Electromagnetic eavesdropping risks of flat-panel displays

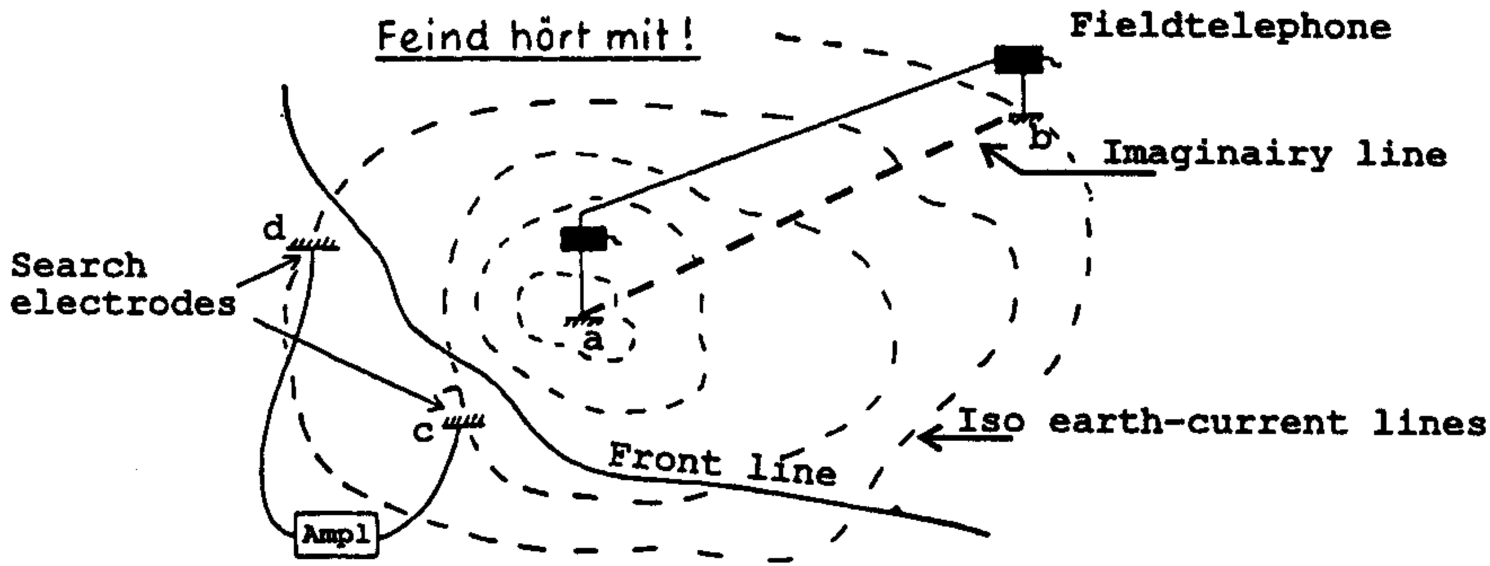
Markus G. Kuhn

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 [Bauer, 1999].

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".

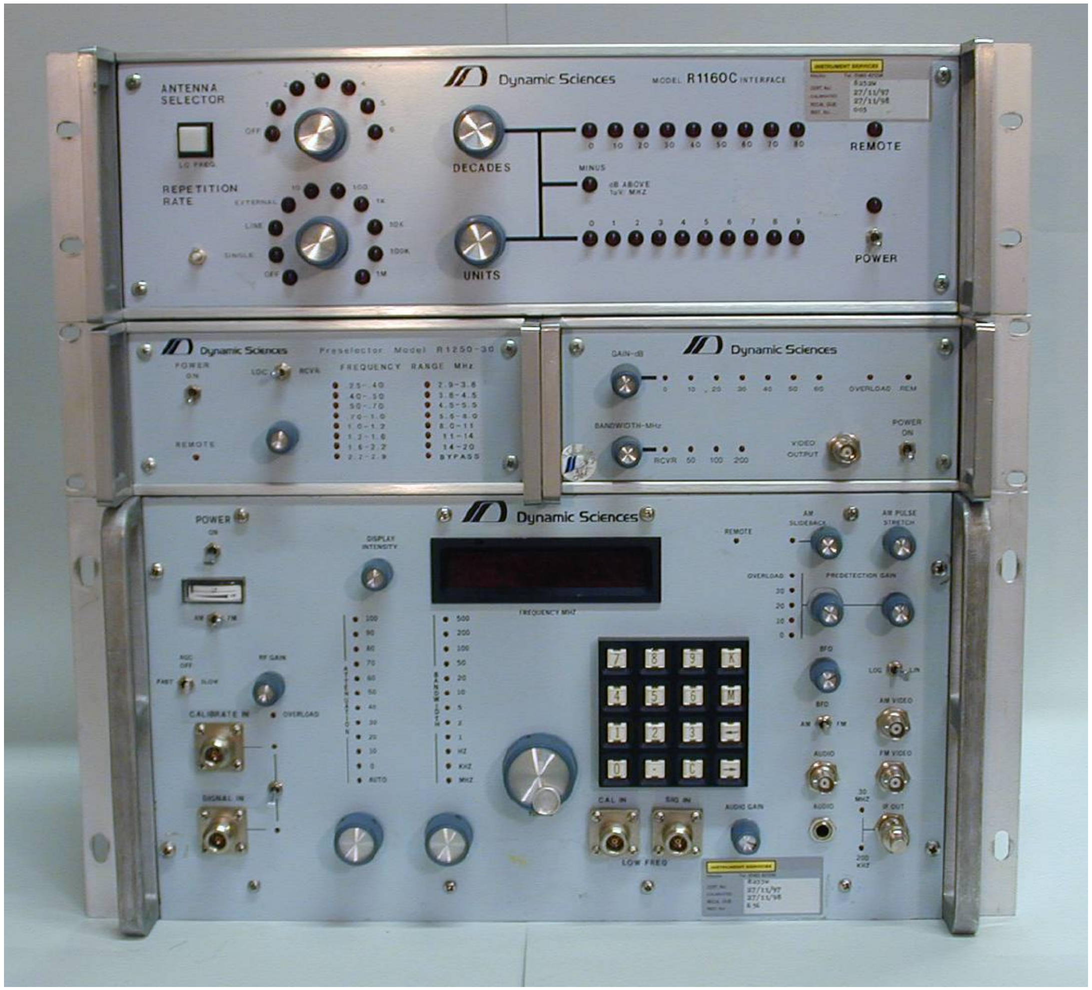
→ 1990: Peter Smulders investigates electromagnetic eavesdropping on RS-232 cables.

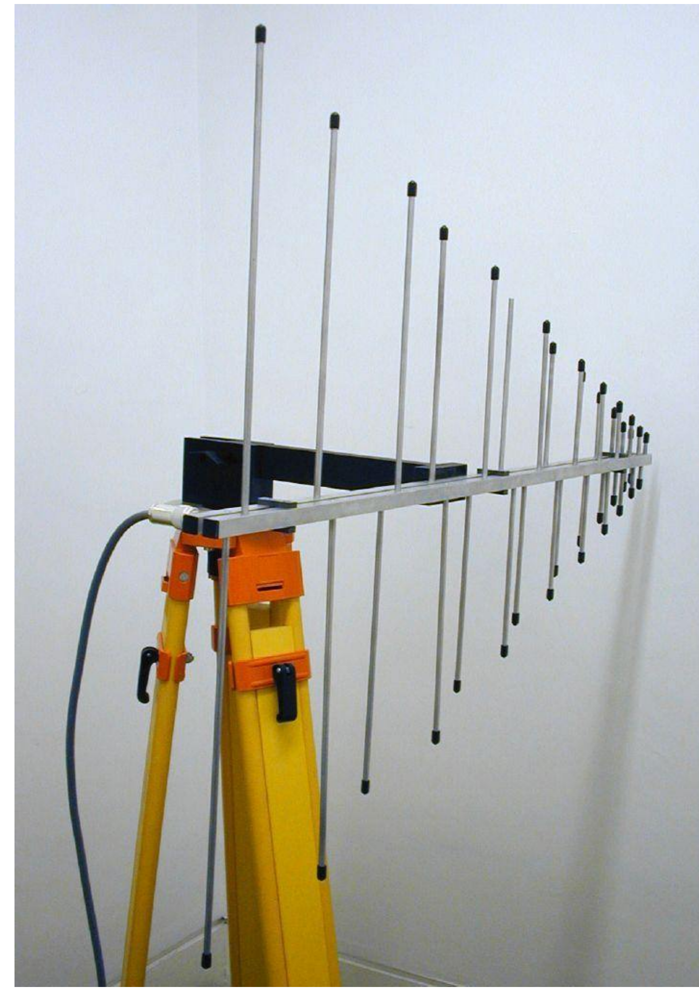
→ 1988/1991: Two Italian conferences on electromagnetic security for information protection.

→ 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





R1250 wideband Tempest receiver

$\longrightarrow$ Can be tuned continuously from 100 Hz to 1 GHz.

$\longrightarrow$ 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

$\longrightarrow$ Especially robust antenna input (for listening on power lines).

