Compromising Emanations of LCD TV Sets

Markus G. Kuhn

University of Cambridge, Computer Laboratory
15 JJ Thomson Avenue, Cambridge CB3 0FD, UK
http://www.cl.cam.ac.uk/~mgk25/

***Abstract*—This study attempts to characterize the radiated compromising emanations from four typical television sets with liquid-crystal display (LCD), in particular the predictability of format and timing parameters. Three were found to emit clear ultrahigh frequency radio signals visually related to the displayed image, from the display controller or its low-voltage differential signaling (LVDS) link to the LCD panel. Although the input signals to all four products followed the same TV standard, the timing parameters of their emanations differed substantially. Some also frequency-modulate their pixel clock to improve compliance with electromagnetic-interference limits. All digitally rescale the input image to the respective display size. The frame rate at which the display panel is driven is, if at all, only loosely phase locked to the input signal. These observations have implications for eavesdroppers, for the design of test standards to limit compromising emanations from video displays, and for the practicality of detecting the mere presence of an active television receiver by correlating the emanations of the circuitry driving its display panel with a known broadcast TV input signal.**

***Index Terms*—compromising emanations, emission security, information security, television receiver detection, video displays**

I. Introduction

ELECTROMAGNETIC waves unintentionally emitted by electronics not only can interfere with nearby broadcast-radio reception, a phenomenon known as electromagnetic interference (EMI), but also can leak processed information and thereby enable eavesdropping. Known as "compromising emanations", such radio signals have been studied and controlled by (still secret) "Tempest" emission-security standards in some government applications since the 1960s. While the problem is not limited to video displays, their compromising emanations are particularly easy to demonstrate. [1], [2], [3]

Most raster-display technologies periodically refresh each pixel at a fixed frequency, usually in the range 40–120 Hz. If the displayed information changes slowly compared to the refresh rate, the high redundancy of the refresh signal helps an eavesdropper to separate it from unwanted background noise, by periodic averaging. [2]

Where the information of each pixel is processed sequentially—one pixel at a time—successive samples from an eavesdropped signal can be attributed to individual pixels and therefore reconstructed as a raster image. In personal-computer (PC) displays, the standardized video interfaces (VGA, DVI, etc.) use a simple timing scheme. If $t_{0,0,0}$ is the time at which the information needed to refresh pixel $(0,0)$ in the top-left corner of the display is processed for the first time, then

$$t_{x,y,n} = t_{0,0,0} + \frac{x}{f_\mathrm{p}} + \frac{y}{f_\mathrm{h}} + \frac{n}{f_\mathrm{v}} \qquad (1)$$

(with $0 \le x < x_\mathrm{d}$ and $0 \le y < y_\mathrm{d}$) is the time when the information to refresh pixel (x, y) for the n-th time is processed. Here f_p is the pixel rate, $f_\mathrm{h} = f_\mathrm{p}/x_\mathrm{t}$ is the horizontal scan frequency (line rate), and $f_\mathrm{v} = f_\mathrm{h}/y_\mathrm{t}$ is the vertical scan frequency (frame rate). The eavesdropper needs to know the integer ratios x_t and y_t between the pixel, line and frame rate. These are larger than the visible display resolution x_d and y_d, to allow for horizontal and vertical blanking intervals in which the display has time to prepare refreshing the next line or frame. The PC industry has standardized a list of combinations $(f_\mathrm{p}, x_\mathrm{t}, y_\mathrm{t}, x_\mathrm{d}, y_\mathrm{d})$ [4], which eavesdroppers can try first, as well as a commonly-used formula for creating further such "video modes" where needed [5], which also helps guessing these parameters for a particular target. Then the eavesdropper picks a time $t_{0,0,0}$ such that the reconstructed image is appropriately aligned, and adjusts and tracks the exact pixel clock frequency f_p in order to deal not only with its 0.5% specification tolerance [4], but also its < 100 ppm manufacturing tolerance and its < 10 ppm short-term temperature drift. [2]

The eavesdropper can now average m voltage samples observed at the output of an amplitude modulation (AM) receiver at times $t_{x,y,0}, t_{x,y,1}, t_{x,y,2}, \ldots, t_{x,y,m-1}$ and display the results as a (suitably scaled) grey value of pixel (x, y) in the reconstructed raster image. In order to limit inter-pixel interference (horizontal blurring), the intermediate-frequency (IF) resolution bandwidth of the receiver used should ideally be of the same order of magnitude as f_p. [2]

The nature of the reconstructed image will depend on the type of signal eavesdropped:

- Analog video signals, such as from a Video Graphics Adapter (VGA) cable or a cathode-ray tube (CRT), usually appear to an eavesdropper with AM receiver as if they have been band-pass filtered and rectified: horizontal lines are reduced to peaks marking their end points and vertical lines are doubled. [2]
- Digital video signals, such as from laptop computers or Digital Video Interface (DVI) cables, undergo a complicated mapping from the bit pattern that encodes the displayed color to the grey value seen by the eavesdropper. This mapping varies with the center frequency to which the receiver is tuned and is related to the Fourier transform of the digital waveform. Where additional stateful encodings are used, such as Transition-Minimized Differential Signaling (TMDS) in DVI, the relationship can be even more complex. [3]
- Sometimes, video display hardware even amplitude modulates the pixel brightness onto a carrier, which can result

