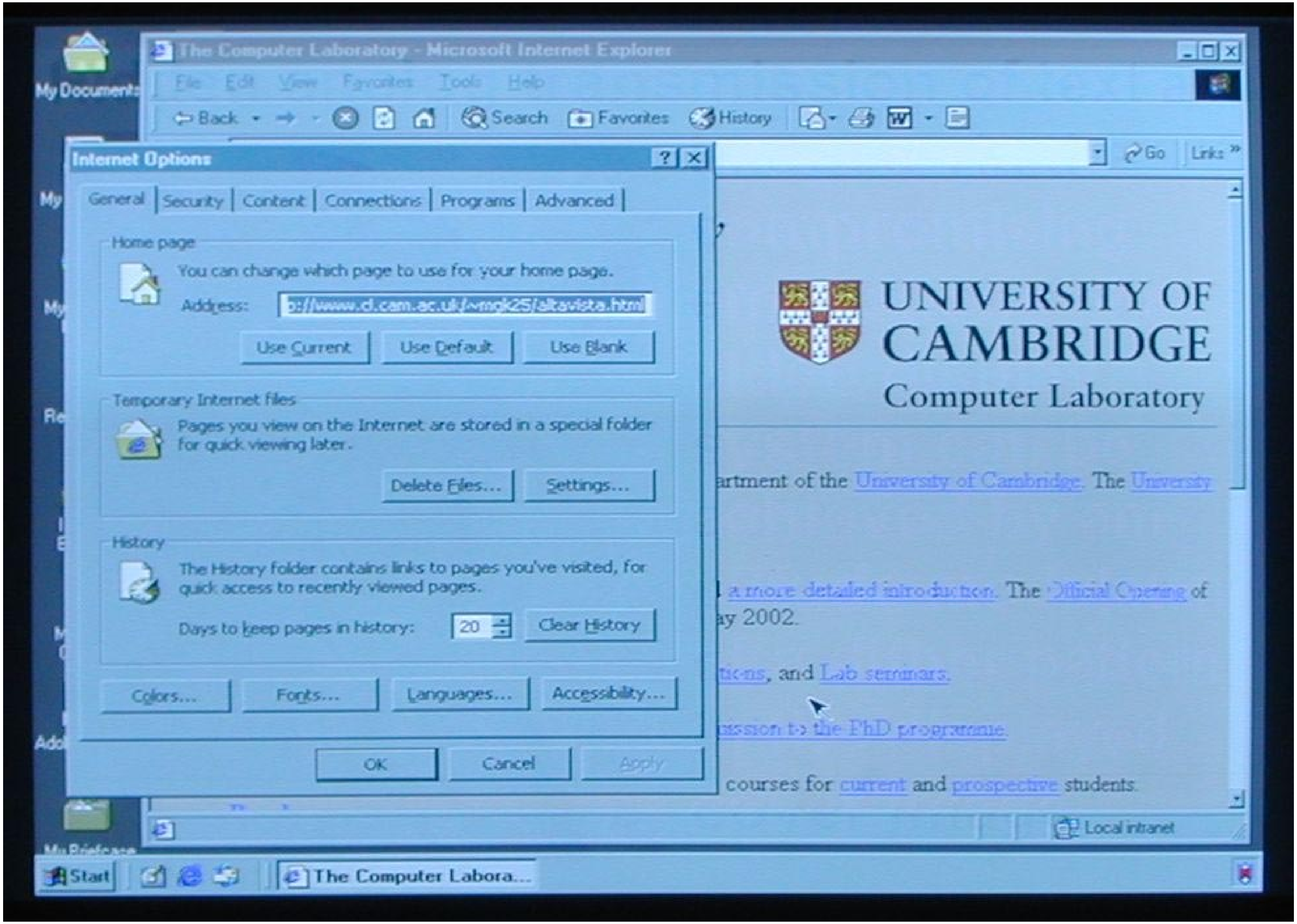
With only 16 frames averaged:

```
  Ihc quick bcown fox_jumps-evec-toe Iazg dsg_=TOE_QHICK-DROWM-EHX JUHPS Q?ER iUE LOZY DH6! -6zi3=
   !"#$%&'()* ,-=ZO!?3‘56709:;< >?@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?)-
```


!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~

Steganographic transmission of images

The user sees on her screen:



Home page

You can change which page to use for your home page.

Address: p://www.cl.cam.ac.uk/~mgk25/altavista.html

Temporary Internet files

Pages you view on the Internet are stored in a special folder for quick viewing later.

History

The History folder contains links to pages you've visited, for quick access to recently viewed pages.

Days to keep pages in history: 20

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

artment of the University of Cambridge. The University

a more detailed introduction. The Official Opening of

ay 2002.

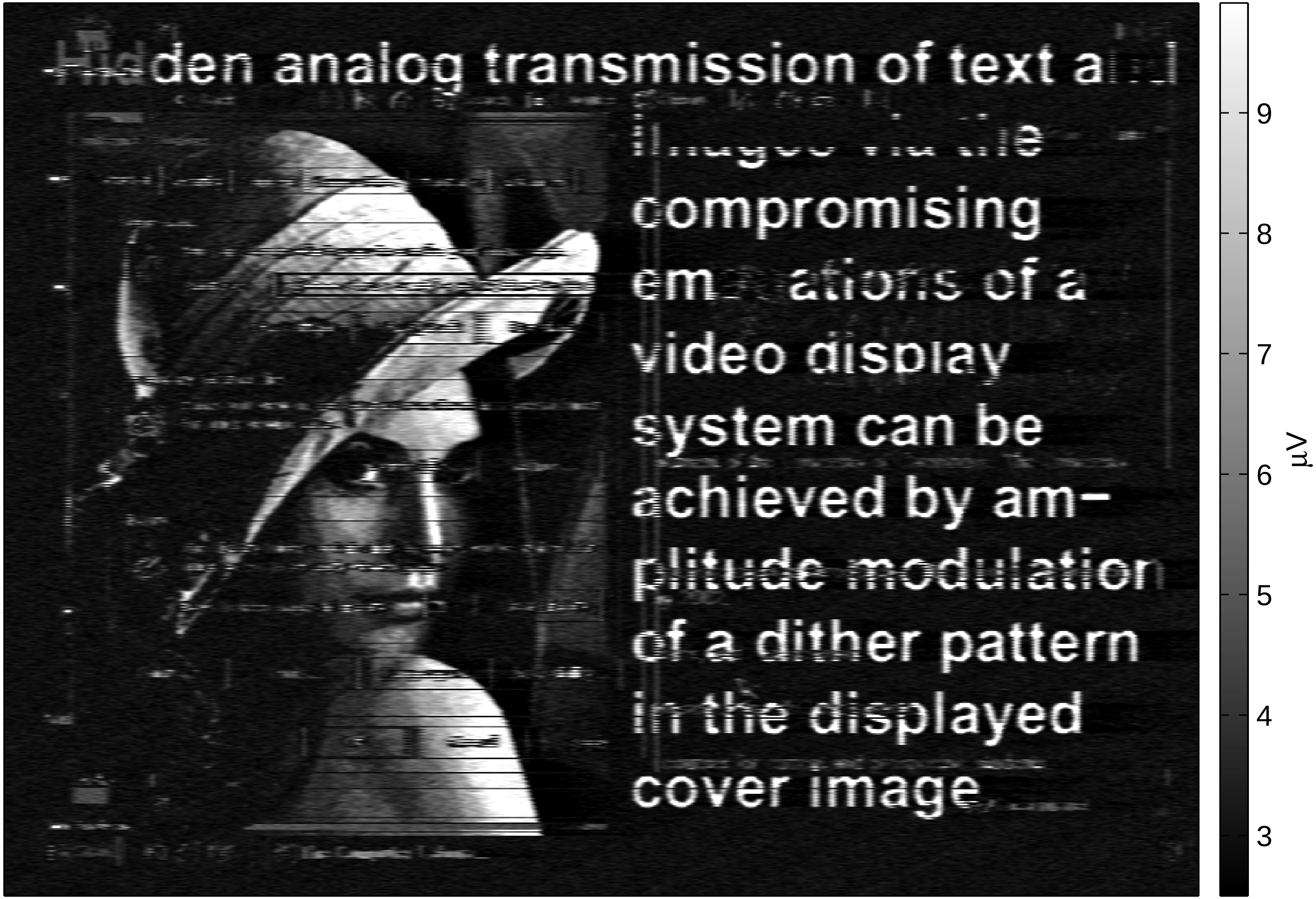
tions, and Lab seminars.

ission to the PhD programme.

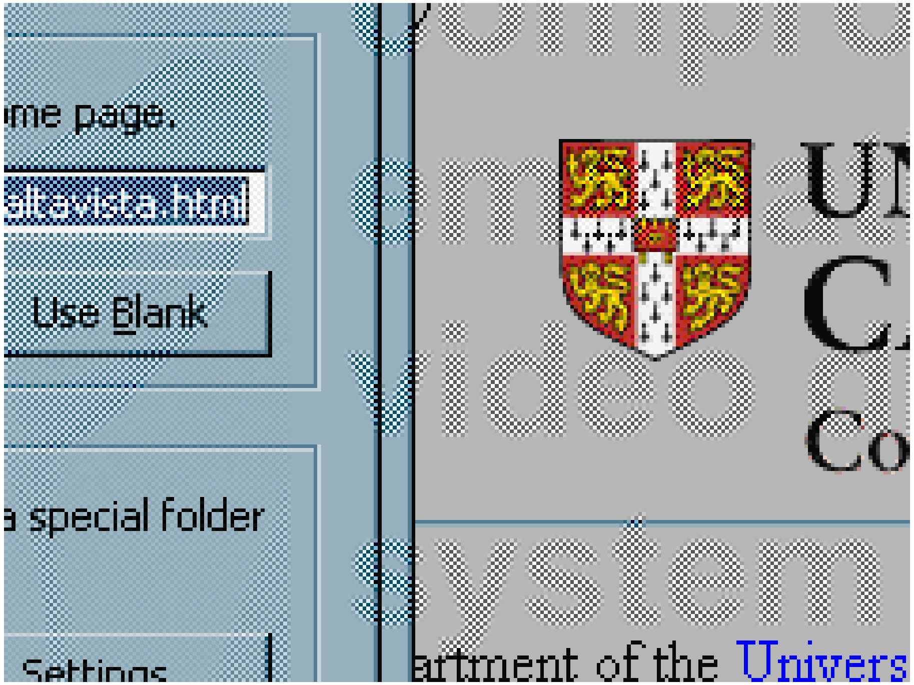
courses for current and prospective students.

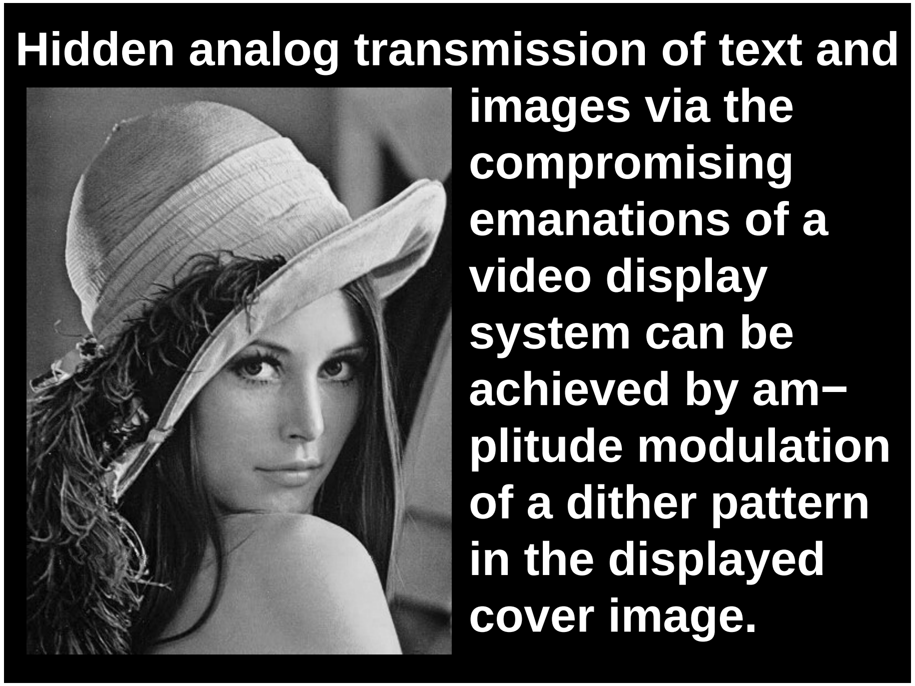
The radio frequency eavesdropper receives instead:

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



Amplitude modulation of dither patterns





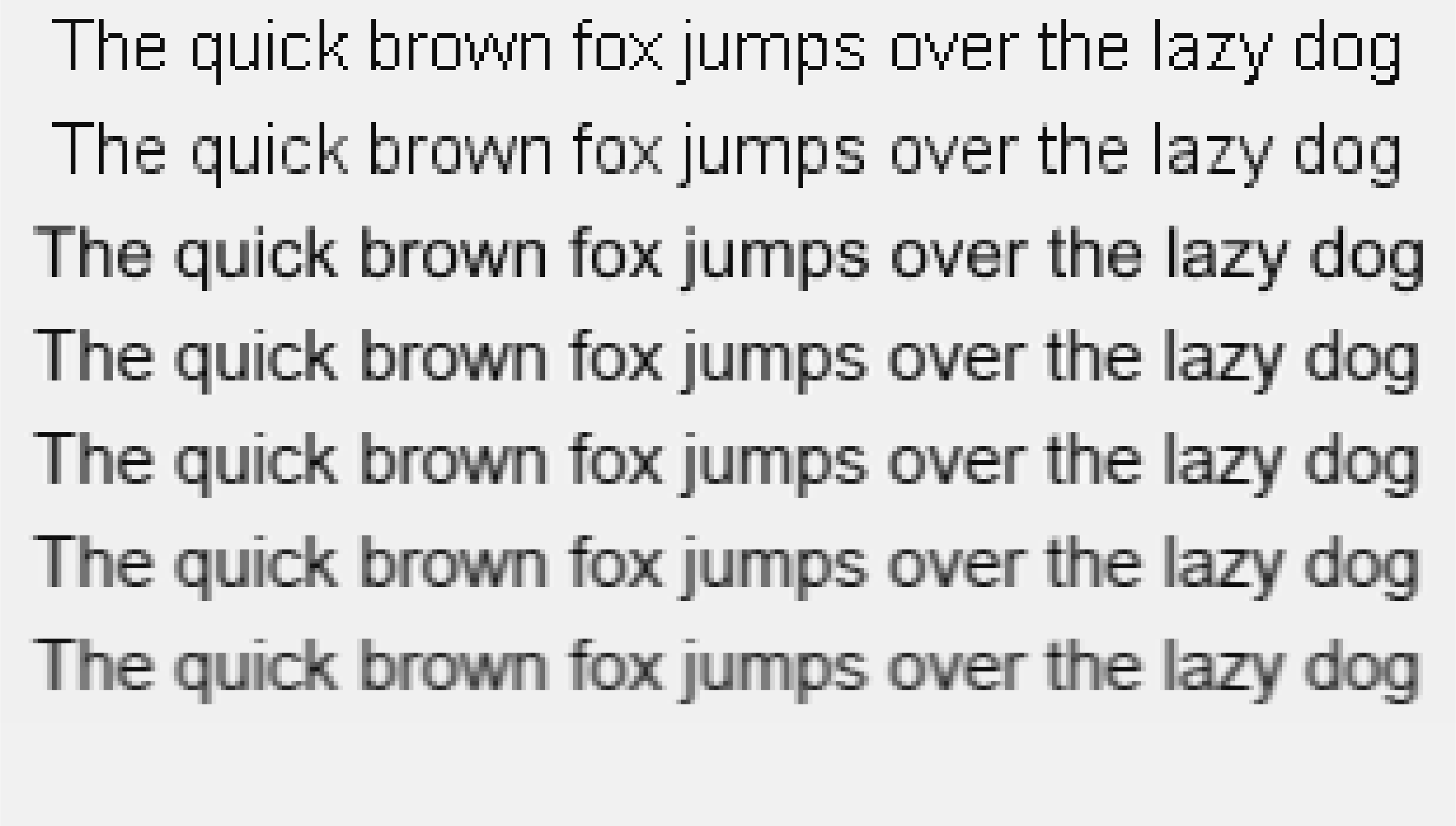
Hidden analog transmission of text and images via the compromising emanations of a video display system can be achieved by amplitude modulation of a dither pattern in the displayed cover image.