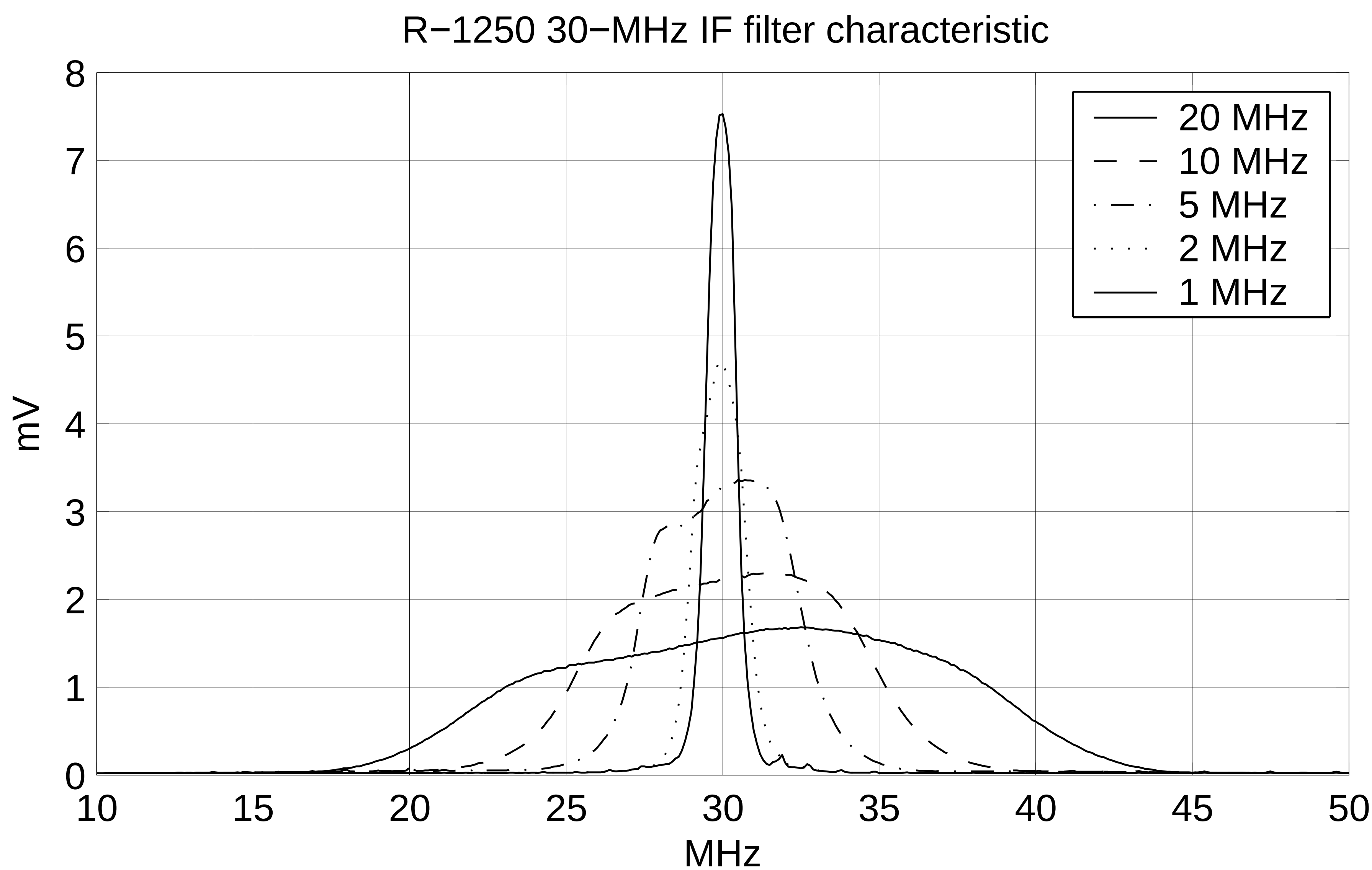
$\longrightarrow$ Gain adjustable by a factor of 10^9.

$\longrightarrow$ Automatic gain control can be deactivated.

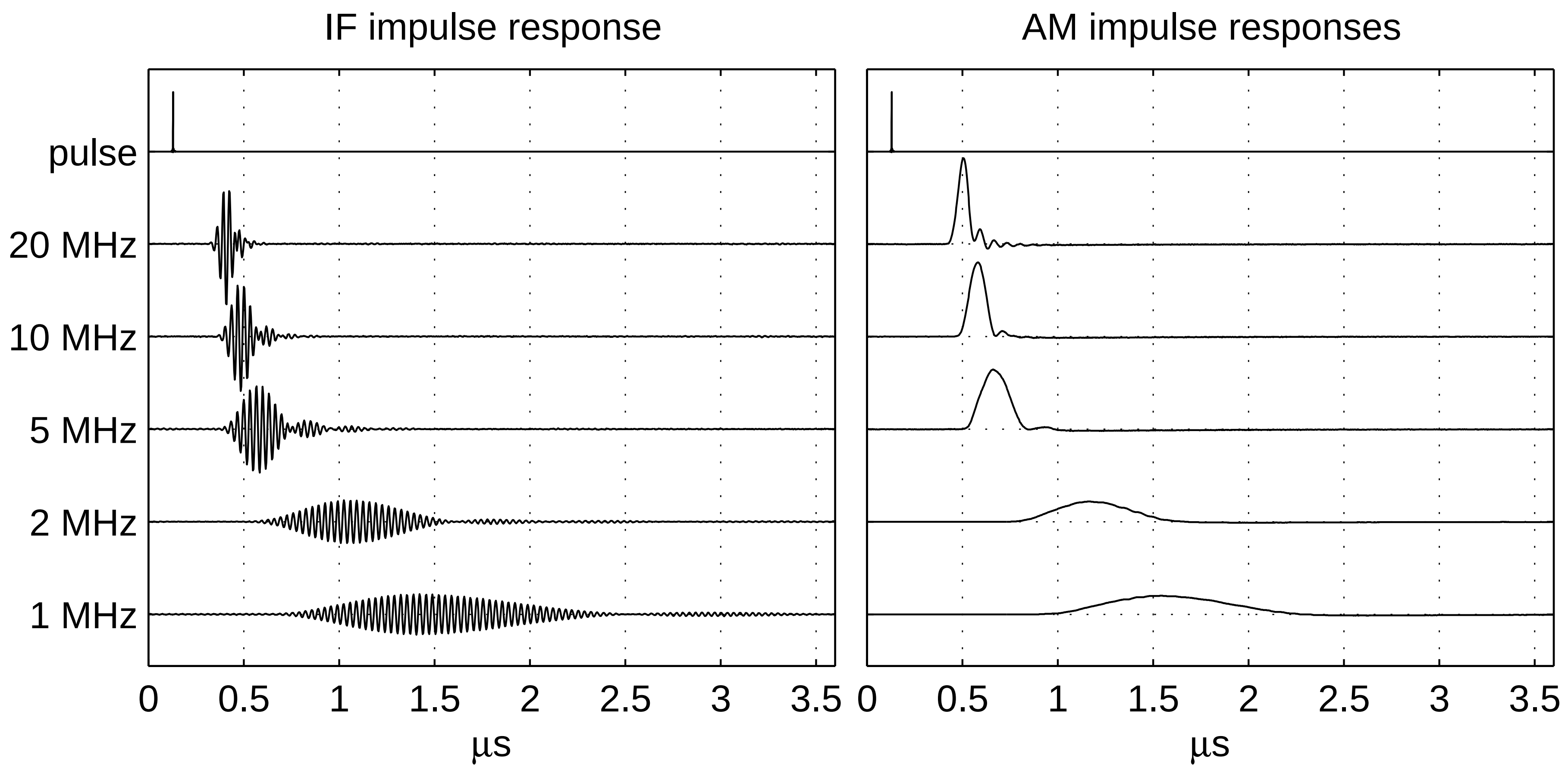
$\longrightarrow$ Demodulators: AM linear, AM logarithmic, FM, BFO.

$\longrightarrow$ Export controlled products, ≈ 30–100 k£
Second hand offers on Internet for < 1 k£

Intermediate frequency bandwidth



Receiving impulse signals



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

Video timing

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

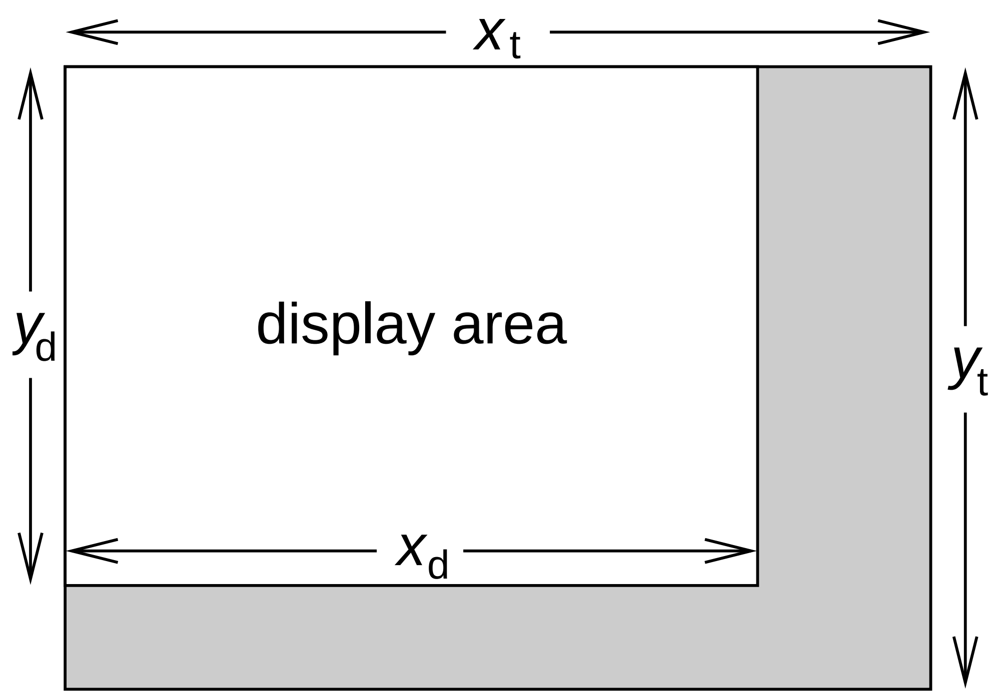
Pixel frequency: f_p

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 $\pm 0.5\%$.