Final version in: IEEE Transactions on Electromagnetic Compatibility,
Vol. 55, No. 3, pp 564–570, June 2013. DOI 10.1109/TEMC.2013.2252353

in particularly good eavesdropped image quality. (The author observed this with a Dutch e-voting terminal in 2007, where the digital-to-analog converter circuit inside a VGA graphics controller chip emitted an amplitude-modulated version of the VGA video signal over its power lines. As a result, the eavesdropper saw an undistorted black-and-white version of the displayed image: the sum of the red, green, and blue components.)

Two reasons motivated this study of the nature of compromising emanations produced by a small sample of TV sets.

Firstly, while the emanations of PC video displays have already been documented, TV sets are also commonly used as large-format computer displays and could show noteworthy differences. After all, unlike PCs, TV sets are fed with an interlaced TV-standard video signal. Also, as integrated devices, their design is not constrained by the backwards-compatibility requirements of the PC industry.

Secondly, there is an eavesdropping application specific to TV sets. In some countries, TV broadcasters are financed by a receiver tax. Some TV licensing agencies equip their inspectors with technical means to detect TV sets in homes and business premises. One technique that has been used widely is to scan for emissions from the local oscillator (LO) of the superheterodyne tuner, which in European analog TV receivers typically oscillates 38.9 MHz above the received video carrier frequency (in the United States: 45.75 MHz). Such LO emissions typically have field strengths of 35–55 dBµV/m at 3 m distance [6], and can be detected 30–50 m away. (European Standard EN 550132 permits up to 57 dBµV/m.) Martin and Ward [7] give a detailed description of a 1980s-era British television detector van equiped to locate television receivers via such emissions; more recently handheld equipment has been deployed for the same purpose. Wild and Ramchandran [8] suggested to detect LO emissions from TV receivers in cognitive radio applications.

No single technique will detect every television set, especially as the technologies used diversify. Some now use direct ("zero IF") receivers, where the local oscillator frequency approximates that of the broadcast carrier, and is therefore difficult to separate from the latter. This motivates finding new ways to detect TV receivers and identify display content.

Enev, Gupta, Kohno and Patel [9] tested the power-line emissions of four plasma display and four LCD television sets and found in the amplitude spectrum, especially at 1–90 kHz, features that correlated with the displayed video image.

Optical sensors can analyze stray light from television screens that leaks through windows. In the case of cathode-ray tube displays, where pixels are updated sequentially, such diffusely reflected light can still allow the reconstruction of screen content [10]. With flat-panel displays (FPDs) that update pixel rows simultaneously, television reception can still be detected optically by correlating the emitted light over many seconds with the average brightness and color of the broadcast image. Both techniques depend on visibility of the window and low background light levels.

Can the compromising RF emissions of digital video cables found inside TV sets provide an alternative means to detect television reception? If these emissions were correlated in a highly predictable way with the (widely available) broadcast input signal of the receiver, this might allow the use of a correlator to automatically detect the location of a television set, even where noise levels do not permit the reconstruction of a recognizeable image. The correlation with a broadcast signal is crucial in this application, not just to increase sensitivity, but also to differentiate a working television receiver from computer displays that use very similar technology.

Fig. 1. Mikomi 15LCD250, Toshiba Regza 42C3030D, Samsung LE19R71B

II. Sample selection

The four LCD television sets (Mikomi 15LCD250, Samsung LE19R71B, Toshiba 42C3030D, Toshiba 42WLT66, Fig. 1) examined here were borrowed or bought in 2007 in the U.K. Their choice attempts to sample a range of prices, dimensions, and vendors. The two larger Toshiba models are used as presentation displays in meeting rooms, but were marketed as TV sets rather than computer displays.

Ideally, a target sample should systematically cover different technologies, panel and chipset families. But as consumer-electronic manufacturers make hardly any information available about the internal operation of their products, target devices had to be chosen using very limited catalogue data.

III. Architecture of LCD TV sets

All examined flat-panel television sets were based around two major integrated circuits, usually located on the same circuit board (see Fig. 2).

The first IC is a *front-end video processor*: it digitizes analog input signals (tuner IF, RGB, Y/C, baseband composite), demodulates and decodes them, and converts them into a digital format, such as ITU-656 [11], a 4:2:2 video bitstream with 13.5 MHz pixel-clock frequency. Such a chip may also contain a demodulator and MPEG decoder for Digital Video Broadcast (DVB) signals. The output still has the same standard resolution, line and frame rate as the input signal (standard definition TV in Europe: 576×720 pixels, 15.625 kHz horizontal, 50 Hz

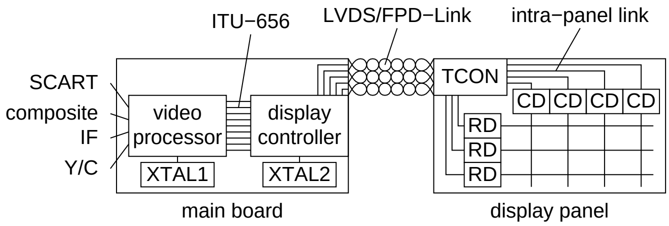

Fig. 2. Typical structure of an LCD TV set.

vertical, 625 lines total, interlaced). Many also integrate an on-chip CPU and graphics adapter, for controlling the entire TV, interactive menus, teletext, etc.