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



The quick brown fox jumps over the lazy dog

The quick brown fox jumps over the lazy dog

The quick brown fox jumps over the lazy dog

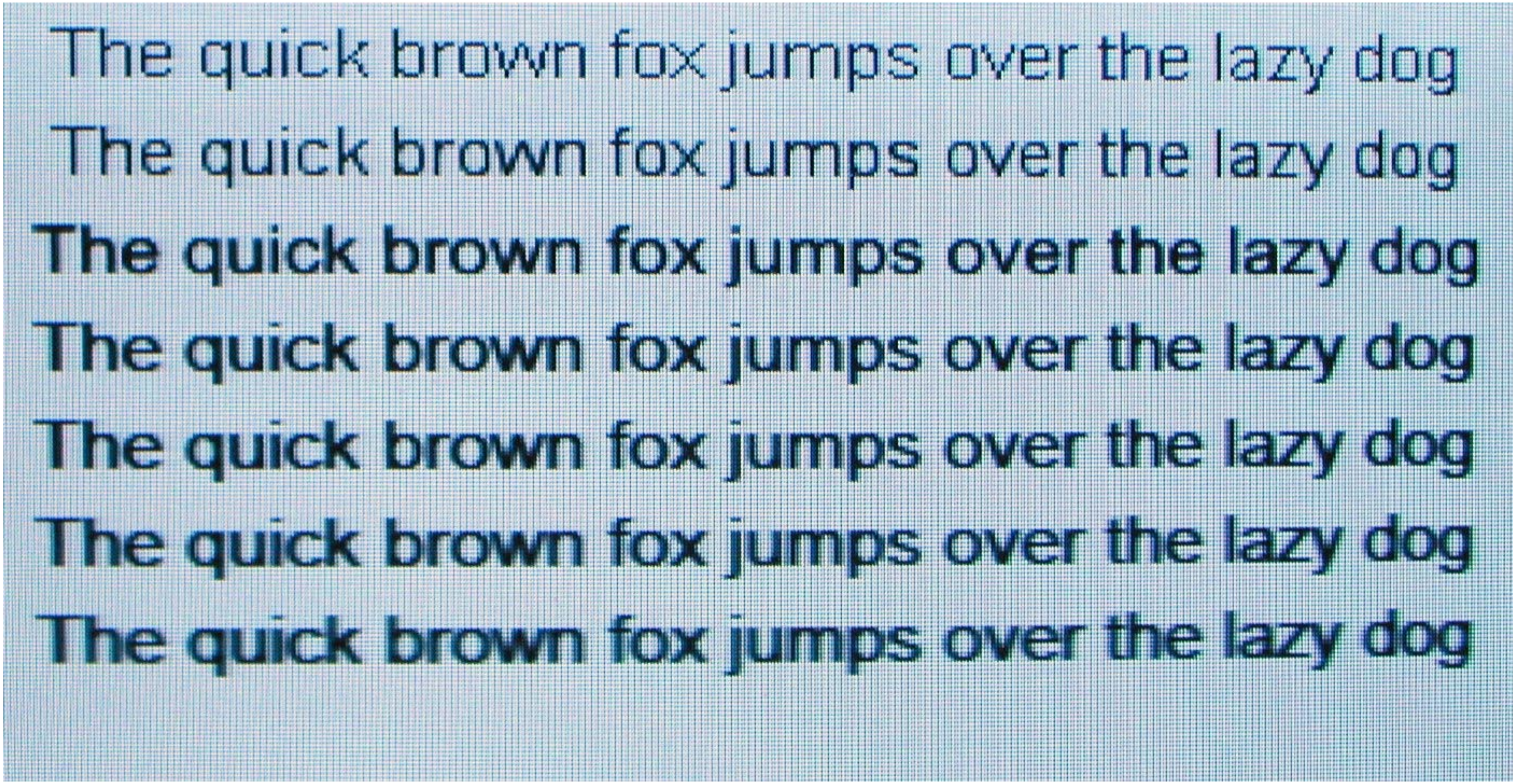
The quick brown fox jumps over the lazy dog

The quick brown fox jumps over the lazy dog

The quick brown fox jumps over the lazy dog

The quick brown fox jumps over the lazy dog

Filtered fonts on the CRT screen



The quick brown fox jumps over the lazy dog

The quick brown fox jumps over the lazy dog

The quick brown fox jumps over the lazy dog

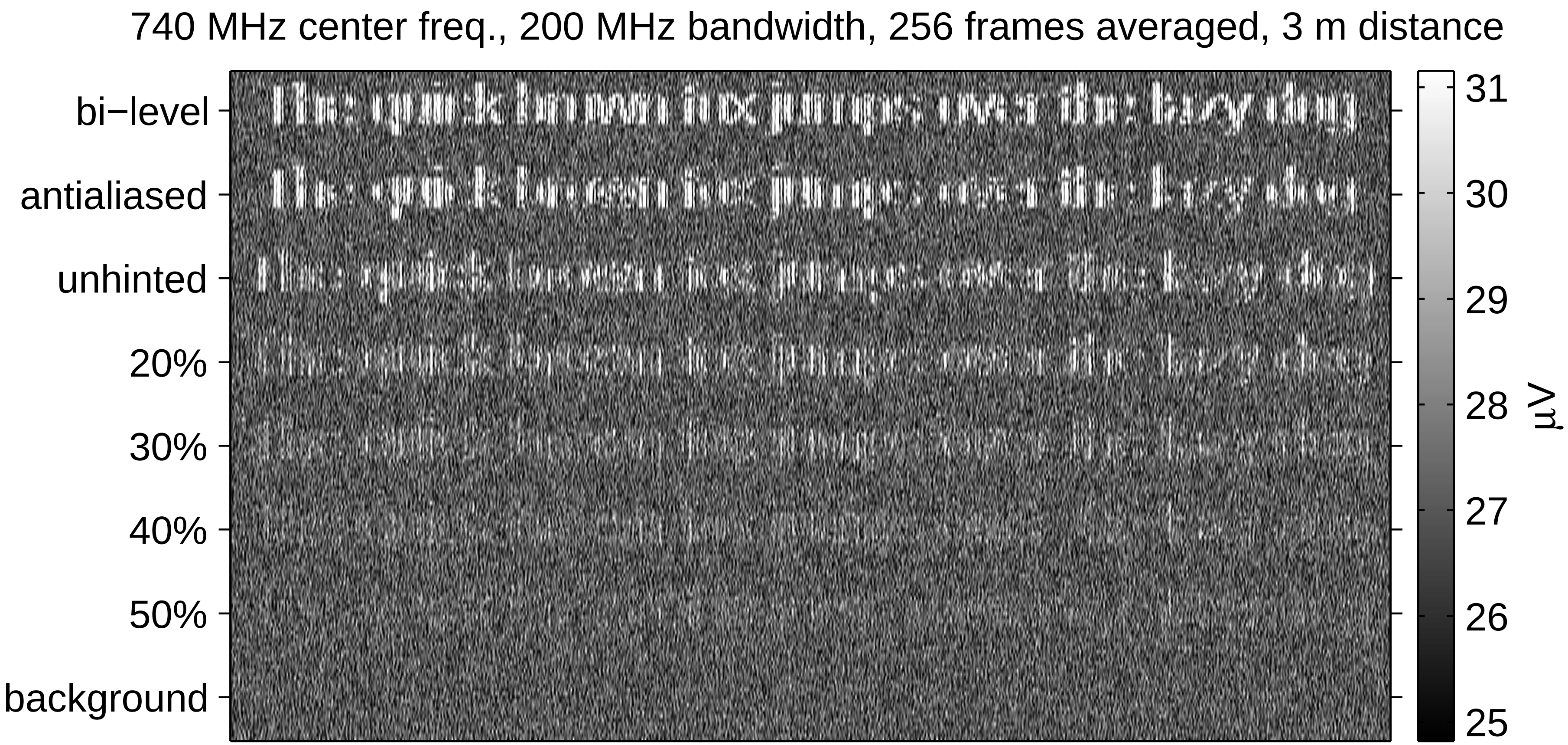
The quick brown fox jumps over the lazy dog

The quick brown fox jumps over the lazy dog

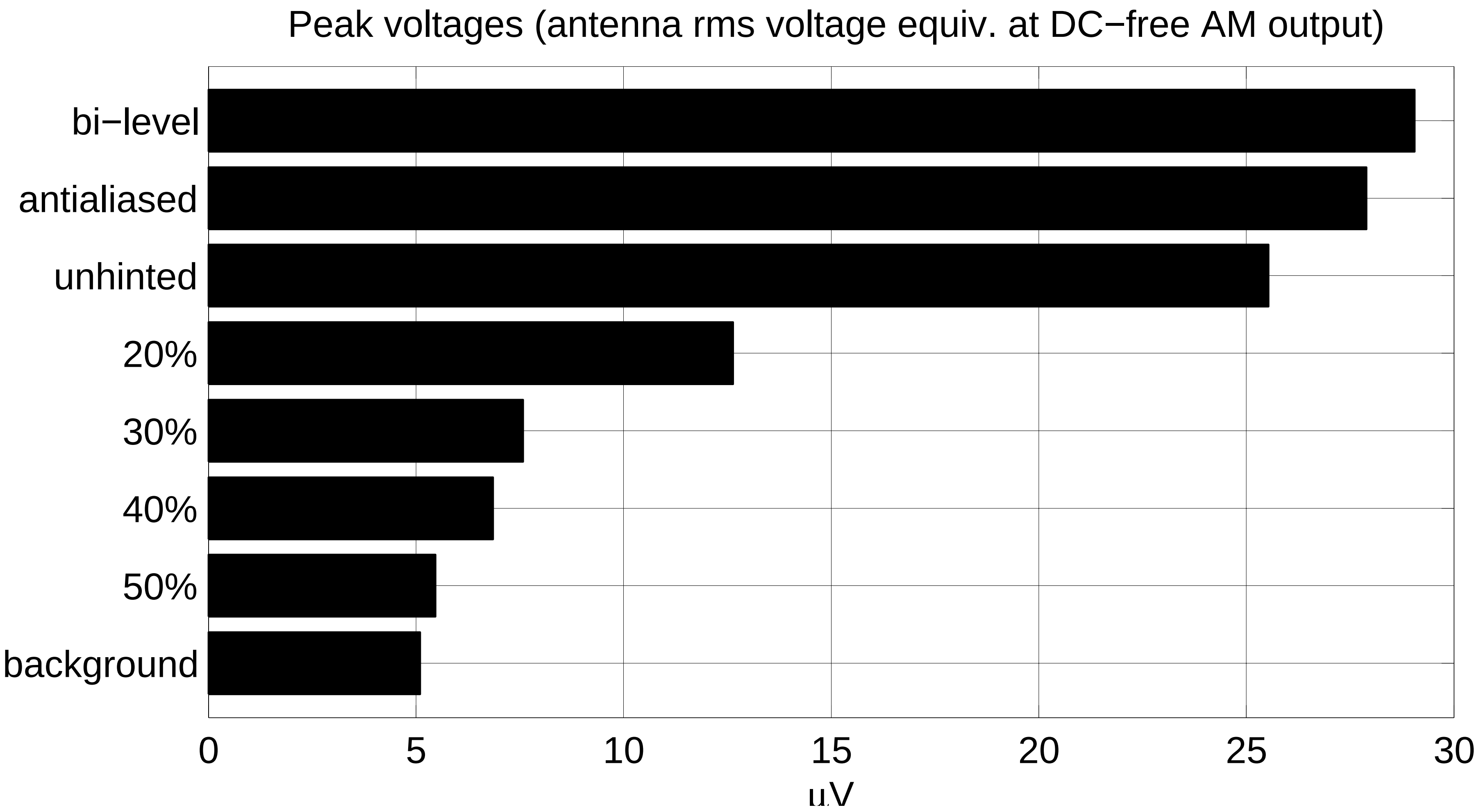
The quick brown fox jumps over the lazy dog

The quick brown fox jumps over the lazy dog

Received radio signal

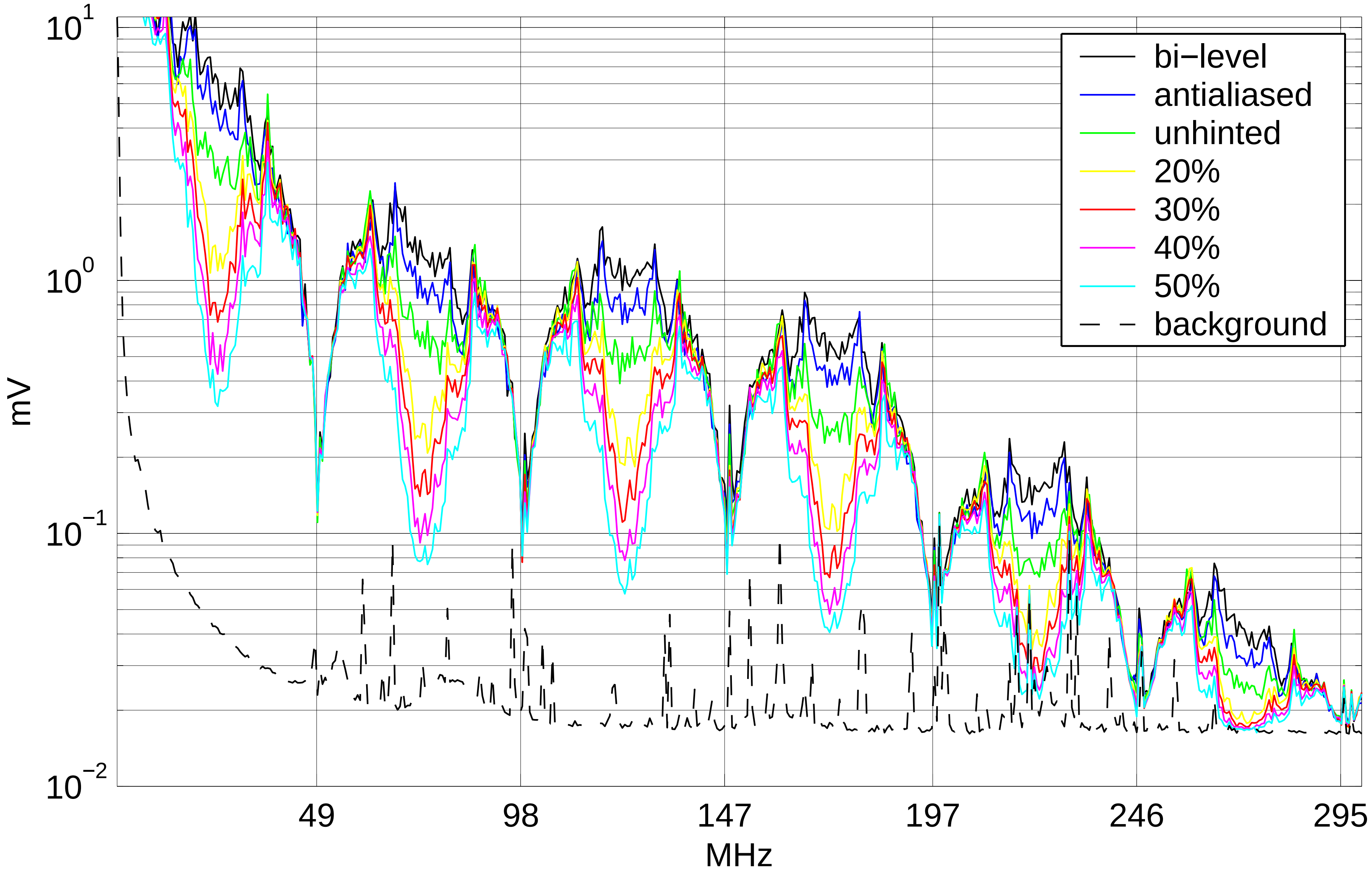


Filtered fonts peak-amplitude comparison



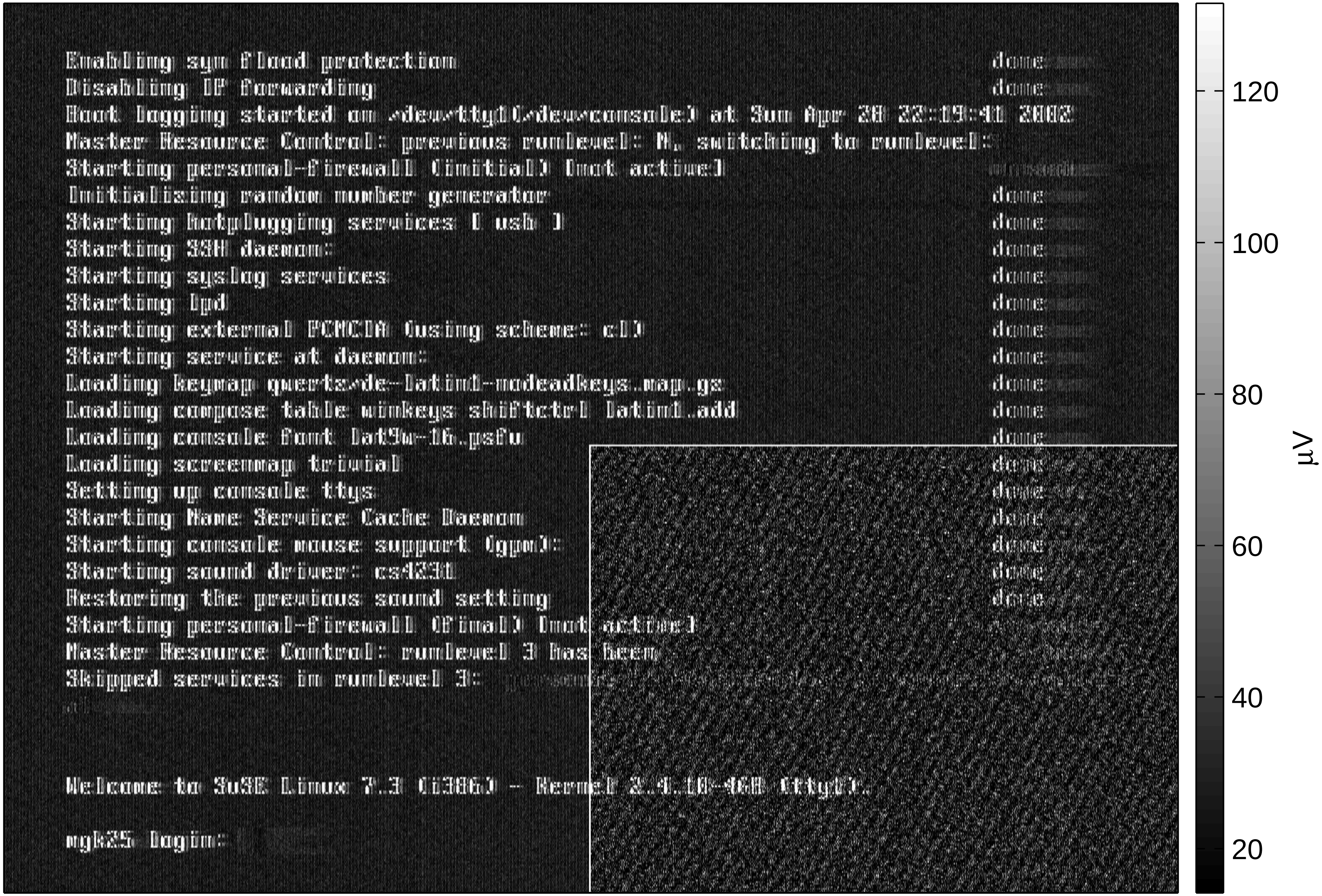
Removing the top 30 % of the spectrum reduces peak emissions by 12 dB, without significantly affecting user comfort. This means the eavesdropper has to come $3\times$ closer, into a $10\times$ smaller area.