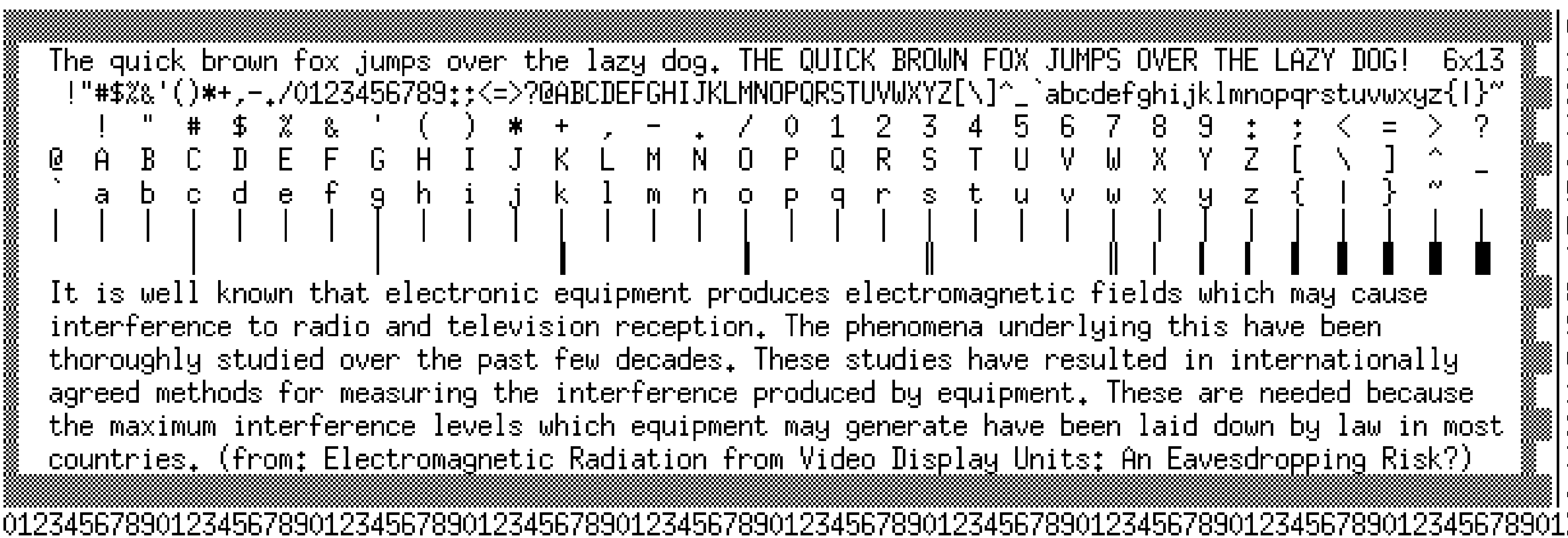
```
ModeLine "1280x1024@85"  157.5  1280 1344 1504 1728  1024 1025 1028 1072
```

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

Eavesdropping of CRT Displays

Cathode-ray tube monitors amplify with $\gg 100$ MHz bandwidth the video signal to ≈ 100 V and applies it to the control 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:

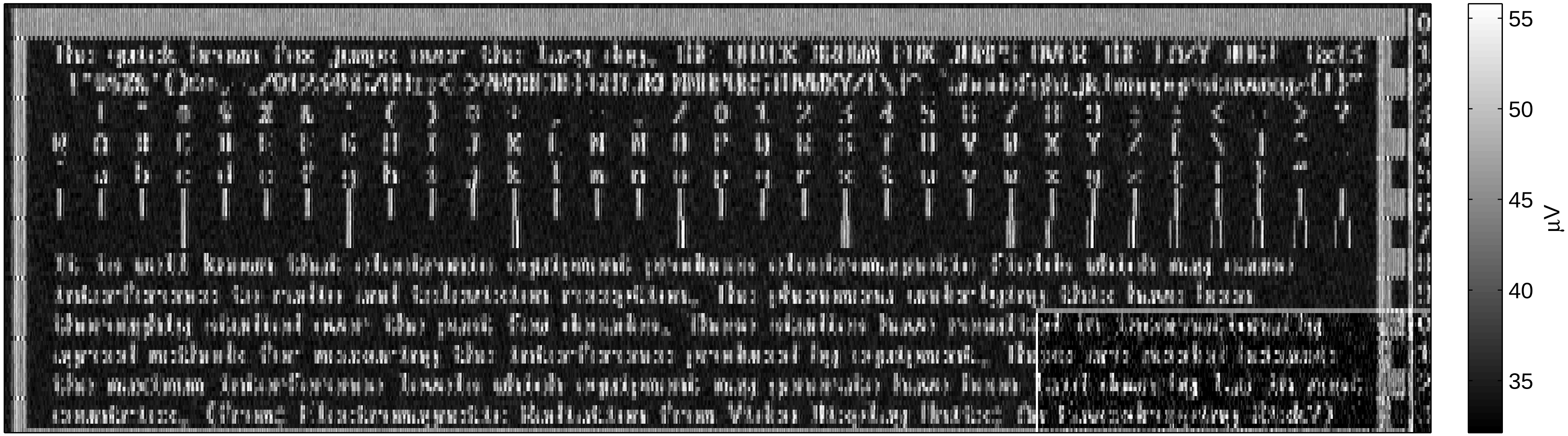


292 MHz center frequency, 20 MHz bandwidth, 256 (16) frames averaged, 3 m distance

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

Too low bandwidths blur the recovered image and limit readability.

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



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

AM receiver bandwidth equal to eavesdropped pixel rate distinguishes individual pixels.

Magnified example of eavesdropped text

Test text on targeted CRT:

The quick brown fox

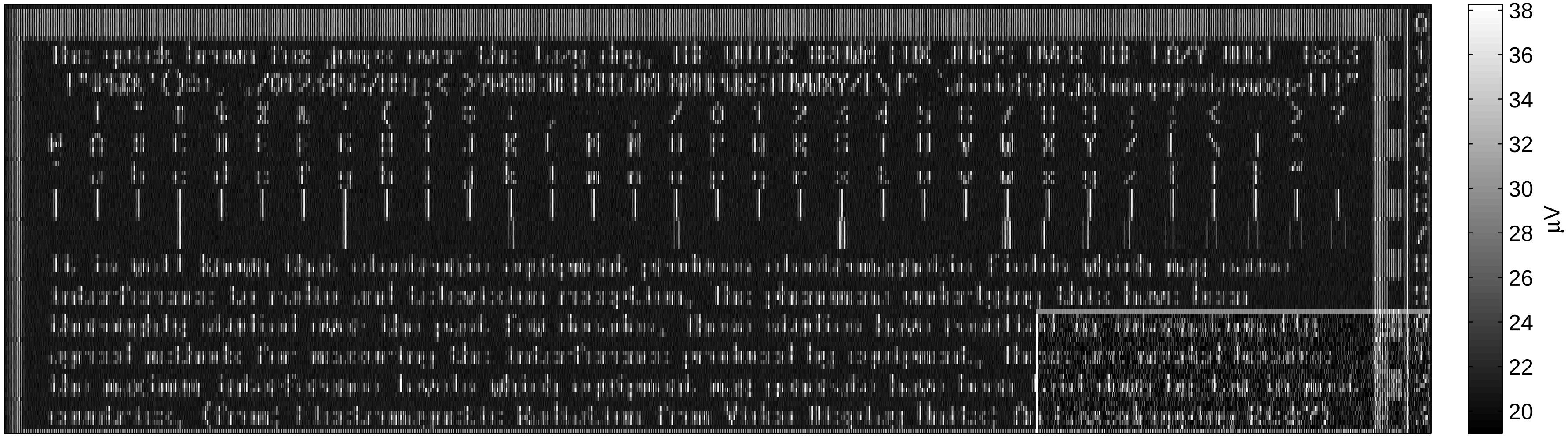
Rasterized output of AM demodulator at 480 MHz center frequency:

Characteristics:

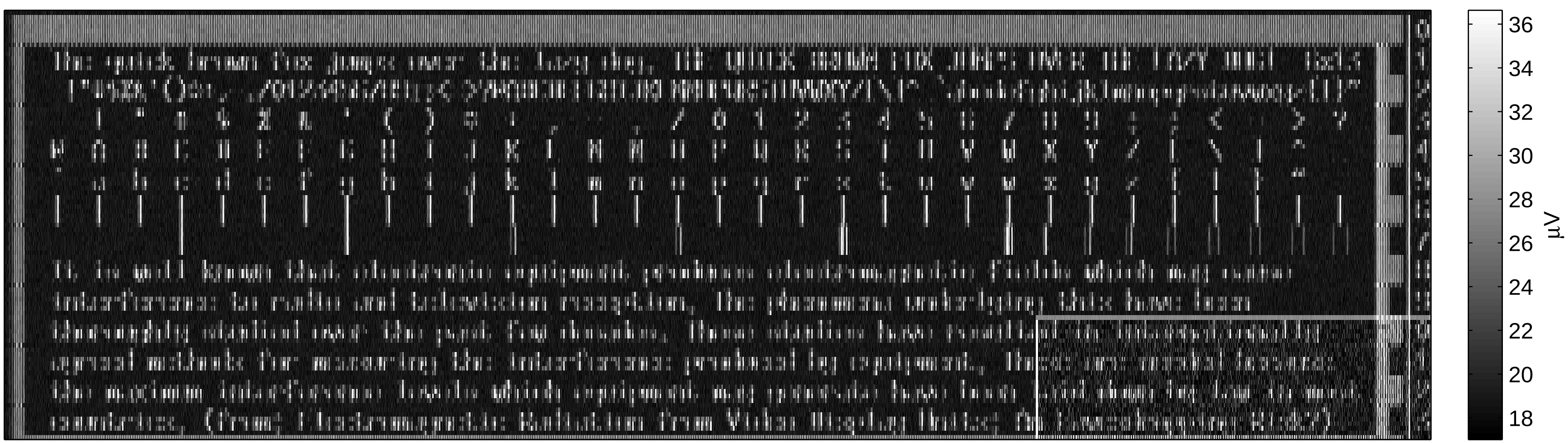
- → Vertical lines doubled
- → Horizontal lines disappear (reduced to end points)
- → Glyph shapes modified, but still easily readable unaided

Pixel frequency: 50 MHz, IF bandwidth: 50 MHz, AM baseband sampling frequency: 500 MHz, measured peak e-field at 3 m: 46 dBμV/m, corresponds to 12 nW EIRP. [Kuhn, 2003]

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



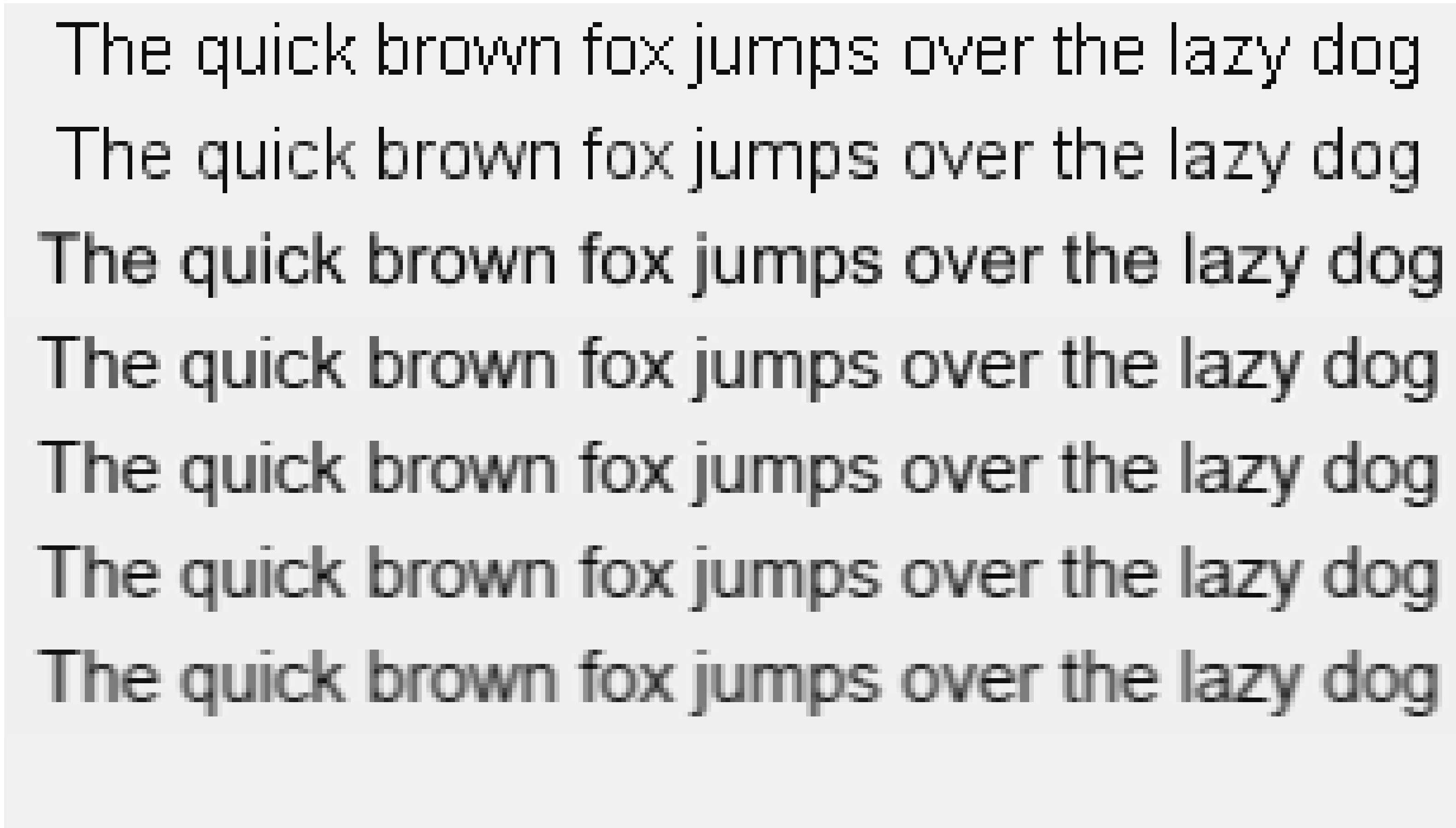
700 MHz center frequency, 100 MHz bandwidth, 256 (16) frames averaged, 3 m distance



Higher bandwidths provide sharper impulses, but no further information about pixel data.

Filtered fonts as a protection measure

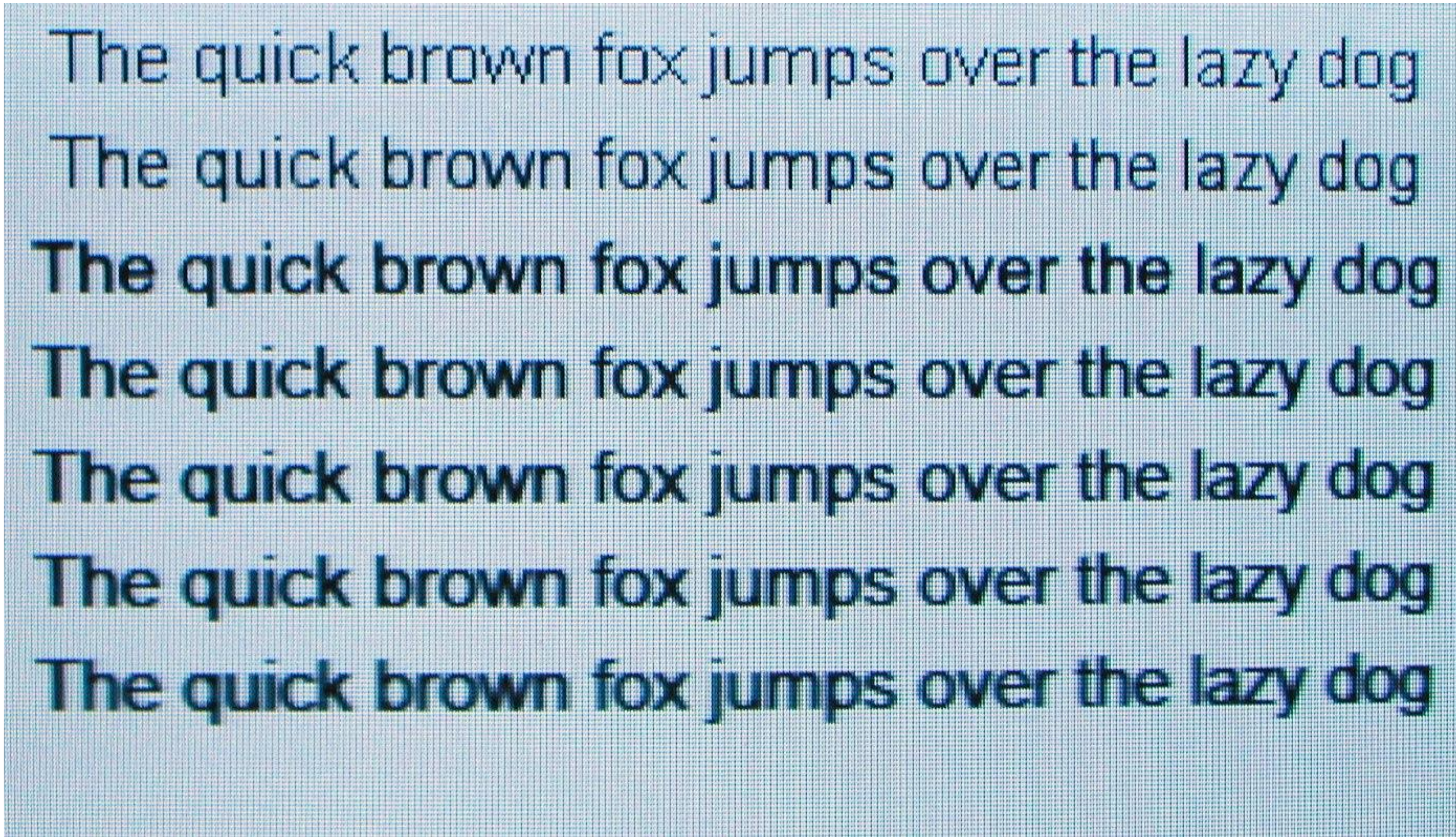
(1)
(2)
(3)
(4)
(5)
(6)
(7)
(8)



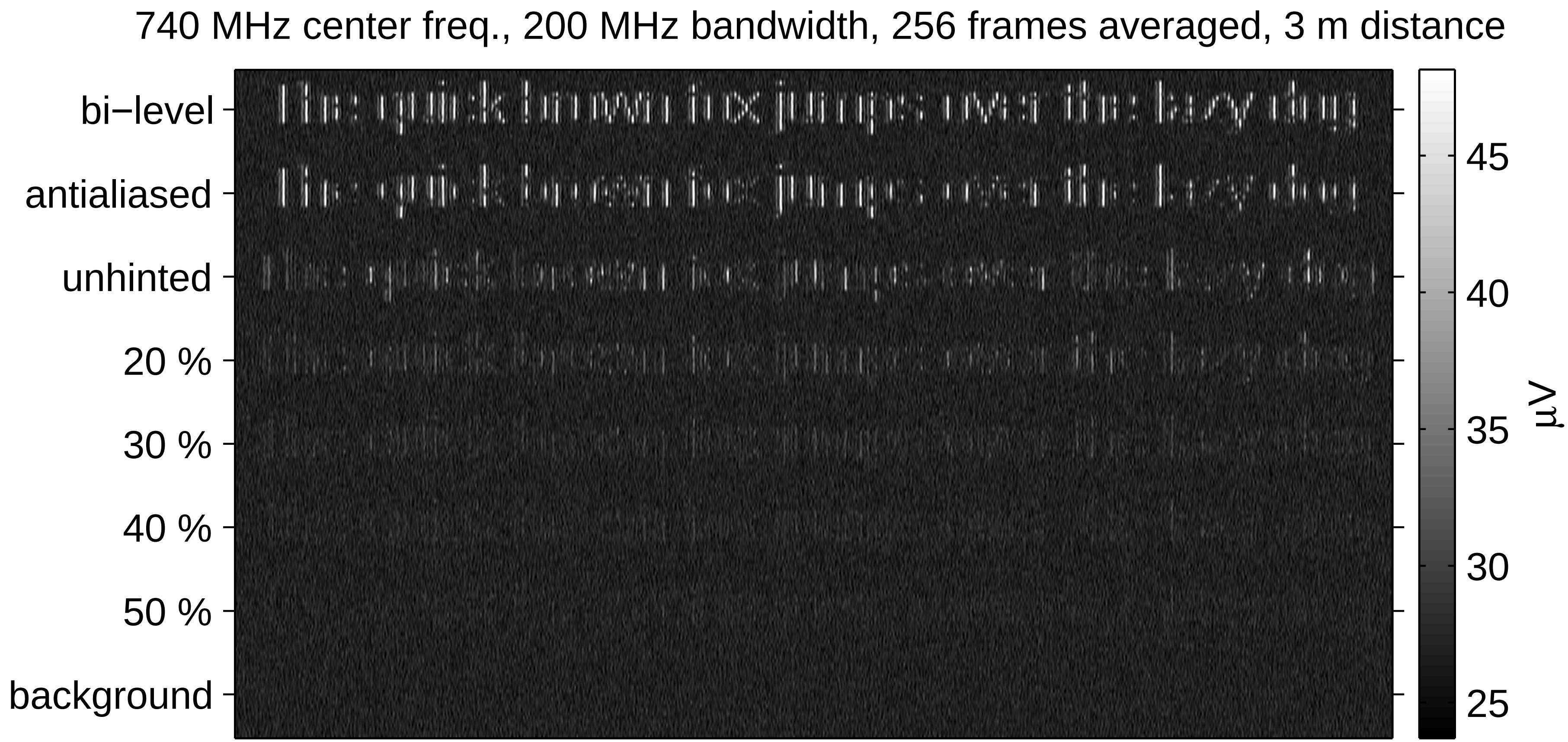
The above lines show (1) bi-level text, (2) anti-aliased text, (3) anti-aliased text without “hinting”, (4–7) anti-aliased text lowpass filtered to remove to 20, 30, 40, and 50 % of the spectrum $[0, f_{\mathrm{p}}/2]$, respectively. Font: Microsoft’s Arial (TTF), rendered at 12 pixels-per-em. [Kuhn, 2003]