Spectral effects of font filtering

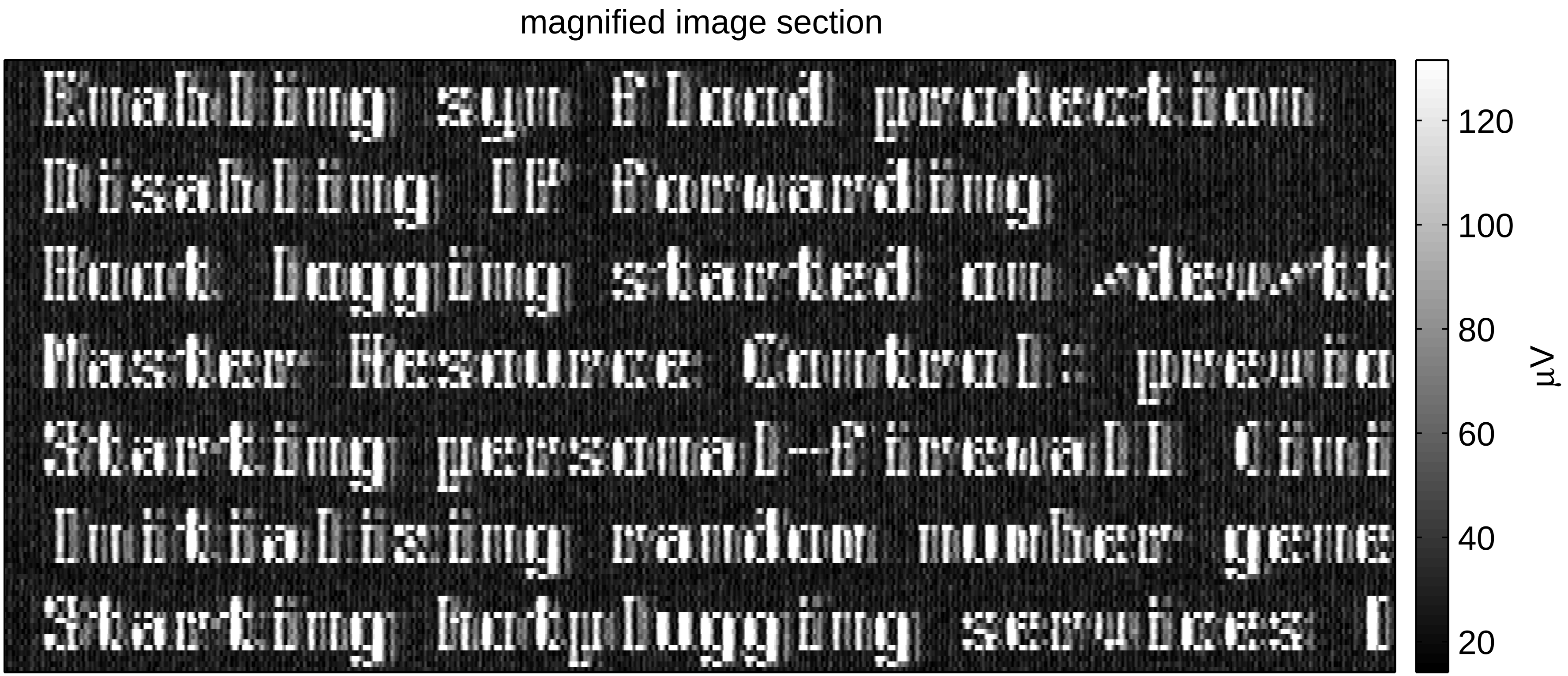


Eavesdropping on flat panel displays

350 MHz center frequency, 50 MHz bandwidth, 16 (1) frames averaged, 3 m distance



```
Enabling syn flood protection                                                   done
Disabling IP forwarding                                                         done
Boot logging started on /dev/tty1(/dev/console) at Sun Apr 28 22:19:41 2002
Master Resource Control: previous runlevel: N, switching to runlevel:
Starting personal-firewall (initial) [not active]
Initializing random number generator                                            done
Starting hotplugging services [ usb ]                                           done
Starting SSH daemon:                                                            done
Starting syslog services                                                        done
Starting lpd                                                                    done
Starting external PCMCIA (using scheme: c1)                                     done
Starting service at daemon:                                                     done
Loading keymap qwertz/de-latin1-nodeadkeys.map.gz                               done
Loading compose table winkeys shiftctrl latin1.add                              done
Loading console font lat9w-16.psfu                                              done
Loading screenmap trivial                                                       done
Setting up console ttys                                                         done
Starting Name Service Cache Daemon                                              done
Starting console mouse support (gpm):                                           done
Starting sound driver: cs4231                                                   done
Restoring the previous sound setting                                            done
Starting personal-firewall (final) [not active]
Master Resource Control: runlevel 3 has been
Skipped services in runlevel 3:


Welcome to SuSE Linux 7.3 (i386) - Kernel 2.4.10-4GB (tty1).

mgk25 login:
```



magnified image section

```
Enabling syn flood protection
Disabling IP Forwarding
Boot logging started on /dev/tt
Master Resource Control: previo
Starting personal-firewall (ini
Initializing random number gene
Starting hotplugging services [
```

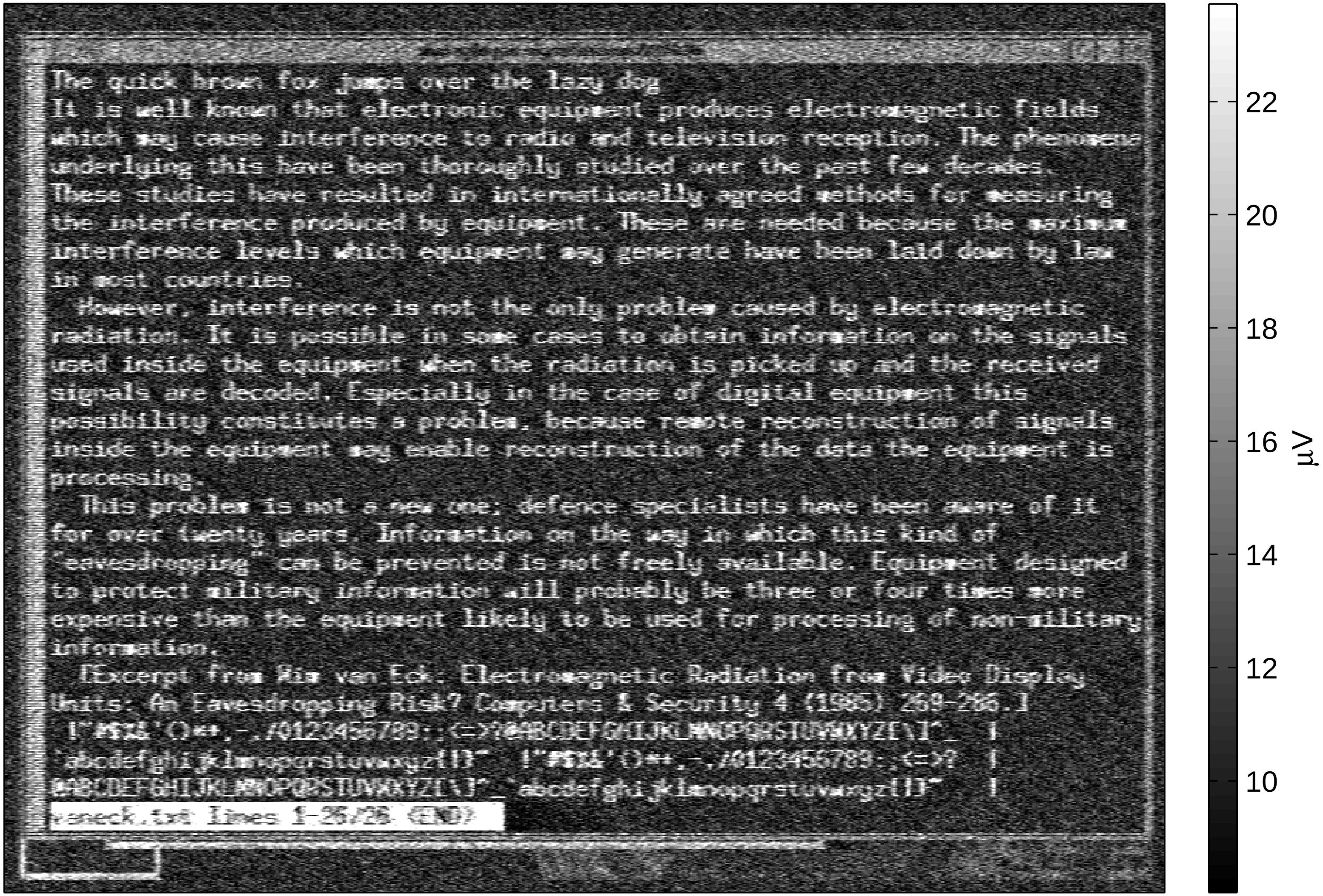
→ 100 μV signal amplitude at receiver input (rms equiv.)

→ 57 dBμV/m (50 MHz BW) field strength at 3 m distance

→ equivalent isotropic radiated power around 150 nW

Eavesdropping across two office rooms

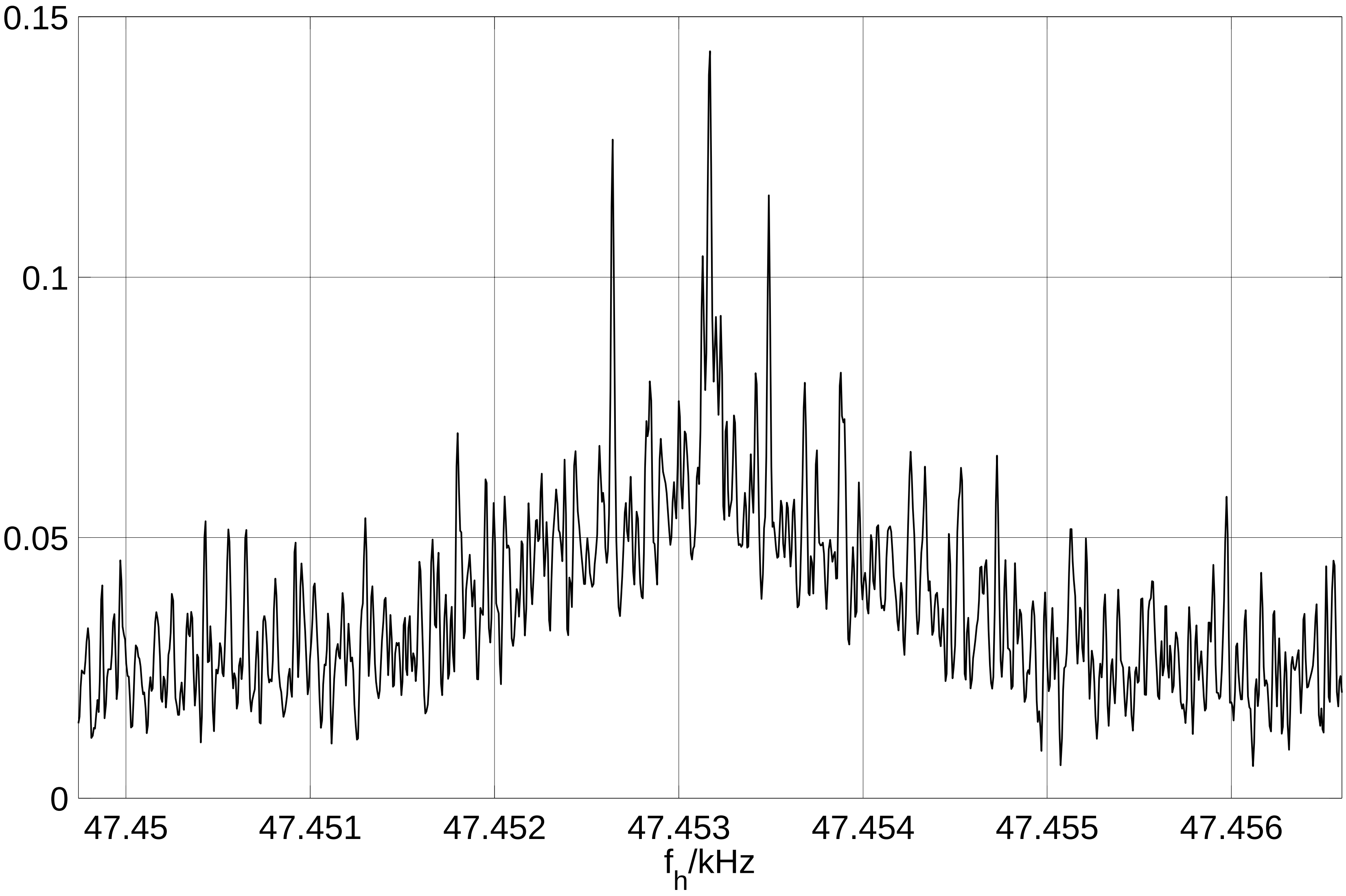
350 MHz, 50 MHz BW, 12 frames (160 ms) averaged



```
The quick brown fox jumps over the lazy dog
It is well known that electronic equipment produces electromagnetic 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.
  However, interference is not the only problem caused by electromagnetic
radiation. It is possible in some cases to obtain information on the signals
used inside the equipment when the radiation is picked up and the received
signals are decoded. Especially in the case of digital equipment this
possibility constitutes a problem, because remote reconstruction of signals
inside the equipment may enable reconstruction of the data the equipment is
processing.
  This problem is not a new one; defence specialists have been aware of it
for over twenty years. Information on the way in which this kind of
"eavesdropping" can be prevented is not freely available. Equipment designed
to protect military information will probably be three or four times more
expensive than the equipment likely to be used for processing of non-military
information.
  [Excerpt from Wim van Eck: Electromagnetic Radiation from Video Display
Units: An Eavesdropping Risk? Computers & Security 4 (1985) 269-286.]
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_  |
`abcdefghijklmnopqrstuvwxyz{|}~  !"#$%&'()*+,-./0123456789:;<=>?  |
@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~   |
vaneck.txt lines 1-26/26 (END)
```

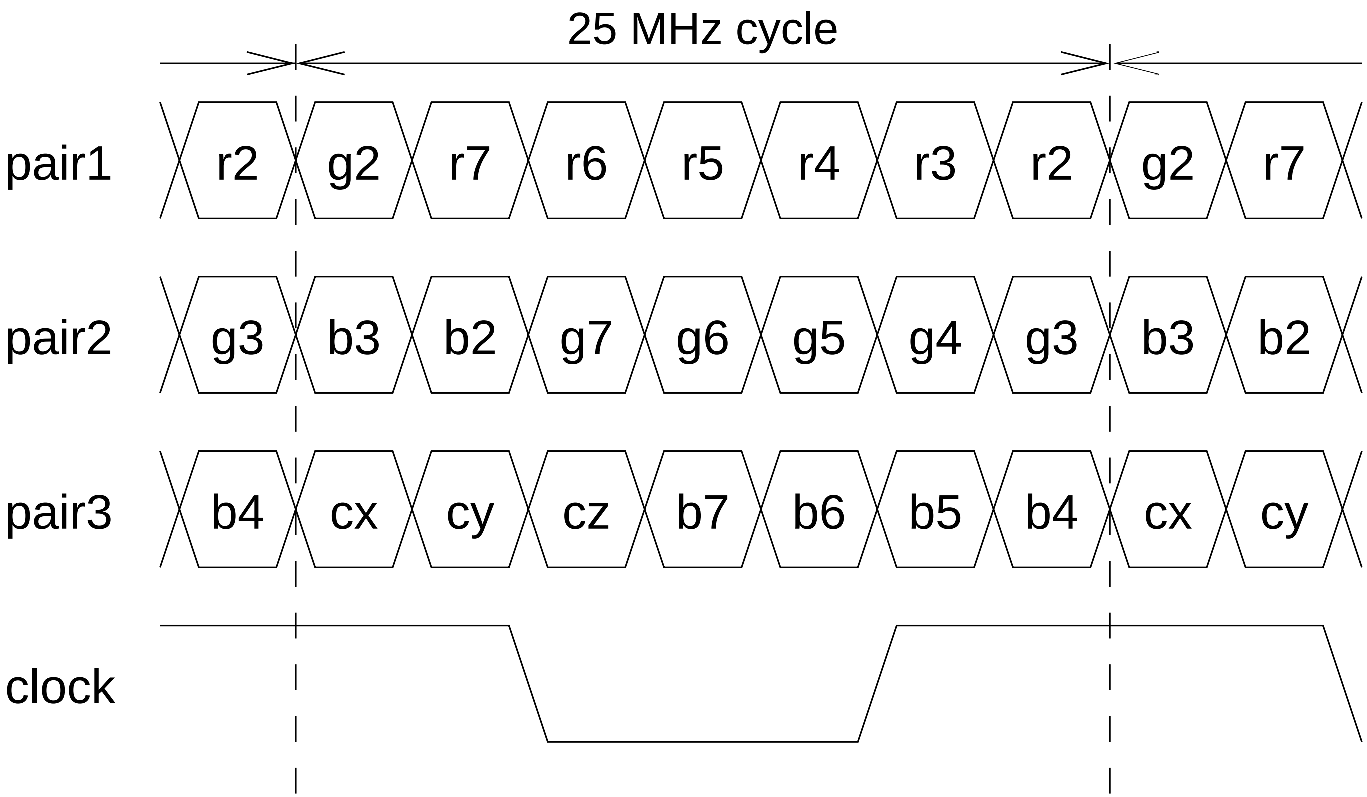
Target in room GE16 and antenna in room GE10 of the William Gates building, with two offices and three plasterboard walls (−2.7 dB each) in between.