Filtered fonts on the CRT screen

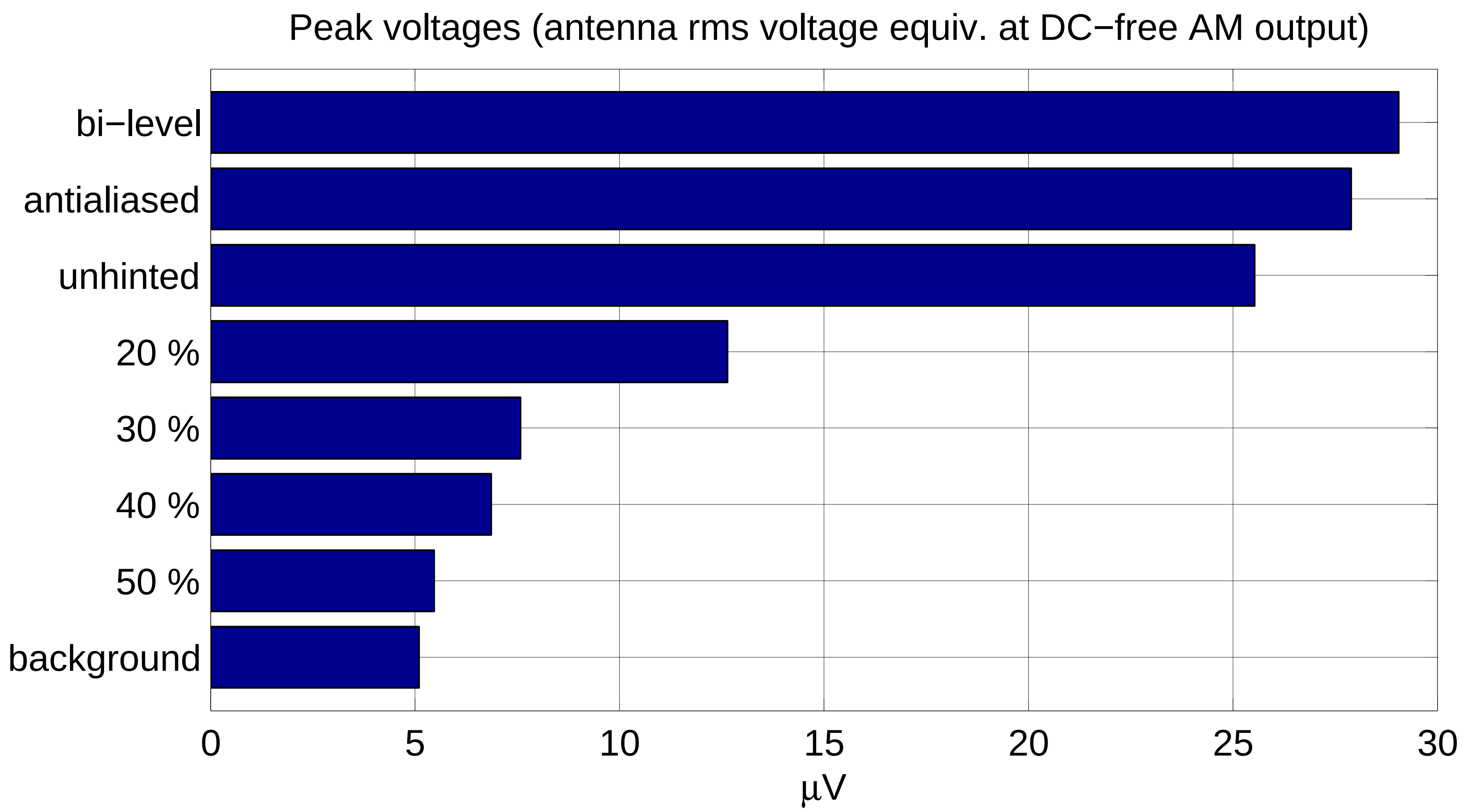
(1)
(2)
(3)
(4)
(5)
(6)
(7)
(8)



Received radio signal



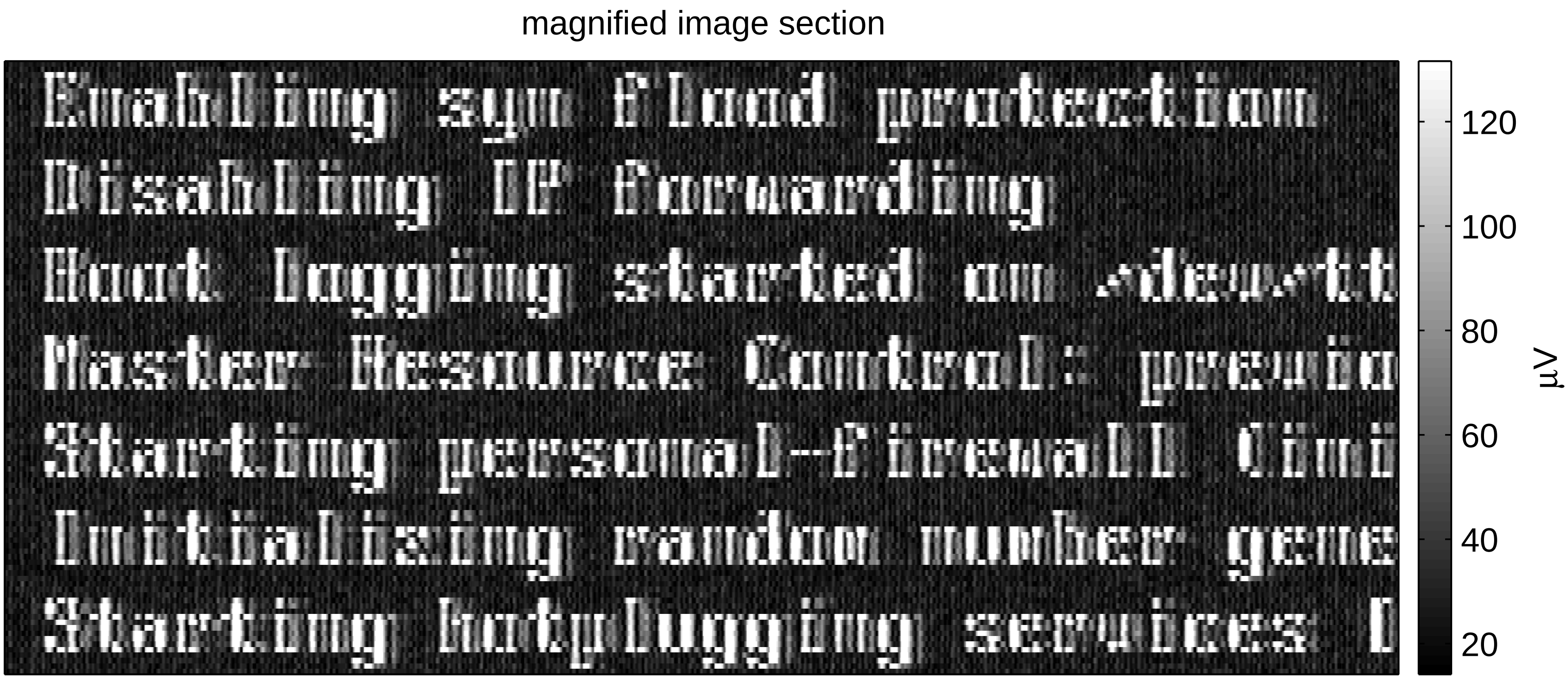
Filtered fonts peak-amplitude comparison



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.

Eavesdropping on flat panel displays

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



$\longrightarrow$ Horizontal lines intact ($\rightarrow$ no analog video signal)

$\longrightarrow$ Horizontal resolution reduced

$\longrightarrow$ 100 µV signal amplitude at receiver input (rms equiv.)

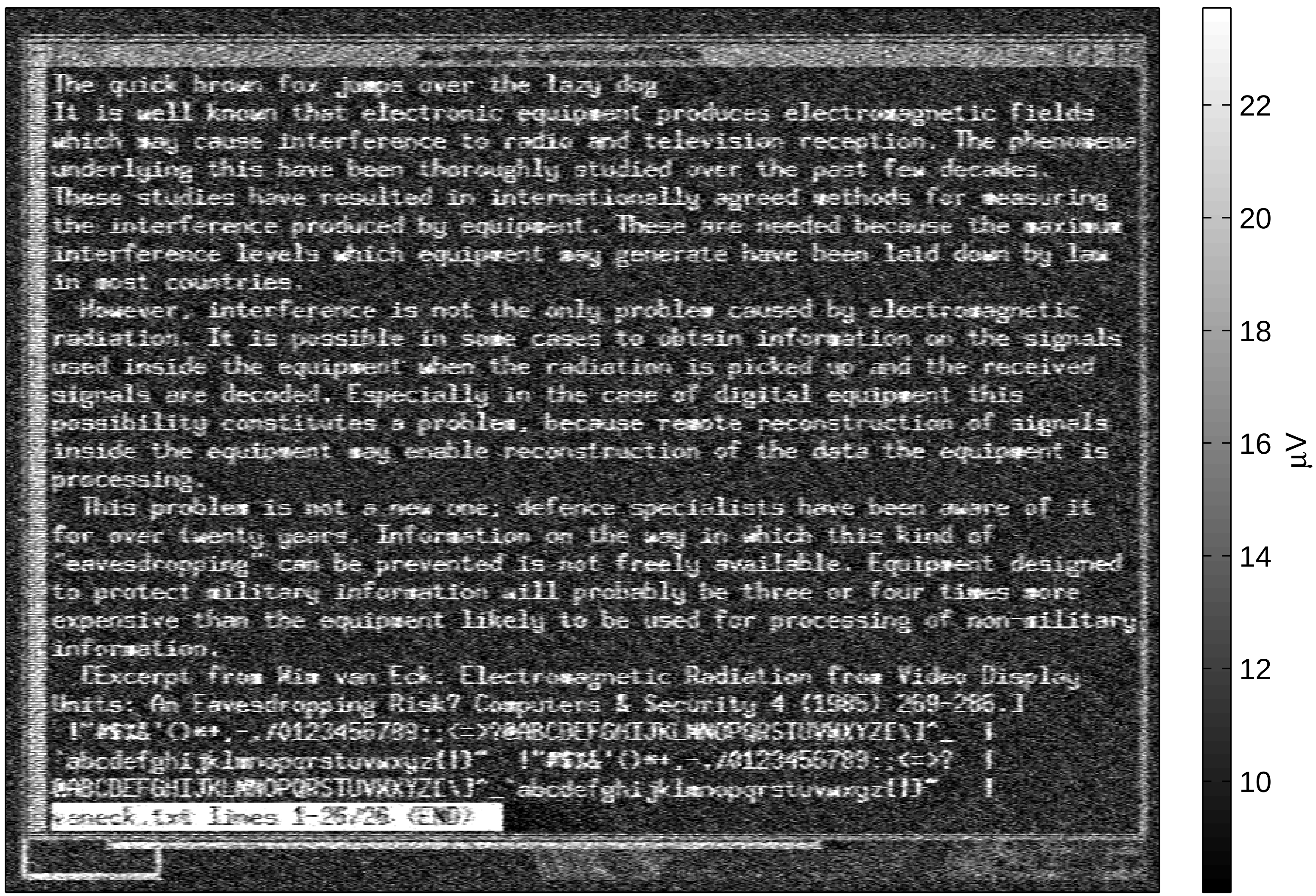
$\longrightarrow$ 57 dBµV/m (50 MHz BW) field strength at 3 m distance

$\longrightarrow$ equivalent isotropic radiated power (EIRP) about 150 nW

Target display: Toshiba 440CDX laptop, 800×600@75Hz, $f_{\mathrm{p}} = 50$ MHz

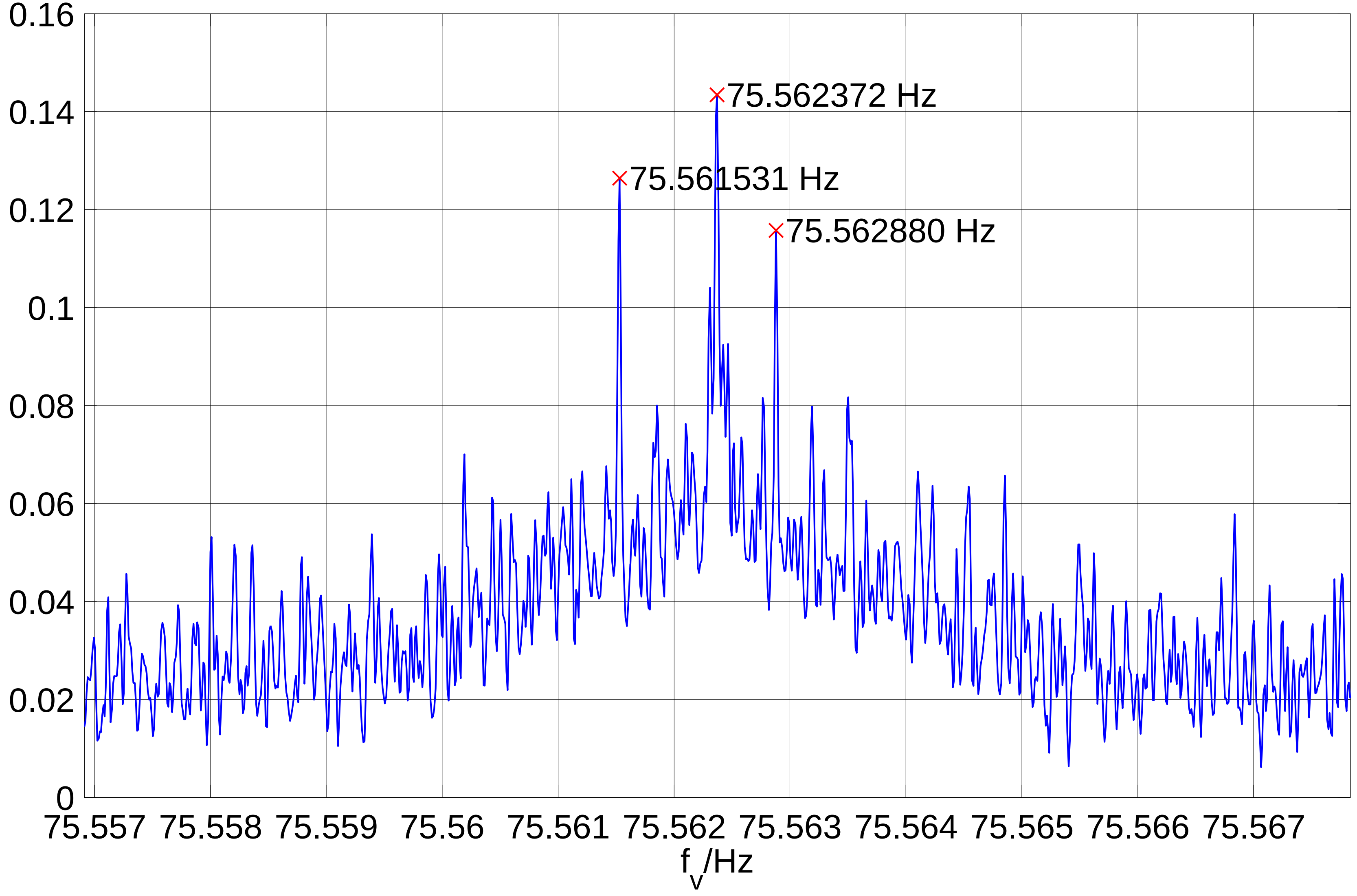
Eavesdropping across two office rooms

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



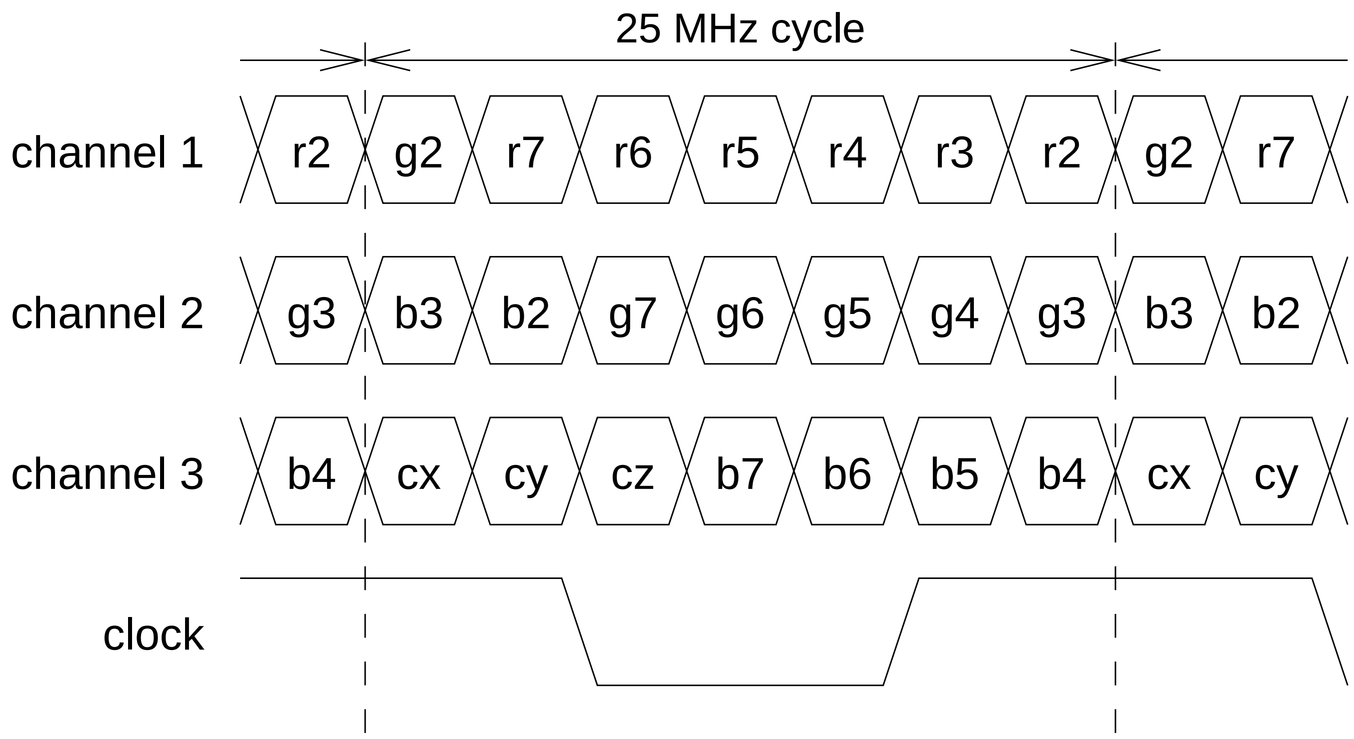
Target and antenna in a modern office building 10 m apart, with two other offices and three plasterboard walls (−2.7 dB each) in between. Single-shot recording of 8 megasamples with storage oscilloscope at 50 Msamples/s, then offline correlation and averaging of 12 frames.