Remote video timing estimation via cross-correlation



FPD-Link – a digital video interface

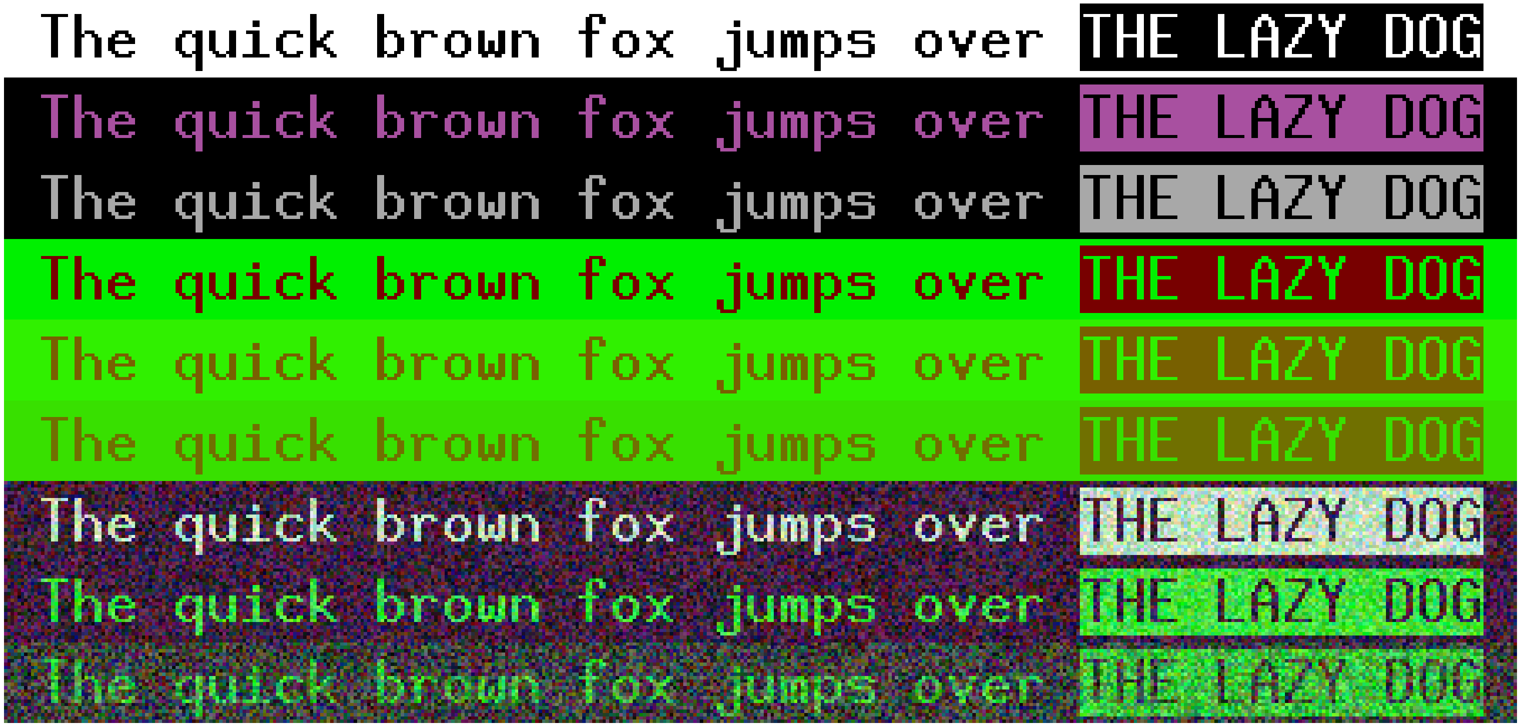
LCD module and video controller are connected in Toshiba 440CDX laptop by eight twisted pairs (each 30 cm), which feed the 18-bit RGB parallel signal through the hinges via low-voltage differential signaling (LVDS, EIA-644).



Minimal/maximal reception contrast

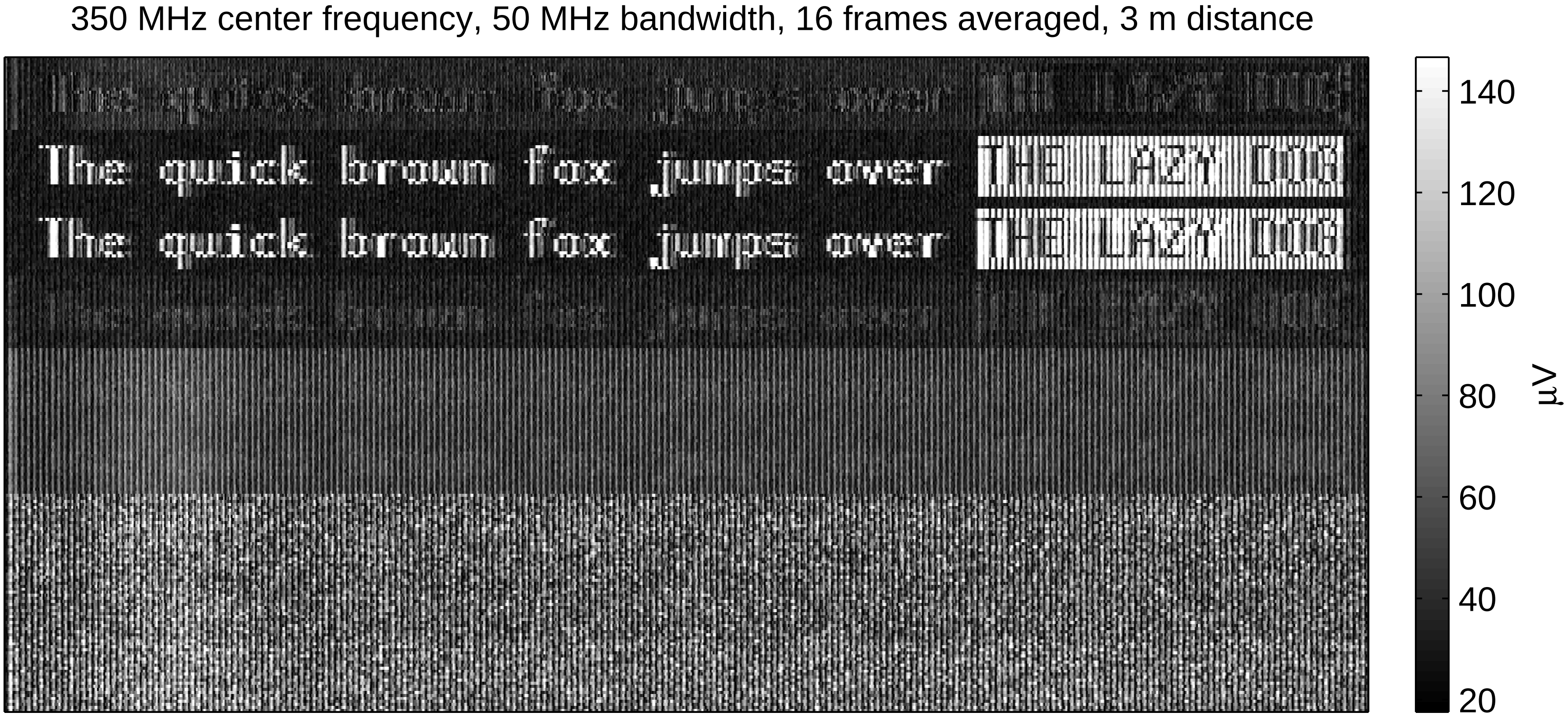
		foreground		background	
line	description	RGB	signal	RGB	signal
1	black on white	00 00 00	000000x 0x00000 xxx0000	ff ff ff	111111X 1X11111 xxx1111
2	maximum contrast	a8 50 a0	010101x 0x01010 xxx1010	00 00 00	000000x 0x00000 xxx0000
3	maximum contrast (gray)	a8 a8 a8	010101x 1x10101 xxx1010	00 00 00	000000x 0x00000 xxx0000
4	minimum contrast	78 00 00	001111x 0x00000 xxx0000	00 f0 00	000000x 0x11110 xxx0000
5	minimum contrast	78 60 00	001111x 0x01100 xxx0000	30 f0 00	000110x 0x11110 xxx0000
6	minimum contrast (phase shift)	70 70 00	001110x 0x01110 xxx0000	38 e0 00	000111x 0x11100 xxx0000

line	description	foreground		background	
		RGB	signal	RGB	signal
7	text in most significant bit, rest random	—	r1rrrrx rx1rrrr xxx1rrr	—	r0rrrrx rx0rrrr xxx0rrr
8	text in green two msb, rest random	—	rrrrrrx rx11rrr xxxrrrr	—	rrrrrrx rx00rrr xxxrrrr
9	text in green msb, rest random	—	rrrrrrx rx1rrrr xxxrrrr	—	rrrrrrx rx0rrrr xxxrrrr



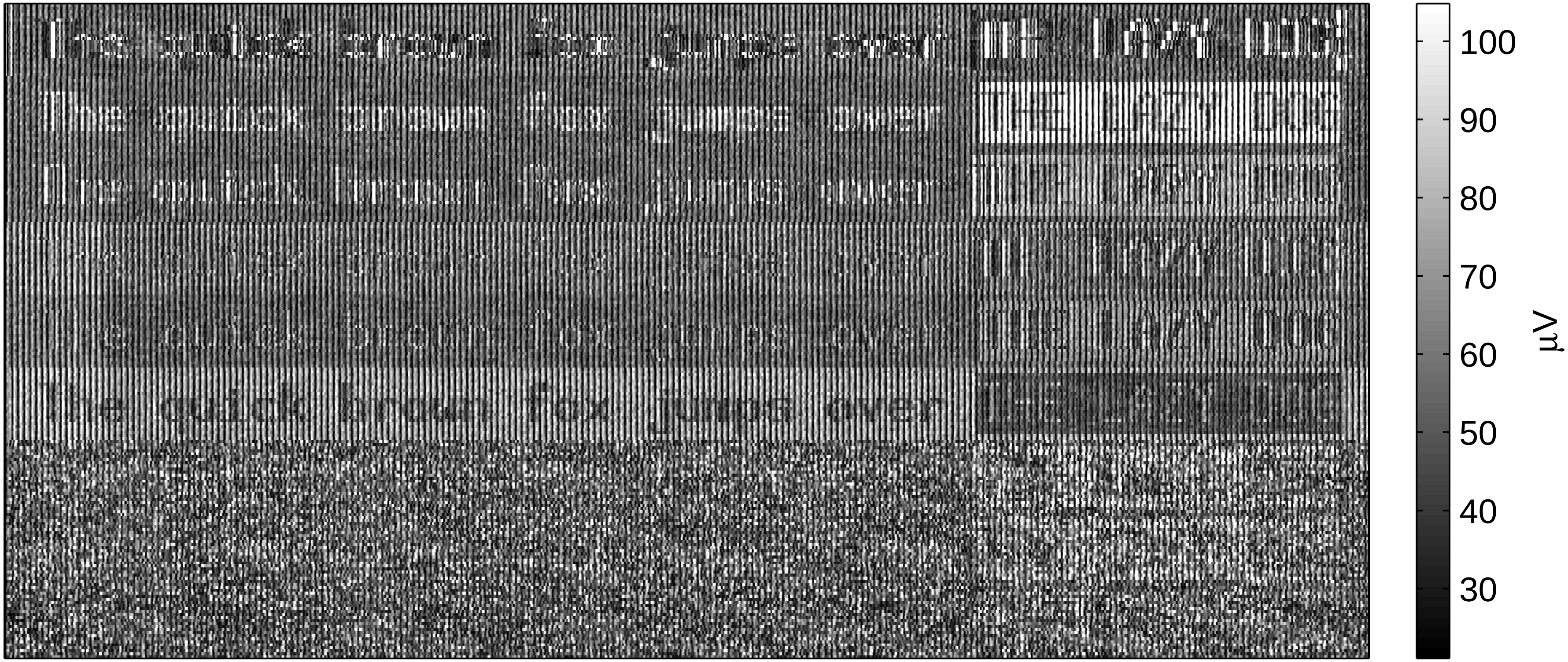
```
The quick brown fox jumps over THE LAZY DOG
The quick brown fox jumps over THE LAZY DOG
The quick brown fox jumps over THE LAZY DOG
The quick brown fox jumps over THE LAZY DOG
The quick brown fox jumps over THE LAZY DOG
The quick brown fox jumps over THE LAZY DOG
The quick brown fox jumps over THE LAZY DOG
The quick brown fox jumps over THE LAZY DOG
The quick brown fox jumps over THE LAZY DOG
```

Minimal/maximal reception contrast

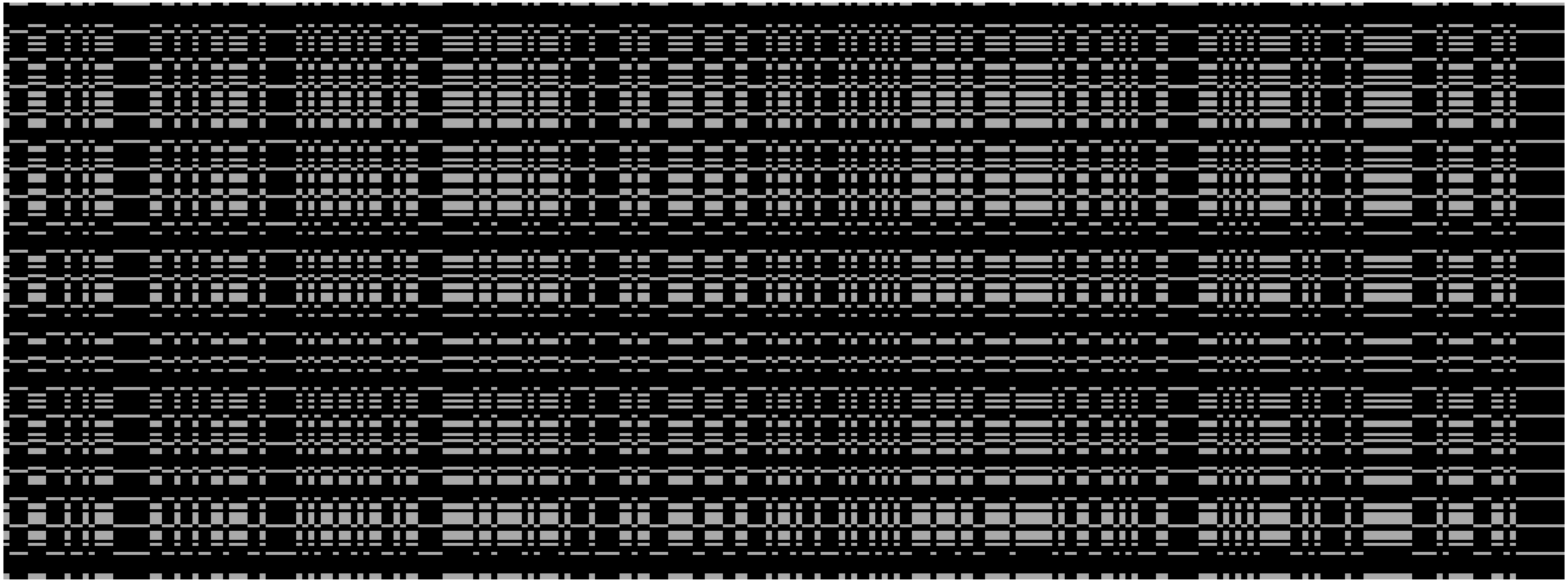


Only random bit jamming effective

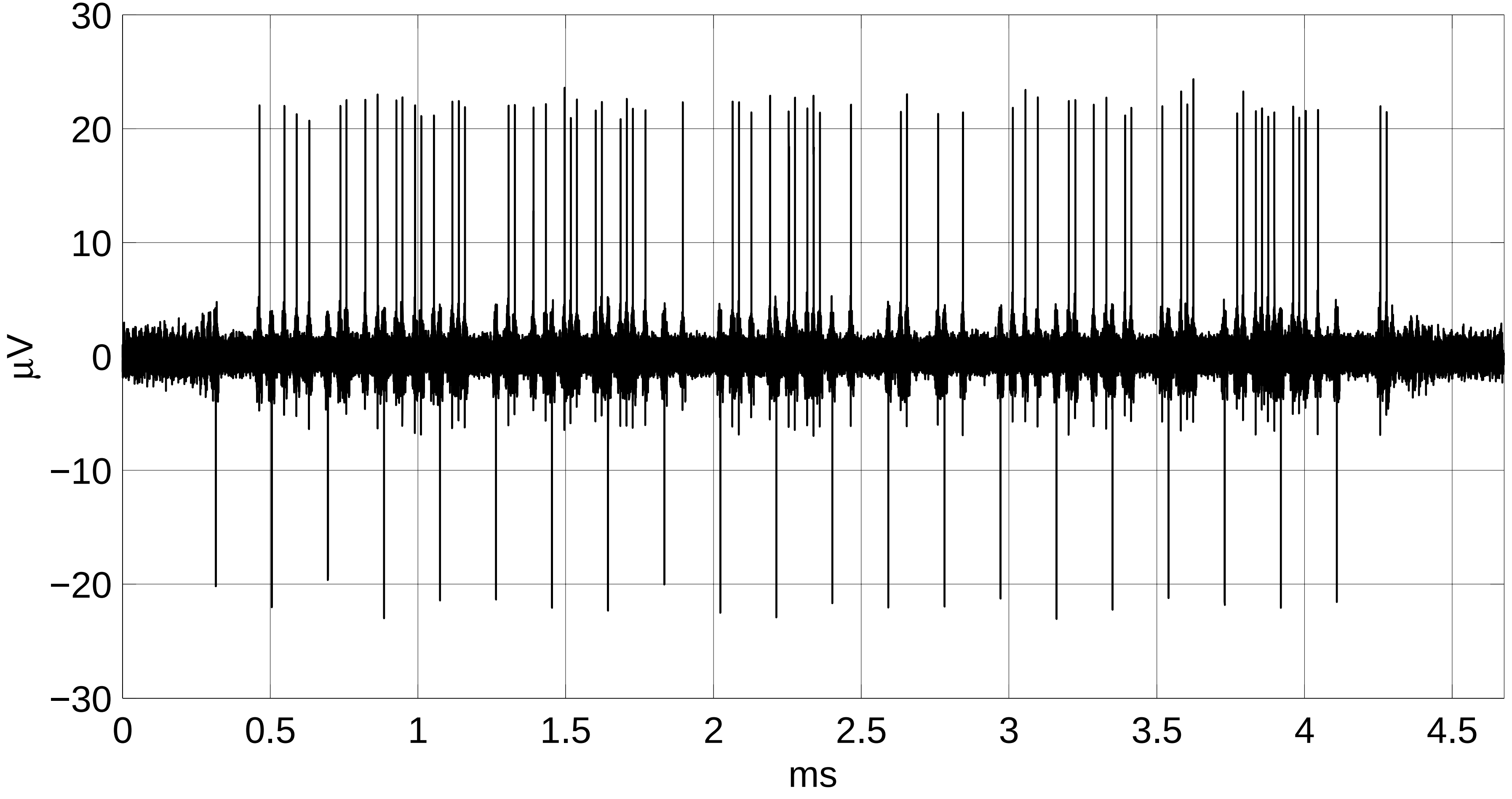
285 MHz center frequency, 50 MHz bandwidth, 16 frames averaged, 3 m distance



Data transmission demonstration



The text "`Tempest in a Teapot`" encoded in ASCII (padded with start- and end-of-text control characters) DSSS-modulated.



Result of convolving the received signal received with the random-bit sequence. Negative peaks mark the start of each byte and positive peaks are the 1 bits (MSB first).

Decoding result: `Tempest in a Teapot`

Transition Minimised Differential Signaling (TMDS)

New industry standard (DVI) for connecting desktop flat-panel displays.

$\longrightarrow$ Differential Gbit/s signaling on three twisted pair channels.

$\longrightarrow$ Coverts byte stream into sequence of 10-bit words.

$\longrightarrow$ Attempts to reduce number of bit transitions.

$\longrightarrow$ Balances the total number of 0 and 1 bits transmitted.

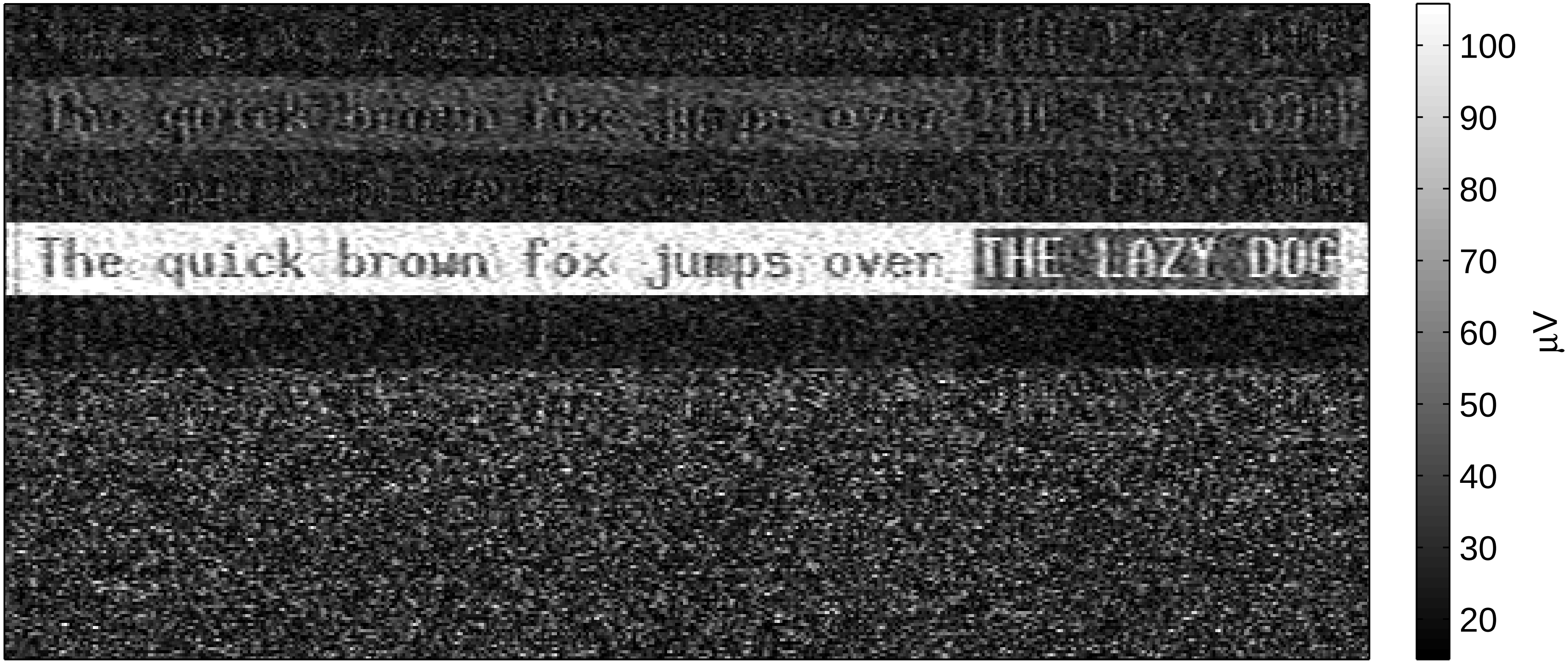
$\longrightarrow$ embeds sync signals using special words.

The DC balancing step adds encoding state and only 52 byte values lead to balanced words that are immune against the balancing algorithm.

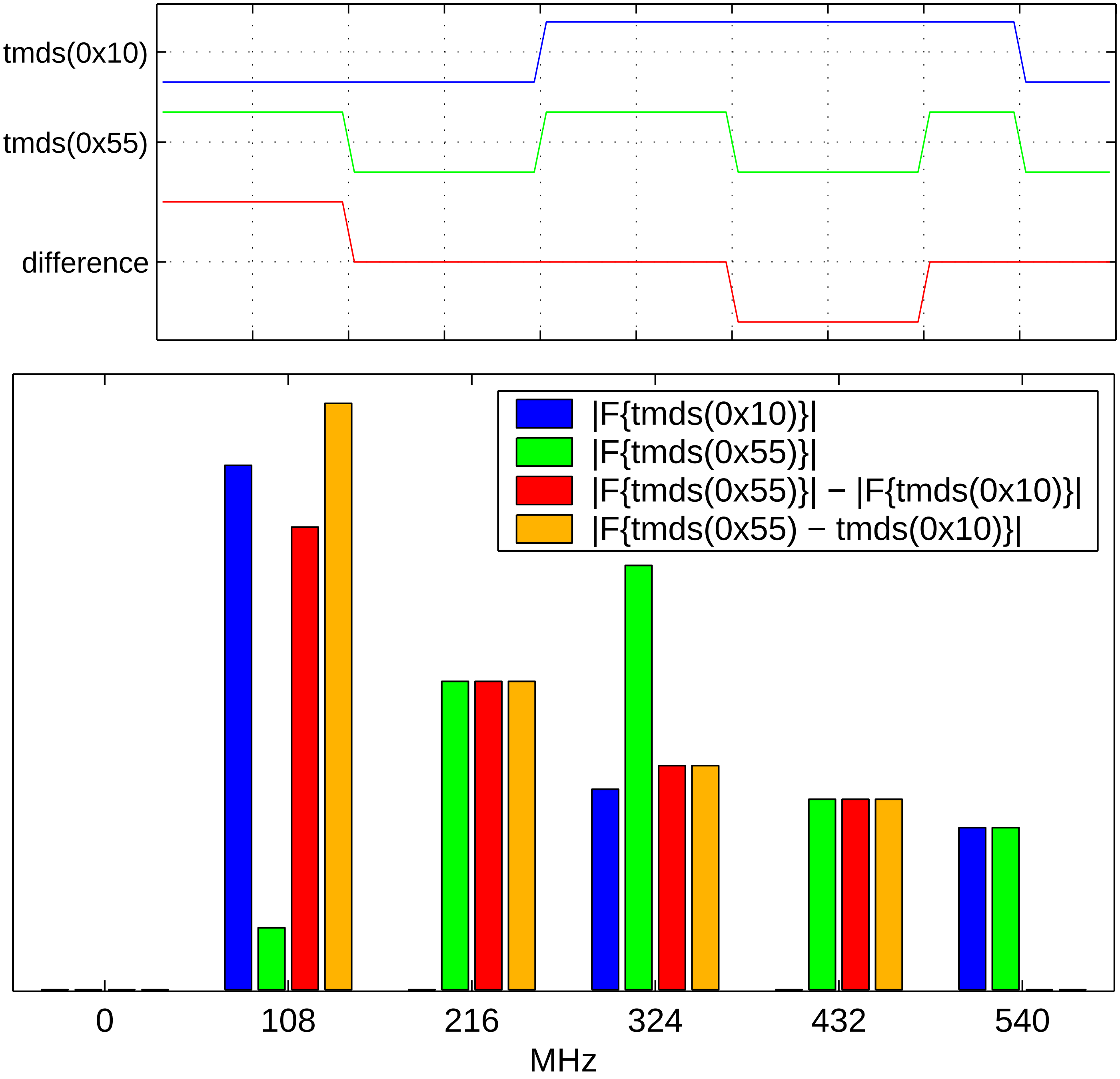
High-contrast pair:

$$\begin{aligned}00001000, 00001000, \ldots &\longrightarrow 0000111110, 0000111110, \ldots\\ 10101010, 10101010, \ldots &\longrightarrow 1100110010, 1100110010, \ldots\end{aligned}$$

Maximum/minimum contrast for DVI



324 MHz center frequency, 50 MHz bandwidth, 5 frames averaged, 3 m distance


tmds(0x10)
tmds(0x55)
difference
|F{tmds(0x10)}|
|F{tmds(0x55)}|
|F{tmds(0x55)}| − |F{tmds(0x10)}|
|F{tmds(0x55) − tmds(0x10)}|
0
108
216
324
432
540
MHz

RF emission limits

What test standards provide adequate protection?

- ⟶ MPR II / TCO'92: Measure only below 400 kHz (deflection coils) and are therefore irrelevant for video signals.
- ⟶ CISPR 22 Class B (CE, FCC, etc.): 37 dBμV/m at 10 m distance in any 120 kHz passband.
- ⟶ MIL-STD-461E (R102): 24 dBμV/m at 1 m distance in any 100 kHz passband.
- ⟶ My proposal: 24 dBμV/m at 1 m distance in any 5 MHz pass band (option: only for periodic averaging results).

The civilian RFI limits do not prevent receivability at quiet site over hundreds of meters with compact directional antenna array and periodic averaging. Impulse level raises linearly with bandwidth, noise level increases normally with square root of bandwidth.

Optical eavesdropping

→ RF emissions are just an unwanted side effect.

→ Displays were designed to emit *light*.

→ Projective observation (telescopes, mirrors, etc.).

→ Observation of light intensity variation.

Display spying with telescopes

Diffraction limit for angular resolution:

$$\theta = \frac{1.22 \cdot \lambda}{D},$$

Aperture required for pixel size r at distance d and viewing angle α:

$$D = \frac{1.22 \cdot \lambda \cdot d}{r \cdot \cos \alpha}$$

Example:

Typical pixel size:	$r = 0.25$ mm (320×240 mm $= 1280 \times 1024$ pixels)
Aperture:	$D = 300$ mm (amateur astronomy reflector)
Range:	$d \approx 60$ m

Time-domain observation of CRT light

Overall light emitted by CRT is proportional to (gamma corrected) video signal $v_\gamma(t)$ convolved with phosphor impulse response $P(t)$:

$$I(t) = \int_0^\infty v_\gamma(t - t')\, P(t')\, \mathrm{d}t'$$

$\longrightarrow$ What does the impulse response curve of commonly used CRT phosphors look like?

$\longrightarrow$ Does it have very fast decay components that preserve the high-frequency areas of the video signal spectrum?

$\longrightarrow$ Are practically usable light sensors available to detect these?

$\longrightarrow$ What limits are there and is this a practical risk?

$\longrightarrow$ What countermeasures are there?

CRT phosphor types

Monitor manual says “P22”, but this is just the generic designation for all RGB phosphor triplets designed for NTSC color TV.

Worldwide Type Designation System (WTDS): XXA, XXB, XBA, . . .

Substances:

- ⟶ Red: yttrium oxysulfide doped with europium (Y_2O_2S:Eu), zinc phosphate with manganese ($Zn_3(PO_4)_2$:Mn).
- ⟶ Green: zinc sulfide doped with copper (ZnS:Cu) and sometimes also with aluminium and/or gold, or zinc silicate doped with manganese and silver (Zn_2SiO_4:Mn,Ag).
- ⟶ Blue: The blue phosphor is usually zinc sulfide doped with silver (ZnS:Ag) and in some cases also aluminium or gallium.

Light sensors

Requirements:

$\longrightarrow$ very sensitive (to reduce preamp noise)

$\longrightarrow$ very fast (bandwidth comparable to $f_\mathrm{p}/2$, ideally $>$100 MHz or $<$5 ns rise and fall time)

Options:

$\longrightarrow$ PIN photodiode (typical sensitivity 0.2–0.6 A/W, μs–ns)

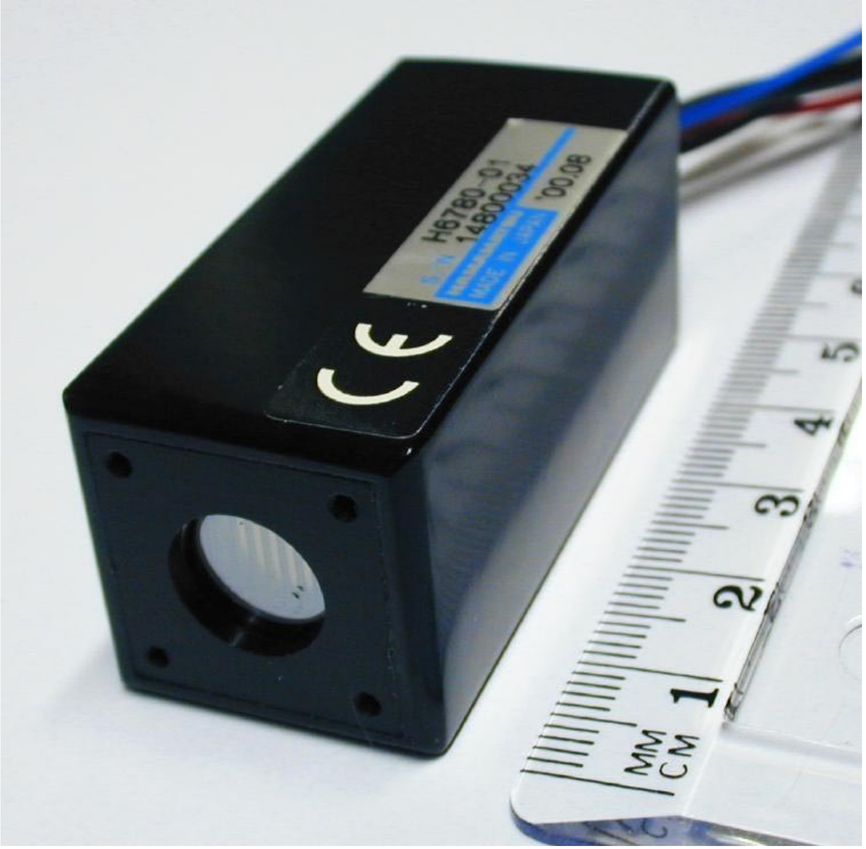
$\longrightarrow$ Avalanche photodiode (internal gain, typical sensitivity 10^2 A/W, < 1 ns raise/fall time)

$\longrightarrow$ Photomultiplier tube (significant internal gain, typical sensitivity 10^1–10^5 A/W, < 1 ns raise/fall time)

The photomultiplier tube (PMT)

Choice: Hamamatsu H6780-01 Photomultiplier tube module with integrated high-voltage circuit allows easy operation from 12 V lab power supply.
Control voltage $0.25 < U_\mathrm{c} < 0.9$ V adjusts radiant sensitivity to

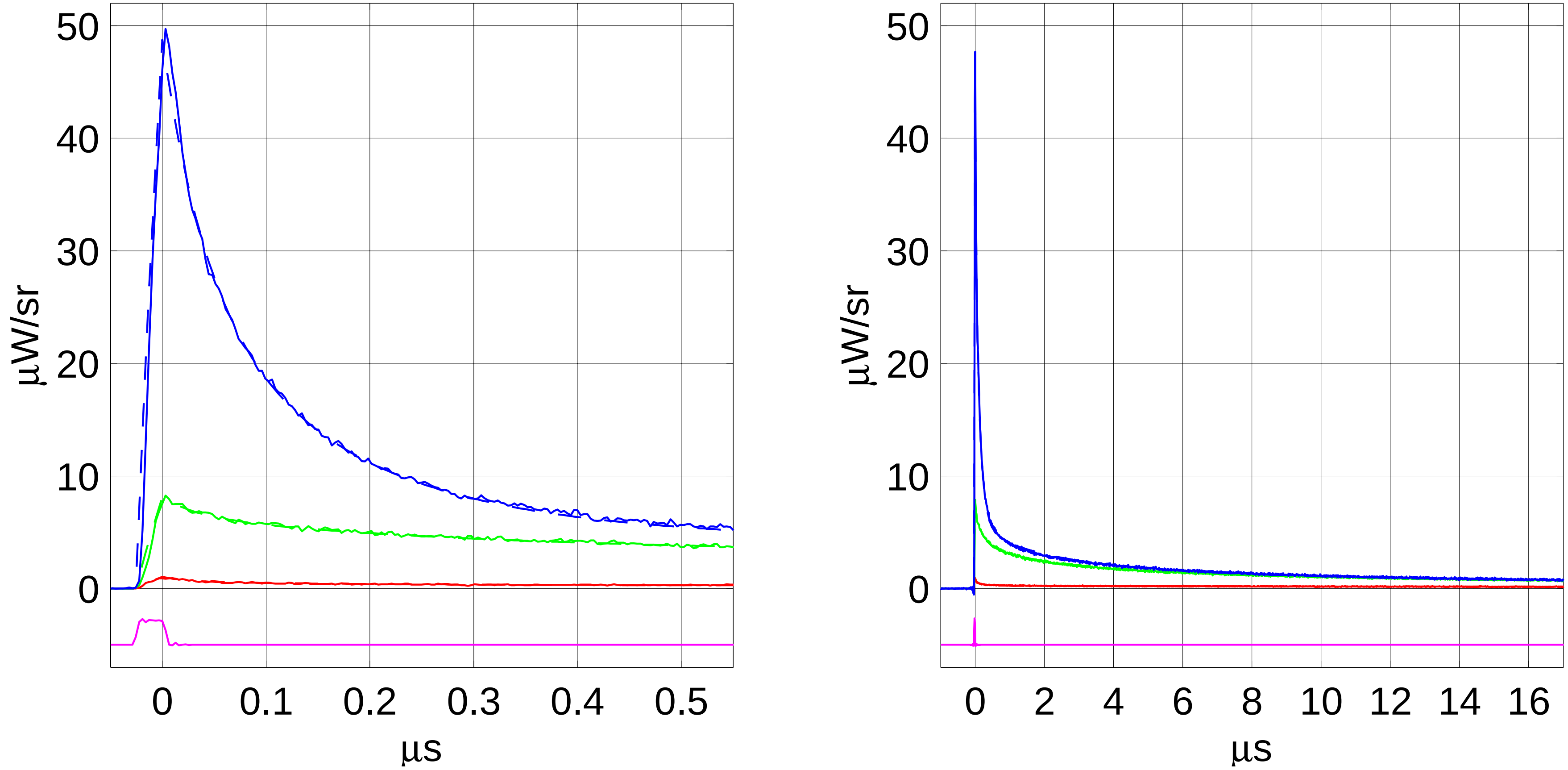
$$1.5 \times 10^5 \ \mathrm{A/W} \cdot \left(\frac{U_\mathrm{c}}{1\ \mathrm{V}}\right)^{7.2}$$



Thanks to high internal gain no need for video pre-amplifier, allowing direct connection to 50 Ω DC input of digital storage oscilloscope.