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 long), which feed the 18-bit RGB parallel signal through the hinges via low-voltage differential signaling (LVDS, EIA-644).



FPD-Link chipset: NEC DS90CF581

FPD link parameters of example target

- $\longrightarrow$ pixel frequency: 50 MHz
- $\longrightarrow$ bits per pixel: 18
- $\longrightarrow$ parallel FPD-Links: 2
- $\longrightarrow$ FPD clock frequency: 25 MHz
- $\longrightarrow$ FPD bit rate: 7×25 MHz $= 175$ MHz
- $\longrightarrow$ total bit rate: $2 \times 3 \times 175$ MHz $=$ 1.05 Gbit/s

Therefore:

- $\longrightarrow$ 01010101...signal would broadcast harmonics at multiples of 87.5 MHz
- $\longrightarrow$ constant-color signal spectrum repeats every 25 MHz

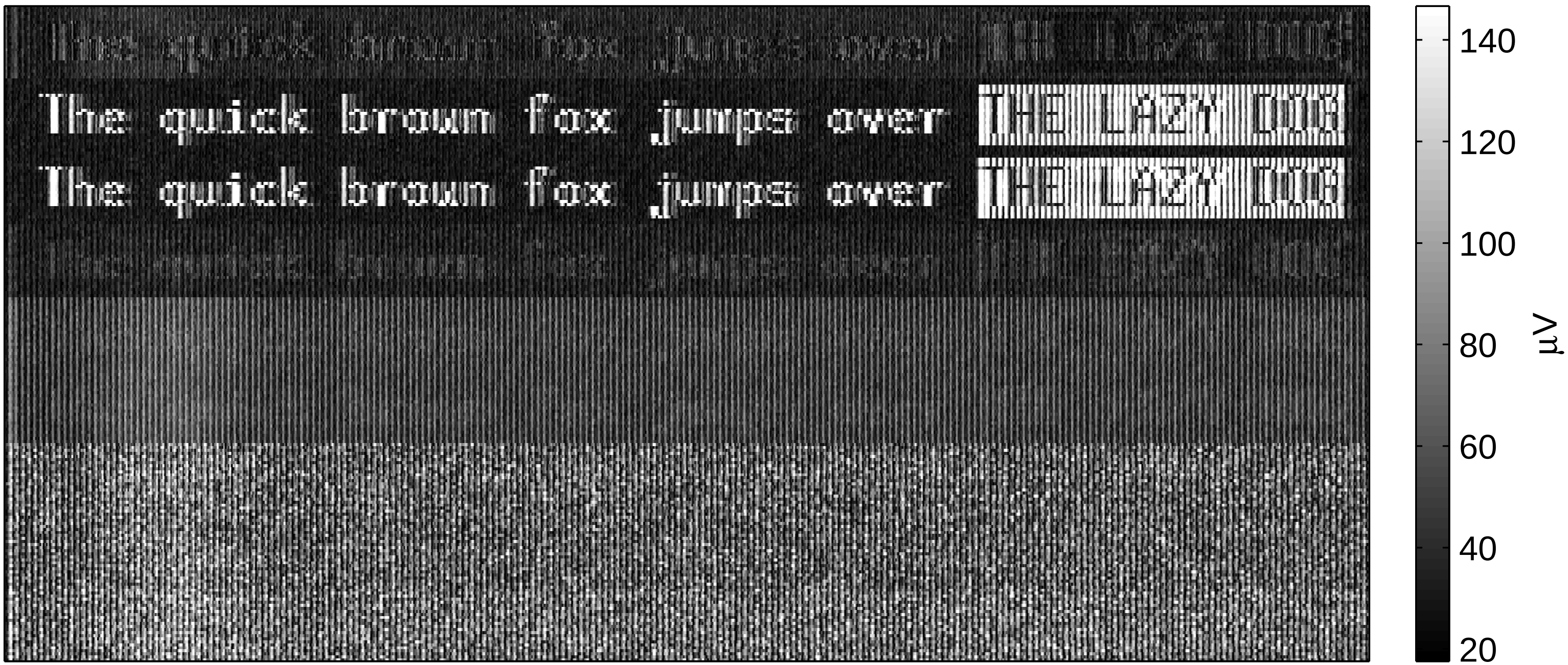
Minimal/maximal reception contrast

line	description	foreground		background	
		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

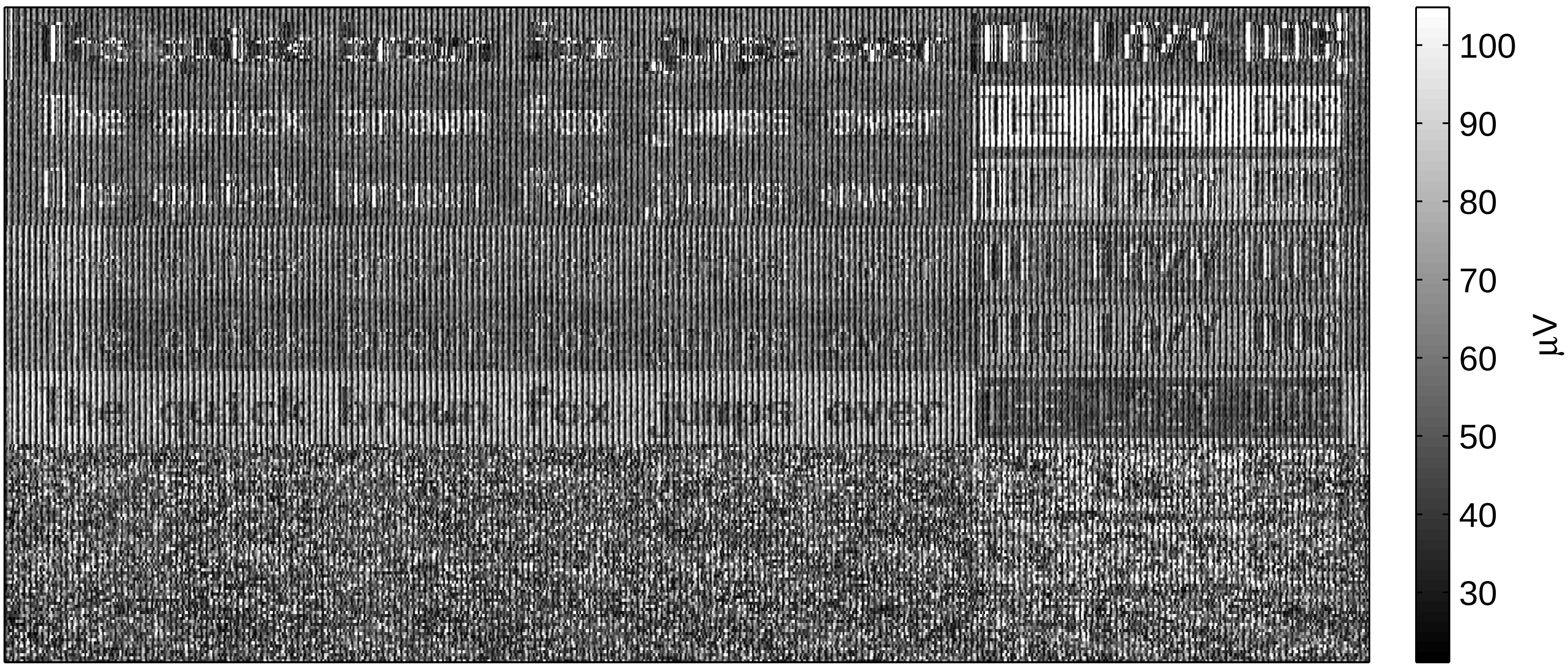
Minimal/maximal reception contrast

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



Only random bit jamming effective

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



Transition Minimised Differential Signaling (TMDS)

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

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

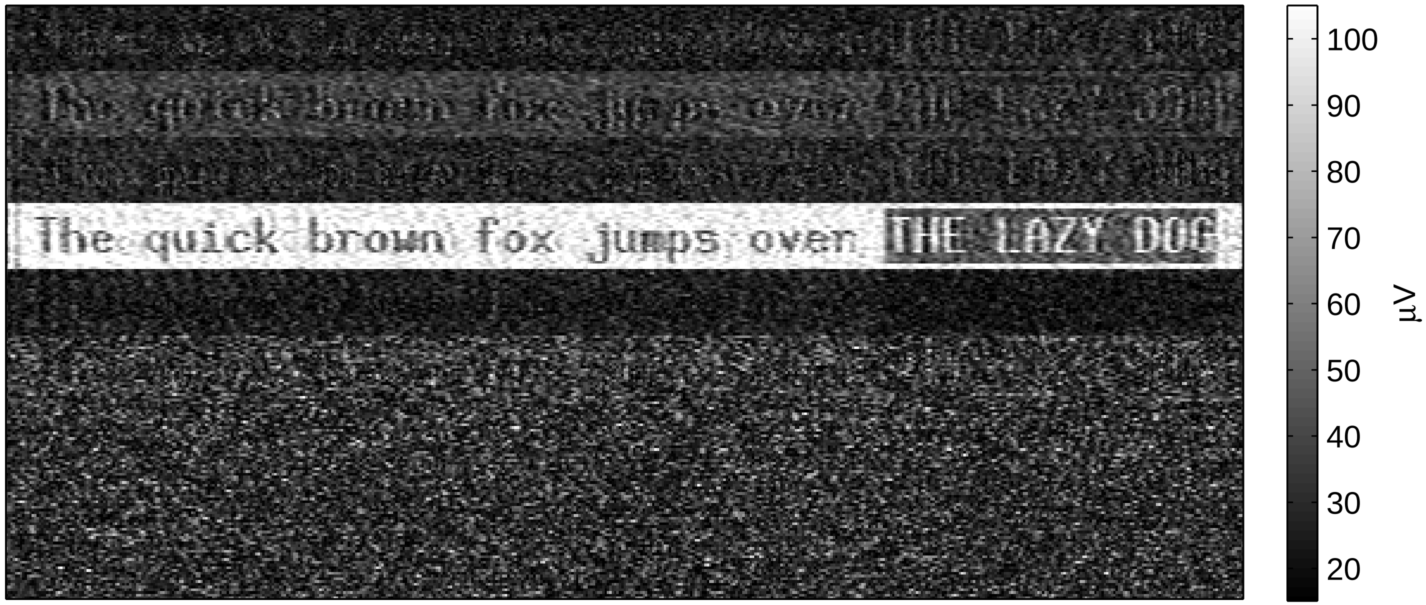
The DC balancing step adds encoding state and only 52 byte values lead to balanced words that are immune against the balancing algorithm.