Measured P22 intensity decay curves

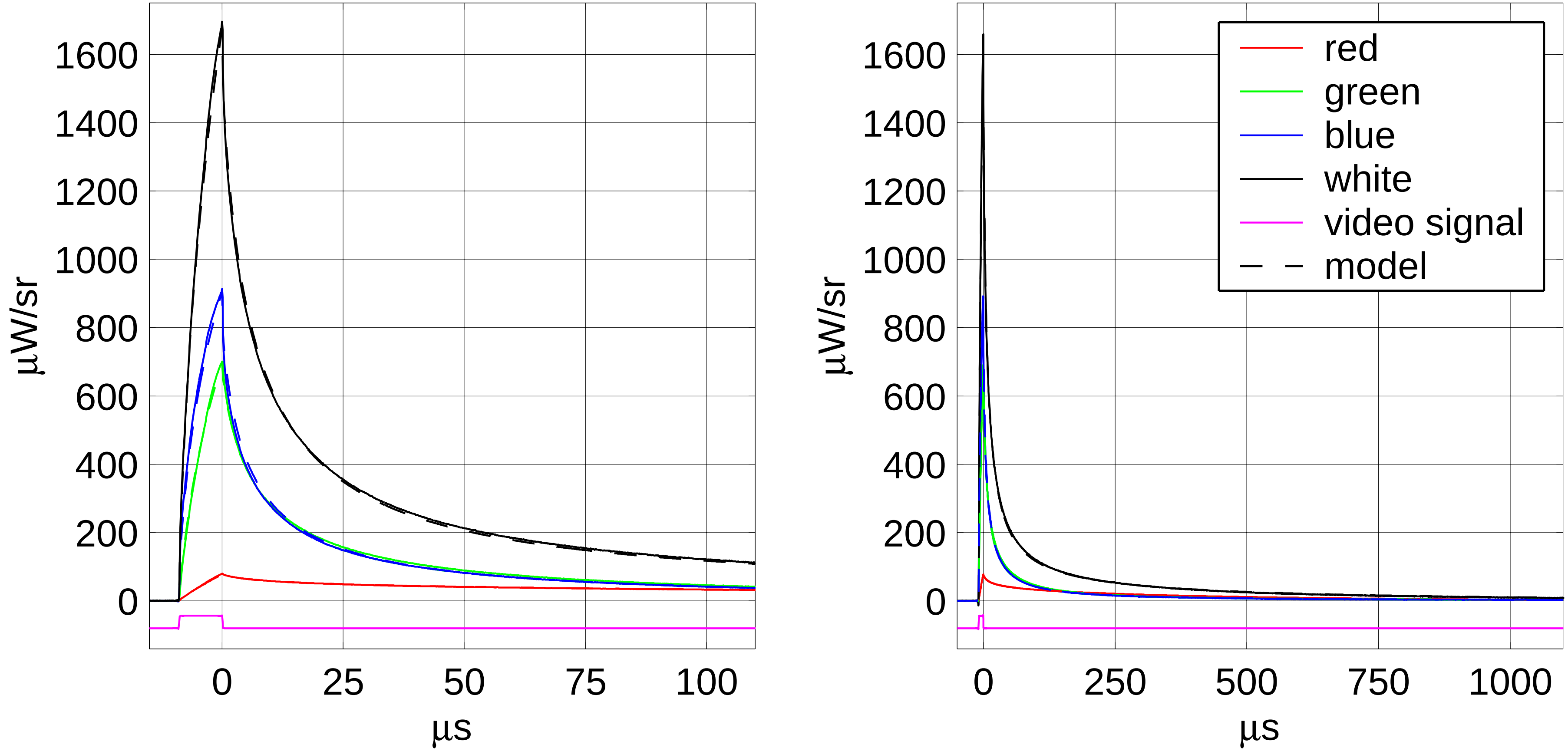
(a) Emission decay of a single pixel (f_p = 36 MHz)



The sensor output voltage is shown here as the equivalent radiant intensity (power per solid angle) of the light source.

Measured P22 intensity decay curves

(b) Emission decay of a 320−pixel line



Modeling phosphor impulse responses

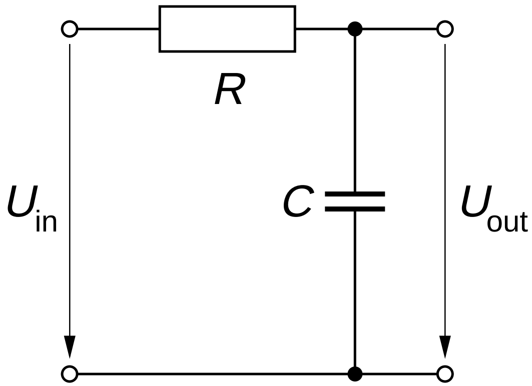
→ Exponential decay curve of a typical phosphorescent substance:

$$I_{\mathrm{e}}(t) = I_0 \cdot \mathrm{e}^{-\frac{t}{\tau}}$$

Note that this is for

$$\tau = \frac{1}{2\pi f} = RC$$

the impulse response of a first-order Butterworth low-pass filter.



→ Power-law decay curve of zinc-sulfide based phosphors:

$$I_{\mathrm{p}}(t) = \frac{I_0}{(t+\alpha)^{\beta}}.$$

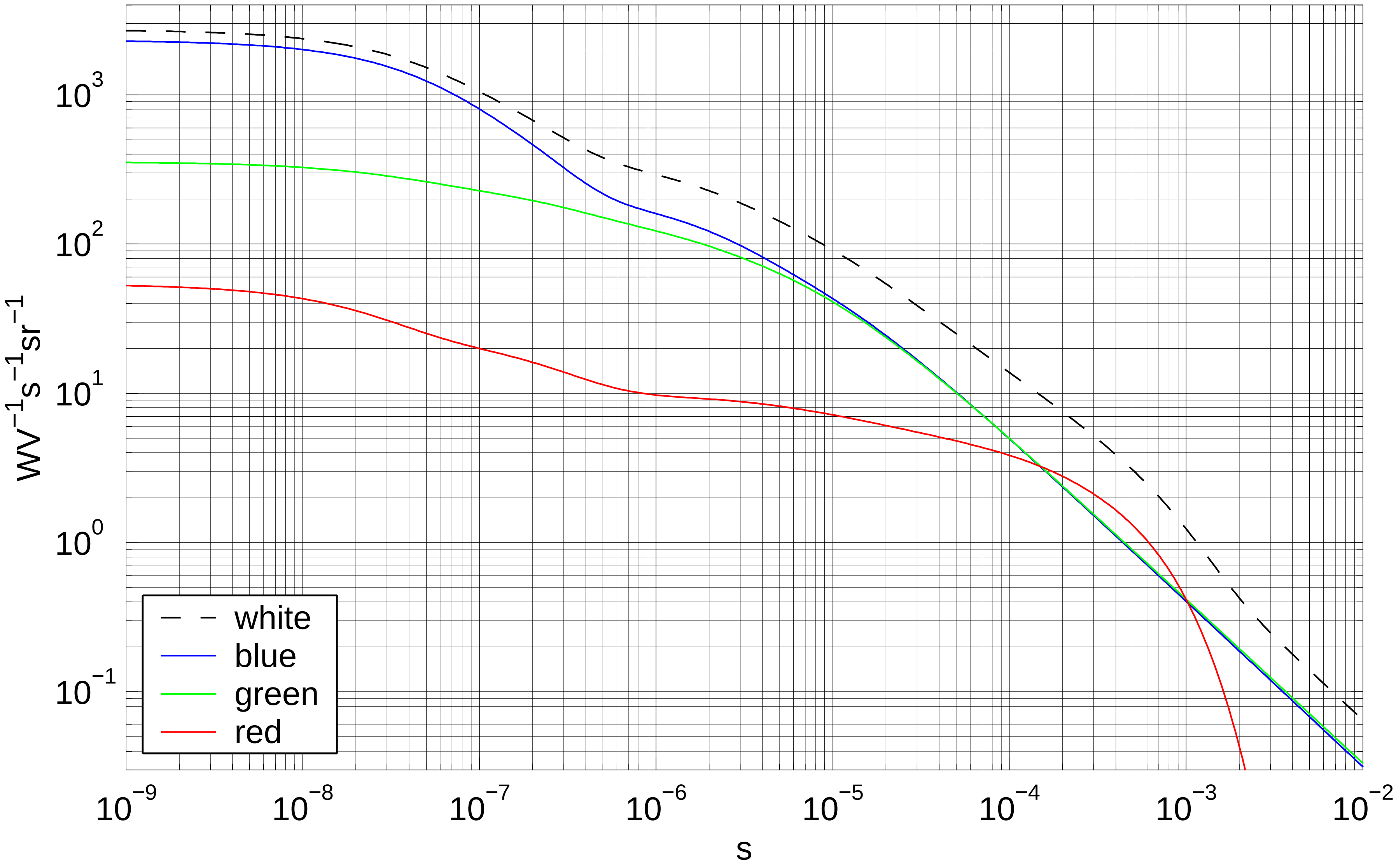
(Results in asymptotically straight line on loglog scale.)

Closed form impulse response model

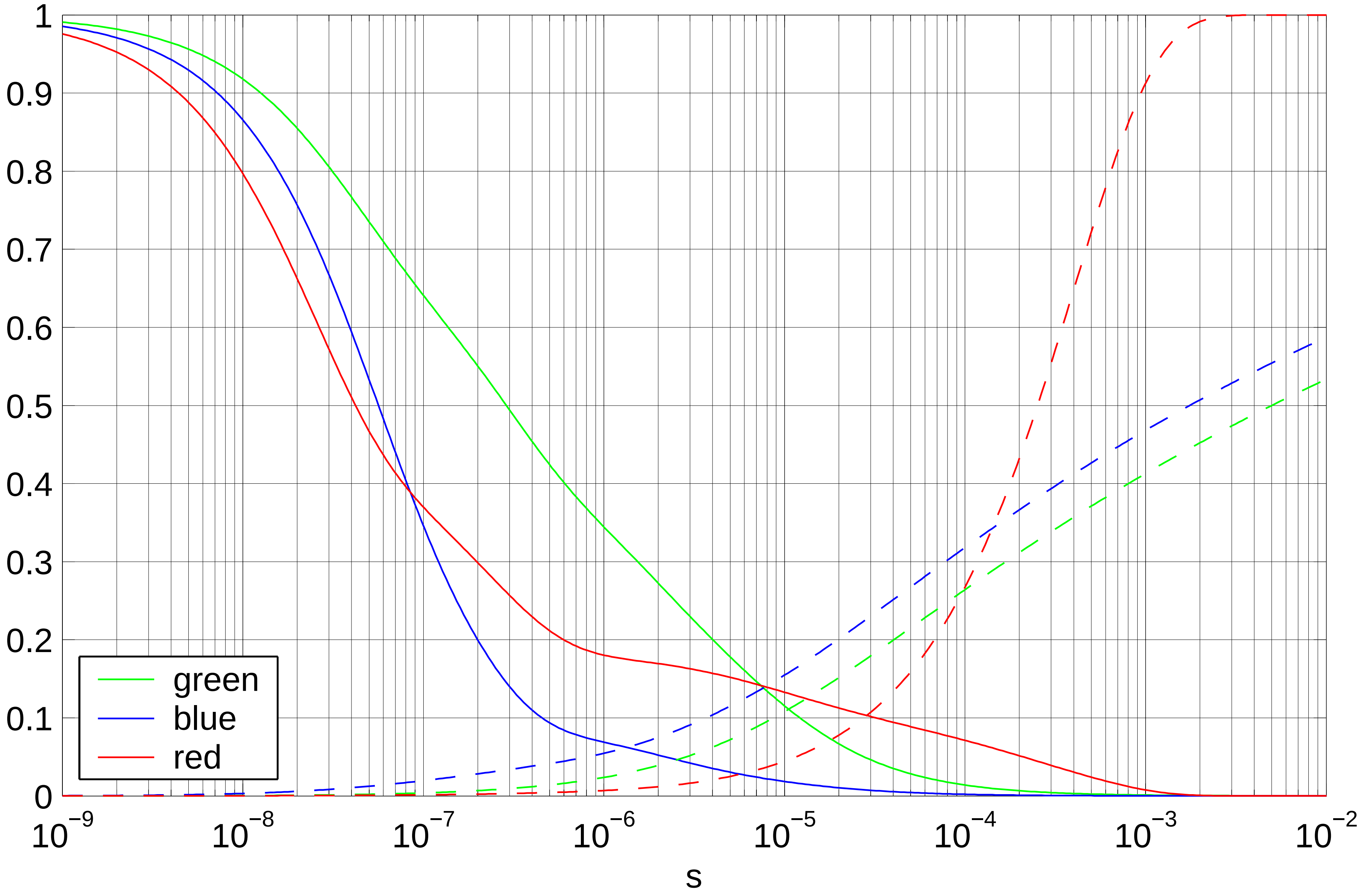
Real impulse response curves have to be approximated by a linear combination of exponential and power-law curves:

$$
\begin{aligned}
P_{\mathrm{P22R}}(t) \,/\, \frac{\mathrm{W}}{\mathrm{V}\cdot\mathrm{s}\cdot\mathrm{sr}} &= 4 \times \mathrm{e}^{-2\pi t \,\times\, 360\ \mathrm{Hz}} + 1.75 \times \mathrm{e}^{-2\pi t \,\times\, 1.6\ \mathrm{kHz}} + \\
&\quad 2 \times \mathrm{e}^{-2\pi t \,\times\, 8\ \mathrm{kHz}} + 2.25 \times \mathrm{e}^{-2\pi t \,\times\, 25\ \mathrm{kHz}} + \\
&\quad 15 \times \mathrm{e}^{-2\pi t \,\times\, 700\ \mathrm{kHz}} + 29 \times \mathrm{e}^{-2\pi t \,\times\, 7\ \mathrm{MHz}} \\
P_{\mathrm{P22G}}(t) \,/\, \frac{\mathrm{W}}{\mathrm{V}\cdot\mathrm{s}\cdot\mathrm{sr}} &= 210 \times 10^{-6} \times \left(\frac{t + 5.5\ \mu\mathrm{s}}{1\ \mathrm{s}}\right)^{-1.1} + 37 \times \mathrm{e}^{-2\pi t \,\times\, 150\ \mathrm{kHz}} + \\
&\quad 100 \times \mathrm{e}^{-2\pi t \,\times\, 700\ \mathrm{kHz}} + 90 \times \mathrm{e}^{-2\pi t \,\times\, 5\ \mathrm{MHz}} \\
P_{\mathrm{P22B}}(t) \,/\, \frac{\mathrm{W}}{\mathrm{V}\cdot\mathrm{s}\cdot\mathrm{sr}} &= 190 \times 10^{-6} \times \left(\frac{t + 5\ \mu\mathrm{s}}{1\ \mathrm{s}}\right)^{-1.11} + 75 \times \mathrm{e}^{-2\pi t \,\times\, 100\ \mathrm{kHz}} + \\
&\quad 1000 \times \mathrm{e}^{-2\pi t \,\times\, 1.1\ \mathrm{MHz}} + 1100 \times \mathrm{e}^{-2\pi t \,\times\, 4\ \mathrm{MHz}} \\
P_{\mathrm{P22}} &= P_{\mathrm{P22R}} + P_{\mathrm{P22G}} + P_{\mathrm{P22B}}
\end{aligned}
$$

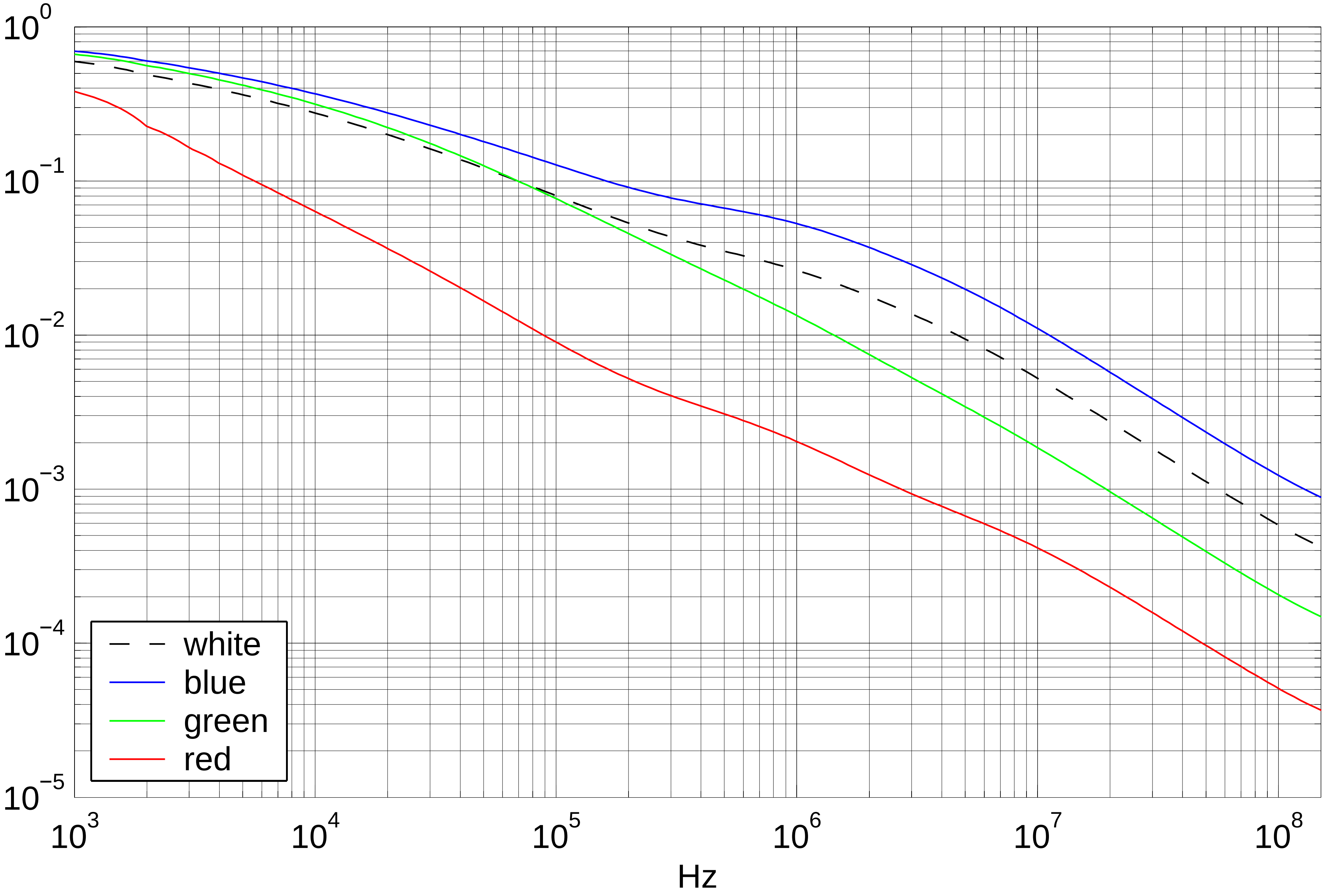
Double-log plot of reconstructed P22 impulse response



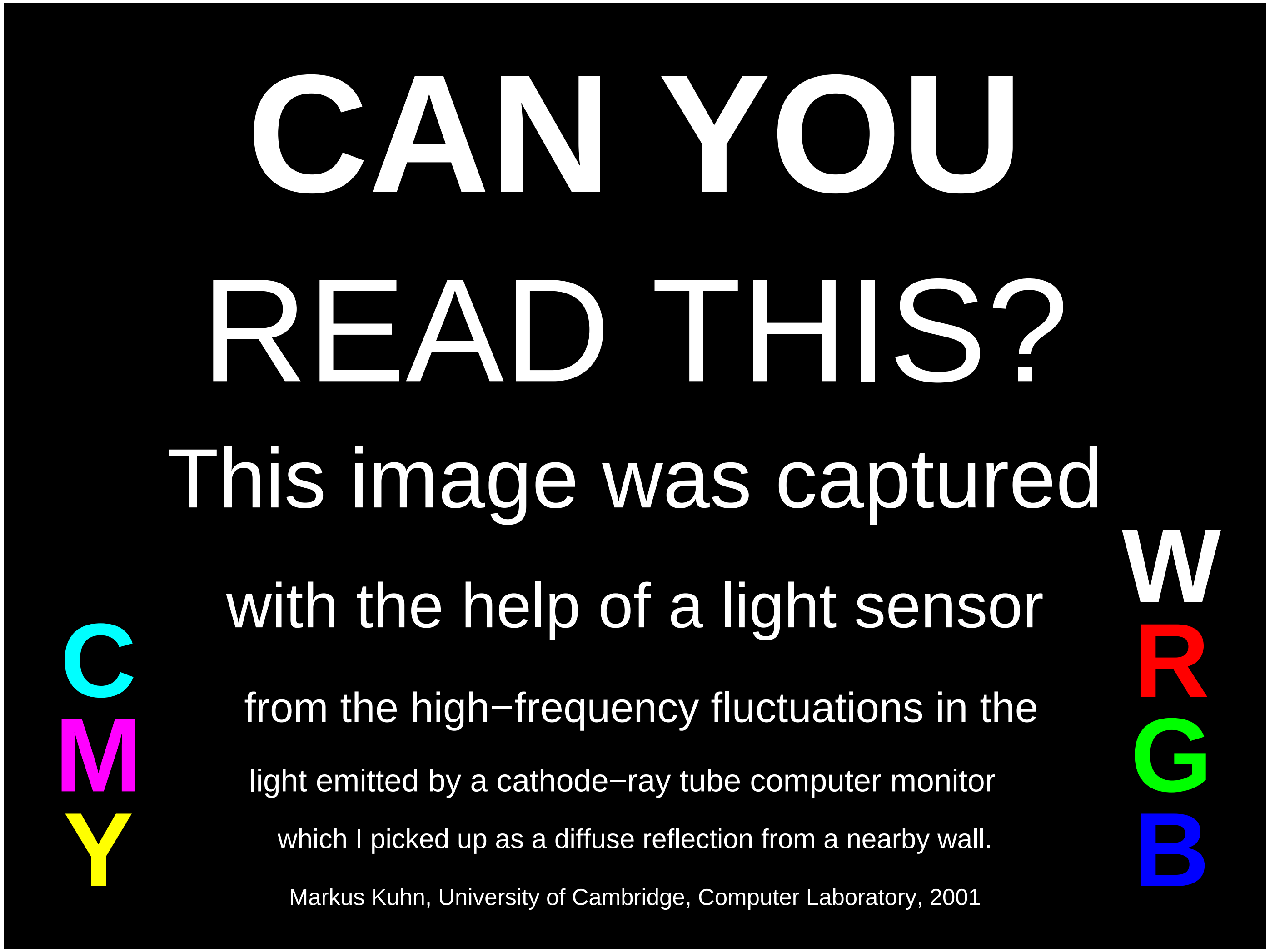
Integrated impulse response curves



Estimated P22 frequency characteristic



Test image shown on target monitor



CAN YOU

READ THIS?

This image was captured

with the help of a light sensor

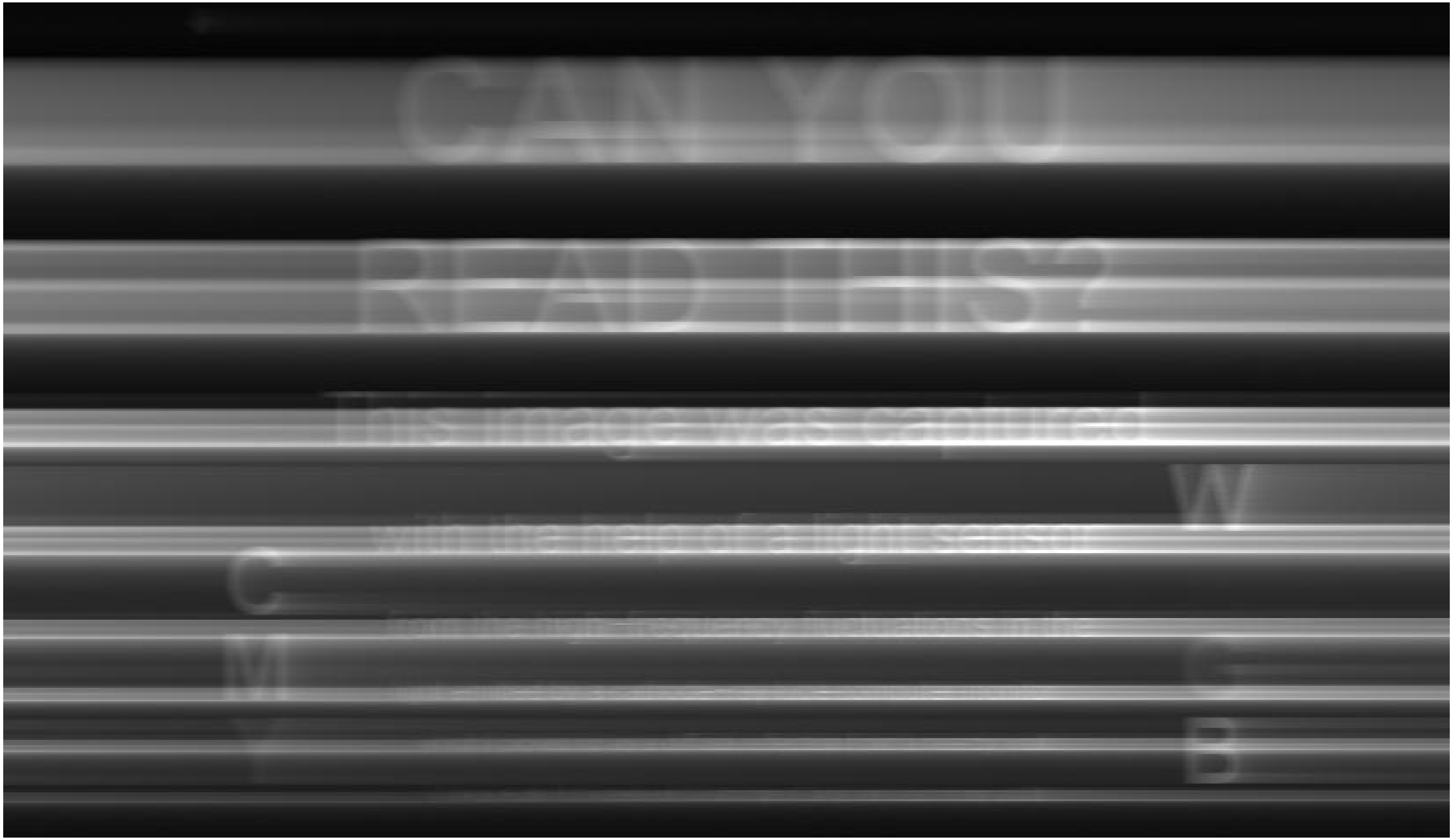
from the high−frequency fluctuations in the

light emitted by a cathode−ray tube computer monitor

which I picked up as a diffuse reflection from a nearby wall.

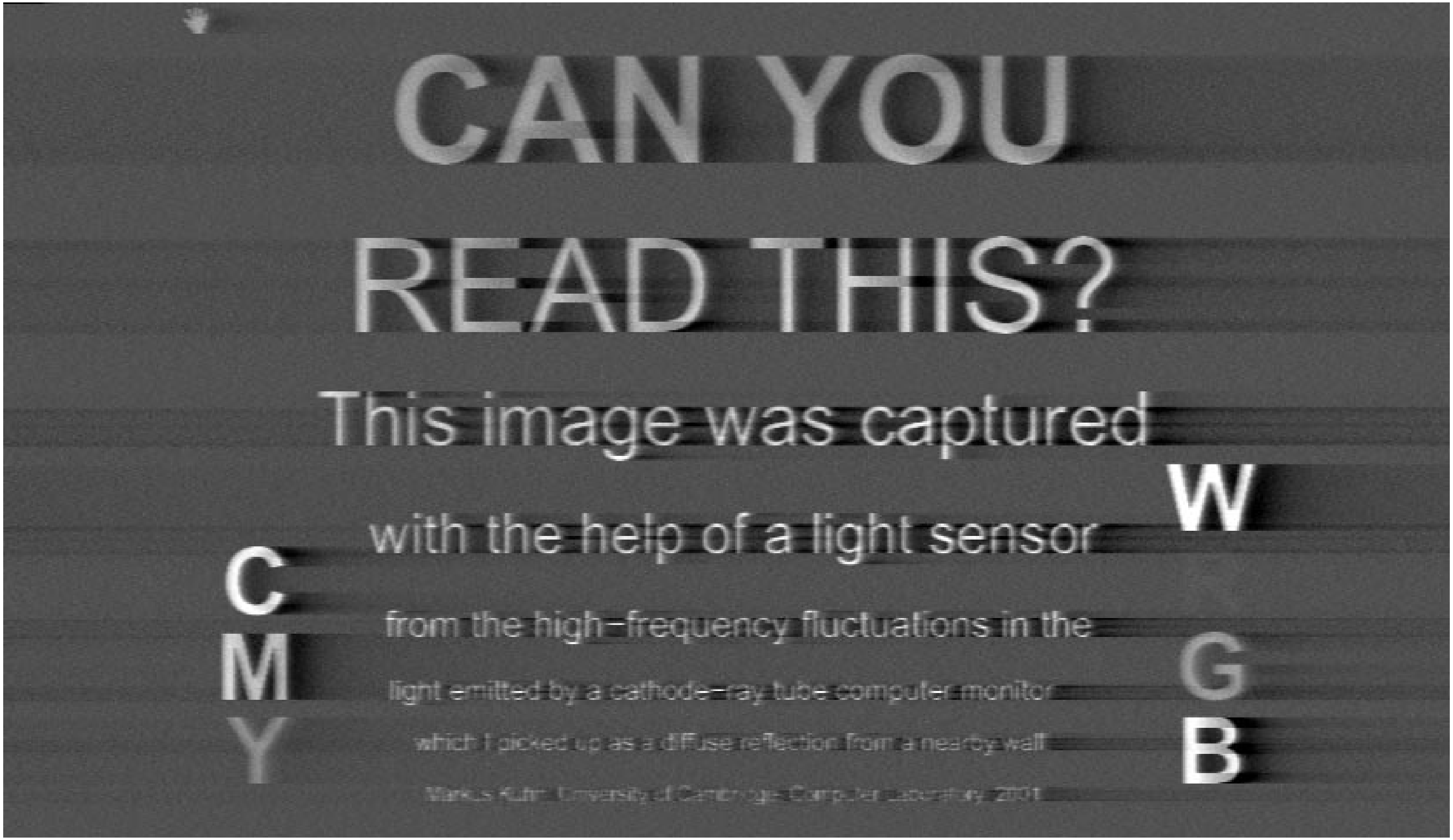
Markus Kuhn, University of Cambridge, Computer Laboratory, 2001

Rasterized raw signal from PMT



VESA mode 640×480@85 Hz, 8-bit sampled at 250 MHz, 256 frames (3.0 s, 753 MB) averaged, scaled to 0.1% saturation

High-pass filtering result



CAN YOU

READ THIS?

This image was captured

with the help of a light sensor

from the high-frequency fluctuations in the

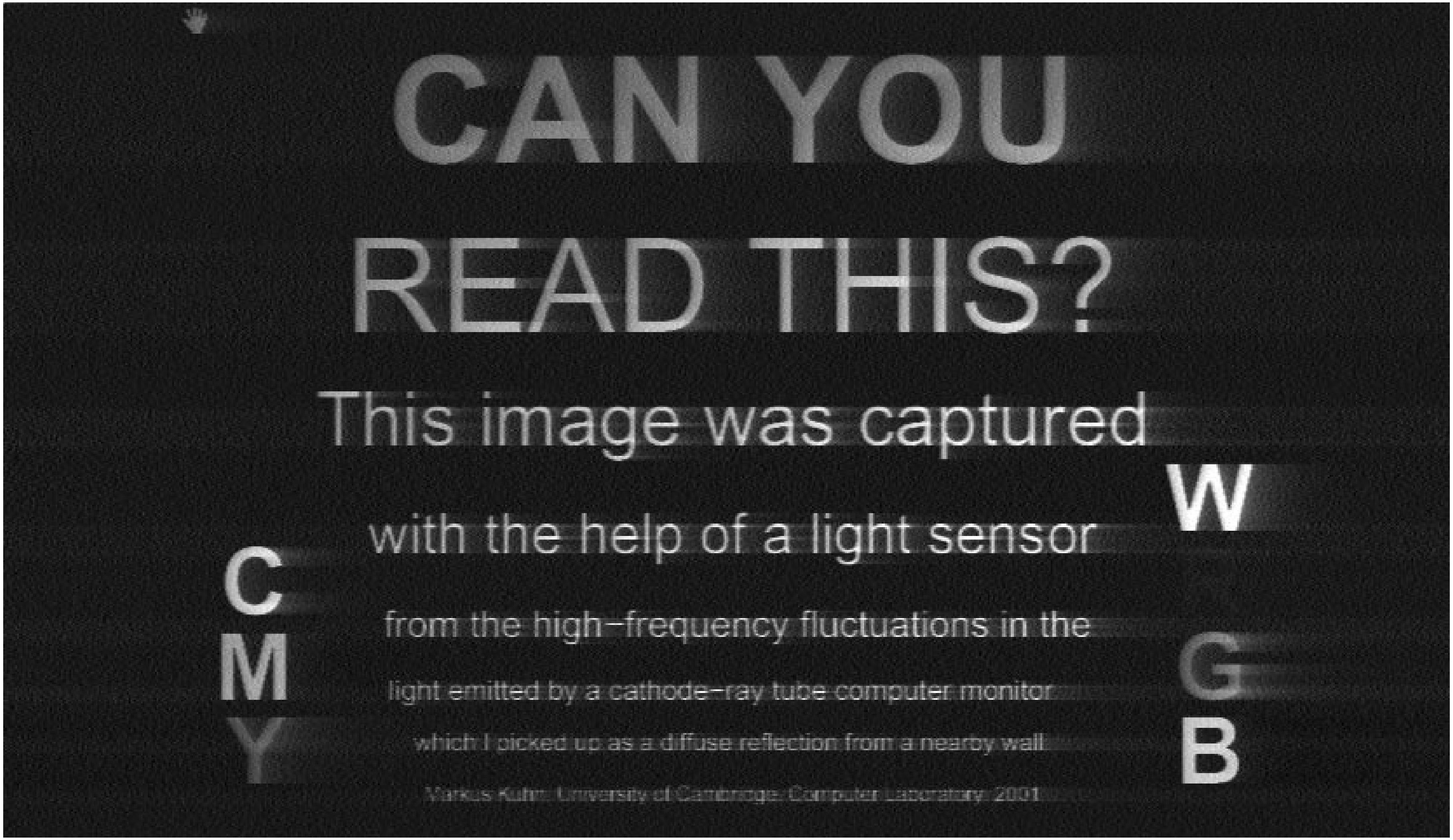
light emitted by a cathode-ray tube computer monitor

which I picked up as a diffuse reflection from a nearby wall

Markus Kuhn, University of Cambridge, Computer Laboratory, 2001

First-order Butterworth high-pass filter applied, 3 dB cutoff at 4 MHz.