High-contrast pair:

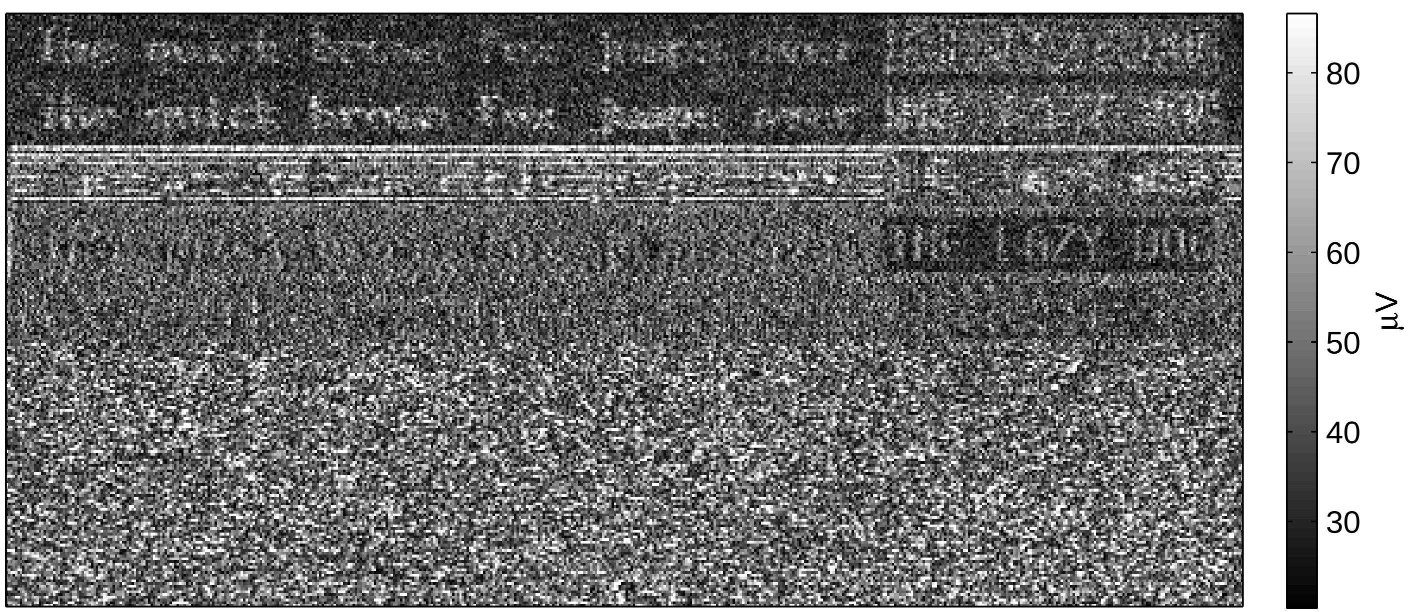
$$00001000, 00001000, \ldots \longrightarrow 0000111110, 0000111110, \ldots$$
$$10101010, 10101010, \ldots \longrightarrow 1100110010, 1100110010, \ldots$$

line	description	foreground RGB	background RGB
1	black on white	00 00 00	ff ff ff
2	maximum bit transition contrast	00 00 00	aa aa aa
3	half bit transition contrast	00 00 00	cc cc cc
4	balanced word, max contrast	10 10 10	55 55 55
5	minimum signal contrast	ff 00 00	00 ff 00
6	low nybble random	0r 0r 0r	fr fr fr
7	text in msb, rest random	—	—
8	text in green two msb, rest random	—	—
9	text in green msb, rest random	—	—

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



648 MHz center frequency, 100 MHz bandwidth, 5 frames averaged, 3 m distance



Random LSB jamming

Random bits can be added to a text image to generate a phase-locked jamming signal that cannot be averaged away by an attacker. Considerations:

→ Foreground/background colors with equal number of bit transitions.

→ Randomize less significant bits of each color channel.

→ These random bits must *only* be changed when the text changes:

- Changing the random bits continuously (like TV noise) would help the attacker to average away the jamming signal.
- Not changing the random bits when the text changes would help the attacker to average away the text and obtain this way a copy of the random signal that can then be subtracted from the received signal.

→ Independent noise bits must be used for *each* occurrence of a character. Beware of glyph caches from which the same bitmap might be used several times.

Open research question: How to jam without leaking update rate of displayed text?

Structure of compromising video signals

Mathematical tools:

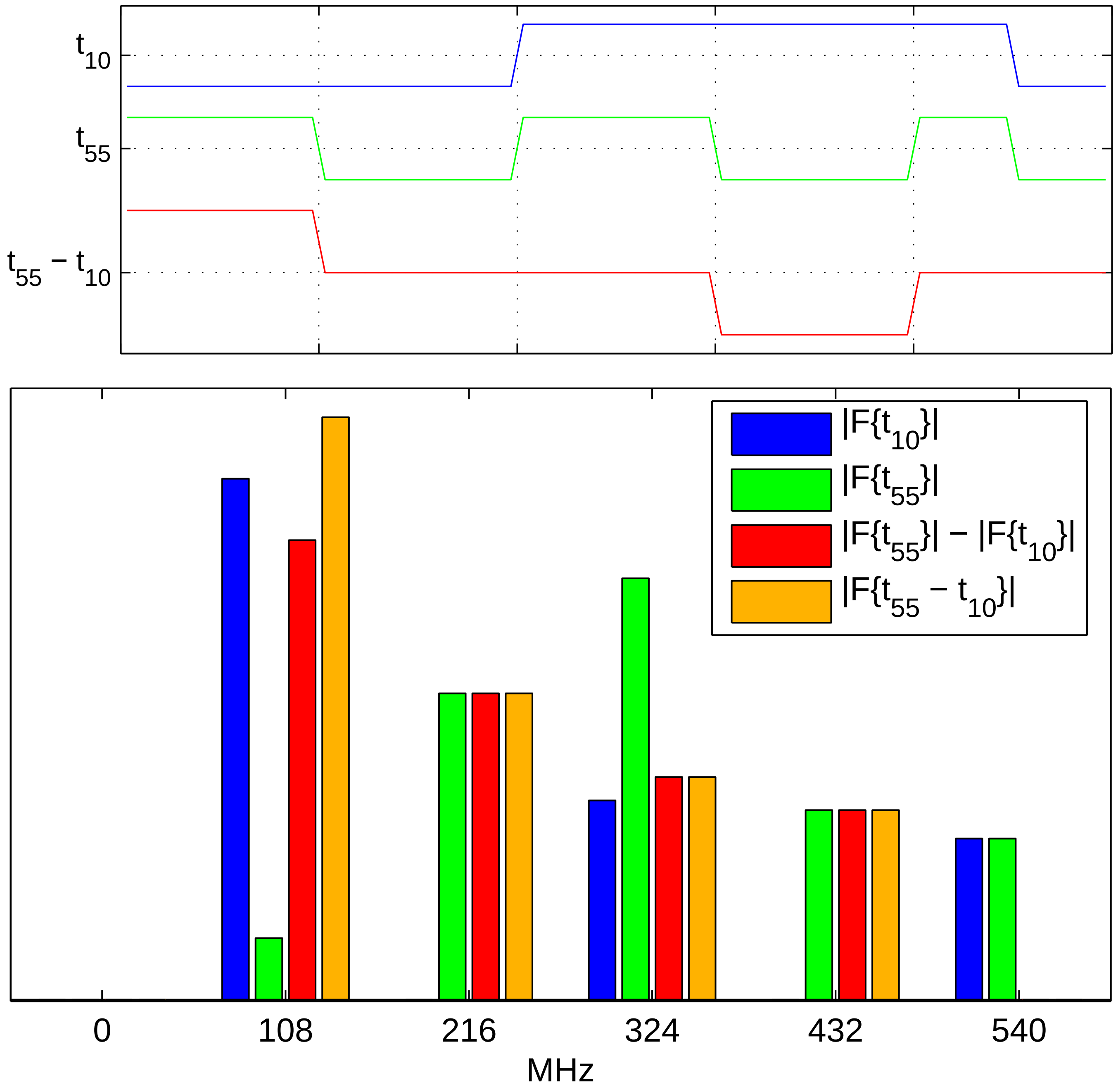
- $\longrightarrow$ Fourier transform: time domain $\leftrightarrow$ frequency domain
- $\longrightarrow$ Convolution theorem: multiplication in time domain is convolution in frequency domain, and vice versa.
- $\longrightarrow$ Sampling theorem: Sampled time-domain signal is periodic in the frequency domain, and vice versa.

Result:

- $\longrightarrow$ Symmetric spectrum of digital 2-color video signal repeats itself at frequency intervals f_p
- $\longrightarrow$ Amplitudes of the individual repetitions of the spectrum are predicted by the difference between the DFTs of the two color code words used.

$\Rightarrow$ Eavesdropping colors can be optimized to place signal energy into quiet part of UHF radio spectrum.

Details: M. Kuhn, Technical Report UCAM-CL-TR-577, 2003.



DVI signal in 1280×102460Hz video mode with $f_\mathrm{p} = 108$ MHz.

Conclusions

- → Digital video interfaces used with flat-panel displays can emit significantly stronger and better to decode signals than CRTs.
- → An understanding of the exact digital transmission format can be used for attack and defense, especially with stateful balanced codes.
- → High RF-contrast colors can be maliciously configured to simplify RF eavesdropping.
- → The selection of low RF-contrast colors is possible, but can have limited effectiveness with simple codes.
- → An effective low-cost software countermeasure are randomized less-significant bits as a correlated jamming signal.
- → Emission security remains a valid concern in applications with very high confidentiality requirements, predictable device usage, and easy longterm outsider access to nearby rooms/buildings.