Deconvolution result



CAN YOU READ THIS?

This image was captured with the help of a light sensor from the high−frequency fluctuations in the light emitted by a cathode−ray tube computer monitor which I picked up as a diffuse reflection from a nearby wall

Markus Kuhn, University of Cambridge, Computer Laboratory, 2001

Deconvolution

We can model highly accurately the sensor signal blurred by the phosphor afterglow as the convolution of the beam current v_γ and the impulse-response function P_{P22}

$$I(t) = \int_0^\infty v_\gamma(t - t')\, P_{\mathrm{P22}}(t')\,\mathrm{d}t'$$

which a Fourier transform turns into a multiplication of frequency-domain signals:

$$\mathcal{F}\{I\} = \mathcal{F}\{\tilde{v}_\gamma\} \cdot \mathcal{F}\{P_{\mathrm{P22}}\}.$$

Deconvolution can be accomplished simply by division in the frequency domain, followed by an inverse FFT, leading to the shown estimate of the original beam current:

$$\tilde{v}_\gamma = \mathcal{F}^{-1}\left\{\frac{\mathcal{F}\{I\}}{\mathcal{F}\{P_{\mathrm{P22}}\}}\right\}$$

Threat analysis

Number of signal photons received per pixel:

$$N_\mathrm{p} = \frac{Q_\mathrm{p}\lambda}{hc}$$

where Q_p is the amount of energy received from a single pixel.

Number of photons received from background light:

$$N_\mathrm{b} = \frac{nt_\mathrm{p}AA_\mathrm{r}L_\mathrm{b}\lambda}{hcd^2}$$

where

A	$=$	observed area $[\mathrm{m}^2]$	L_b	$=$	wall radiance $[\mathrm{W}/(\mathrm{sr}\cdot\mathrm{m}^2)]$
A_r	$=$	receiver aperture $[\mathrm{m}^2]$	t_p	$=$	f_p^{-1} = pixel duration [s]
d	$=$	observer distance [m]	n	$=$	number of frames averaged

Arrival of photons at a sensor is a Poisson process

$\longrightarrow$ we expect N_b photons per pixel

$\longrightarrow$ the standard deviation of photon count will be $\sqrt{N_\mathrm{b}}$

$\longrightarrow$ “shot noise”

Risk zone

Eavesdropped signal must dominate background-light shot noise:

$$N_\mathrm{p} > \sqrt{N_\mathrm{b}}$$

Number of photons reflected of a wall

$$N_\mathrm{p} = \frac{\varrho n t_\mathrm{p}^2 A A_\mathrm{r} V P(0) \lambda}{2\pi h c d^2 d'^2}$$

where

ϱ = reflectivity of wall (white ≈ 0.8)

$P(t)$ = phosphor impulse response function [W/$(\mathrm{V} \cdot \mathrm{s} \cdot \mathrm{sr})$]

V = video voltage (gamma corrected) [V]

d' = distance wall/CRT [m]

d = distance wall/receiver [m]

The detection process is approximated here by integrating $P_\mathrm{P22}(t) \approx P_\mathrm{P22}(0)$ over pixel time t_p to estimate pixel brightness after high-pass filtering.

More accurate estimate with numerical simulation of detection and deconvolution.

CRT risk zone calculation

Upper limit for receiver distance to wall:

$$d < \frac{VP(0)}{d'^2}\sqrt{\frac{\varrho n \lambda t_{\mathrm{p}}^3 A A_{\mathrm{r}}}{4\pi E_{\mathrm{b}} hc}}$$

Applied to some example values:

- $\longrightarrow$ Illuminance 2 lux ("late twilight") corresponds to irradiance $E_{\mathrm{b}} = 1$ mW/m^2 onto the wall ($A = 2$ m^2 and $\varrho = 0.5$)
- $\longrightarrow$ CRT at $d' = 2$ m from the wall has an initial impulse response of $P(0) = 10^3$ W/$(\mathrm{V} \cdot \mathrm{s} \cdot \mathrm{sr})$ and $V = 1$ V for a white pixel.
- $\longrightarrow$ Eavesdropper has $A_{\mathrm{r}} = 0.3$ m^2 telescope and averages $n = 100$ frames.

Then

$$d < 50 \text{ m}$$

Diffuse reflection of status indicator light

Of 39 tested communication devices, 14 emitted serial port data in light from transmit/receive line status LEDs. [Loughry/Umphress, 2002]

Model number N of photons received by eavesdropper as normal distribution with

$$\begin{aligned}\mu &= \begin{cases} N_\mathrm{b} + N_\mathrm{p} & \text{when LED on} \\ N_\mathrm{b} & \text{when LED off}\end{cases} \\ \sigma &= \sqrt{N_\mathrm{b}}\end{aligned}$$

Detector compares N with threshold $N_\mathrm{b} + \frac{1}{2}N_\mathrm{p}$, resulting in bit-error rate

$$p_\mathrm{BER} = Q\left(\frac{N_\mathrm{p}}{2\sqrt{N_\mathrm{b}}}\right) \quad \text{with} \quad Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty \mathrm{e}^{-\frac{y^2}{2}}\,\mathrm{d}y$$

LED bit-error rate calculation

$$N_\mathrm{p} = \frac{t_\mathrm{p} A_\mathrm{r} I_\mathrm{p} \lambda}{hcd^2}, \qquad N_\mathrm{b} = \frac{t_\mathrm{p} A A_\mathrm{r} \varrho E_\mathrm{b} \lambda}{\pi hcd^2}$$

Applied to some example values:

$\longrightarrow$ Green ($\lambda = 565$ nm) LED with 7 mcd (corresponds to radiant intensity $I_\mathrm{p} = 10^{-5}$ W/sr) located $d' = 2$ m from wall shows 10 kbit/s signal ($t_\mathrm{p} = 10^{-4}$ s).

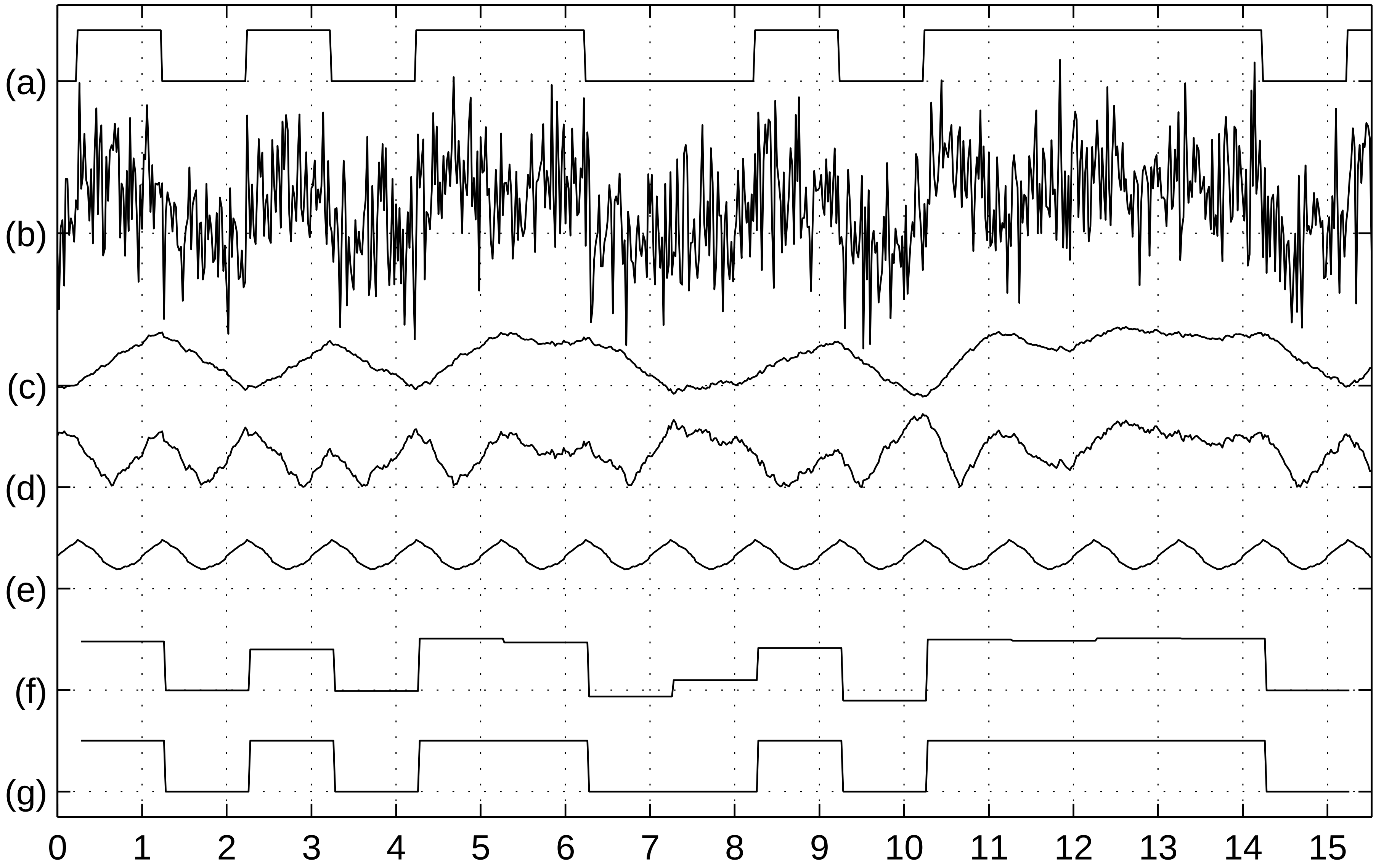
$\longrightarrow$ Eavesdropper observes $A = 2$ m^2 wall at $d = 50$ m distance with $A_\mathrm{r} = 0.3$ m^2 telescope.

$\longrightarrow$ Wall reflects $\varrho = 0.5$ of ambient illuminance $E_\mathrm{b} = 1$ mW/m^2 ("late twilight").

Resulting bit-error rate due to shot-noise limit:

$$p_\mathrm{BER} > 10^{-4}$$

Clock recovery and detection of serial data



Receiver design considerations

$\longrightarrow$ Use zoom telescope and mechanism to mask area of interest with best signal-to-noise ratio.

$\longrightarrow$ Use large-aperture optics (imaging quality less relevant).

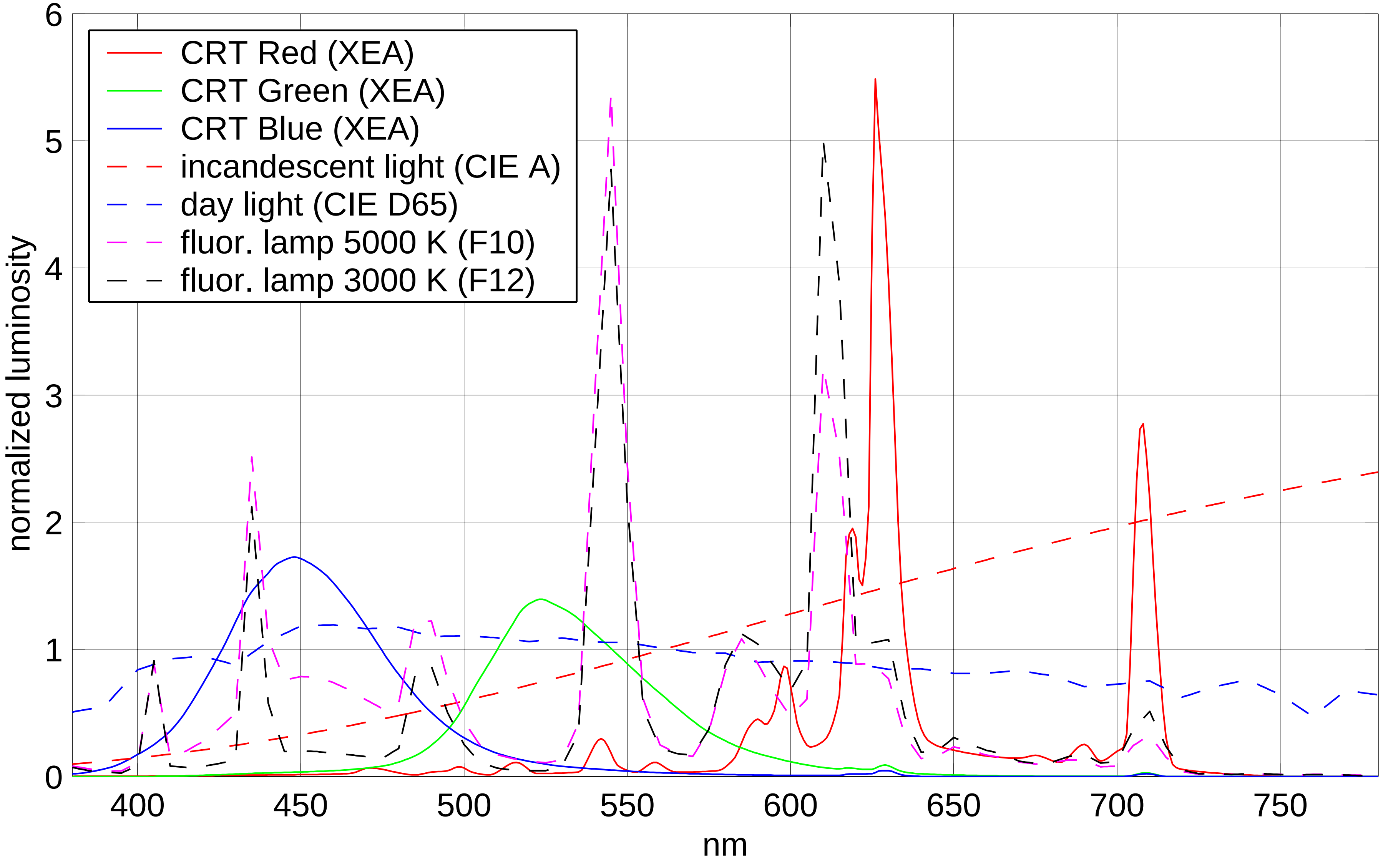
$\longrightarrow$ Characterize phosphor impulse response in different wavelength subbands.

$\longrightarrow$ Use filter set or spectrometer to select wavelength range with best signal-to-noise ratio.

$\longrightarrow$ Where older fluorescent lamps driven with 50/60 Hz currents are used, collect signal during dark periods (gated PMT).

$\longrightarrow$ Use analog preprocessing of photomultiplier output to reduce quantization and amplifier noise.

Spectral coverage of CRT phosphors and flourescent lamps



Possible countermeasures

- → Avoid line-of-sight access to displays, keyboards, documents.
- → Ensure good background illumination that covers the entire spectrum of wavelength emitted by the CRT phosphors.
- → Avoid fluorescent lamps driven with low-frequency currents.
- → Using only the red channel to display particularly critical information has two advantages: (1) video signal is filtered better, (2) incandescent light jams red better than blue.
- → CRT and phosphor manufacturers should document phosphor impulse response curves in data sheets (double-logarithmic diagram with 10^{-9}–10^{-2} s timescale). Monitor manufacturers should document exact CRT types used.
- → CRT type security certification.
- → Common types of flat panel displays (LCD) seem to pose no threat because of parallel addressing of pixel rows and slower response times.

Conclusions (optical)

⟶ It is feasible to reconstruct the image displayed on a raster screen CRT from the emitted light, even after diffuse reflection.

⟶ A sufficiently dark environment (i.e., after sunset) is needed to avoid shot noise dominating the signal.

⟶ Etched/frosted/milky window glass does not necessarily prevent readability of CRT displays at a distance.

⟶ Off-the-shelf equipment sufficient for a lab demonstration.

⟶ Real-world attacks will require specially designed receivers and patience.

⟶ The threat level seems roughly comparable to that of compromising radio-frequency emanations.

Conclusions (RF)

→ Digital video interfaces used with flat panel displays can emit significantly stronger and better signal than CRTs.

→ CRT emissions dependent significantly on graphics card.

→ Human-readable text and radio character recognition is possible with contemporary video modes and equipment in nearby rooms even without directional antennas.

→ Various low-cost software countermeasures possible (filtered fonts, random bit jamming).

→ First civilian RF emission security test standard could be based on MIL RFI standard with increased bandwidth.

→ Emission security remains a valid concern in applications with high confidentiality requirements, predictable device usage and easy longterm access to neighbour rooms.

Open questions and future research

- → Software radio instead of AM/FM demodulator (to preserve polarity of pulses), phase lock center and pixel frequency, etc.
- → Larger product vulnerability surveys
- → Intentional broadcasts via non-periodic sources (bus lines, etc.)
- → Test and documentation of rumoured historic exploits (acoustic and power-line emanations of IBM golfball printer)
- → Refinement of test standard proposal (power lines, distinction between signal types, unshielded rooms, etc.)
- → Licence enforcement applications
- → Search for further new vulnerabilities and emanation channels
- → Stimulate FOI release of past military research