The second IC is a *display controller* back end. It performs several functions:

- The commonly used LCD panels in TV sets use PC-industry standard formats, such as 640×480 (VGA), 800×600 (SVGA), and in particular 1024×768 (XGA), 1366×768 (WXGA), or 1440×900 (WXGA+), and *not* the broadcast resolution (576×720 in Europe). The display controller has to convert the resolution and scan rate of the digitized TV signal provided by the front-end video processor into the resolution and line rate required by the display panel. If it keeps the field rate the same, the conversion needs to buffer only a few lines at a time. Better versions may buffer entire frames to implement filter algorithms for dealing with interlacing, which also allows adjusting the frame rate.
- Display controllers may offer several different resolution-scaling options, especially to cope with both the 4:3 and 16:9 aspect rations (letterboxing, zoom).
- Some display controllers also support computer interfaces such as VGA, DVI or HDMI, which allow the TV set to be used as a PC monitor.

The display controller outputs a digital video signal with the fixed resolution required by the display panel. The two are connected via a cable of twisted-pair wires, usually 10–50 cm long. Since about 1997, the signal levels on these cables have followed the low-voltage differential signaling (LVDS) specification [12], which represents 0 as a combination of 1.1 and 1.4 V on a wire pair, whereas 1 is encoded as 1.4 and 1.1 V instead. LVDS connections are terminated by a 100 Ω resistor and driven by a 3.5 mA current source. The examined display interfaces all followed the synchronization scheme used by National Semiconductors's FPD-Link system [13], which is also commonly used in laptop computers, namely one twisted pair carries a clock signal, and the others carry a data stream with a bitrate that is seven times the clock signal. Many different pin and bit assignments are used on these interfaces. The fact that several proposed standard assignments [14], [15], [16] did not match the LVDS pinout found in any of the examined products suggests that the standardization of such interfaces has yet to affect the market.

The FPD-Link connection ends in a third chip, the *timing controller* (TCON), which is located on the display panel itself. A display panel is a tightly integrated unit that combines a printed circuit board (often with flip-chip mounted ICs) with the actual liquid-crystal chamber and transparent panels, and is not easily examined in a non-destructive way. From the provided clock frequency the TCON chip generates timing signals for row-driver chips. It also demultiplexes the incoming video datastream and forwards it to a set of column-driver chips that contain digital-to-analog converters for each pixel column. Intra-panel interfaces used between TCON and column drivers initially used standard CMOS voltages, but EMI concerns have caused manufacturers more recently to move to specialized communication architectures, such as National Semiconductor's RSDS [17], WhisperBus and PPDS [18]. These use point-to-point links, where the data rate transmitted to an individual column-driver can be substantially lower than the pixel frequency, as each column driver needs to receive only a fraction of all pixels per line. Intra-panel interfaces are a less attractive source of compromising emanations than the FPD-Link panel interface, if

- the data for multiple columns is transmitted simultaneously (e.g., done in PPDS),
- the data rate and edge rise/fall times (which determine the upper end of the spectral presence of the data signal) are lower and longer,
- the tighter coupling to the ground plane of a printed circuit board (PCB) and the tighter manufacturing tolerances of PCB traces (compared to loose twisted-pair wires) reduce the impact of transmitter imbalance and large ground-return loops.

The most prominent compromising emanations appear to come from the display controller's LVDS drivers or the LVDS panel link, rather than from intra-panel circuits. What is received can be a common-mode signal on an imperfectly balanced LVDS pair, causing emissions via a ground loop. Being unintentional, both imbalances between LVDS driver pairs and ground return path conductivity can vary much between devices from the same production line.

IV. Instrumentation

This investigation of radio emissions has focused on the 200–850 MHz band, which covers the bit rate and its first harmonic and which permits good reception in the unshielded laboratory in which the measurements took place. A log-periodic EMC measurement antenna designed for 200–1000 MHz was placed 1–2 m from the surface of the tested TV set (far field) and vertical polarization provided among the best results. The radio receiver used was a Dynamic Sciences R1250, an older purpose-built Tempest measurement receiver with up to 20 MHz IF bandwidth. Its intermediate-frequency (IF) output was initially connected to a video raster processing system [19] that the author had built using a field-programmable gate array (FPGA) development board for digital signal processing (DSP) applications. It allows the user to quickly try all line frequencies that are an integer multiple of the standard TV field rate. It displays in realtime on a VGA multisync CRT monitor the received video signal and helps the experimenter to quickly scan through a wide range of tuning frequencies, antenna positions, and horizontal/vertical deflection frequencies, in order to get a quick overview of the available emissions.

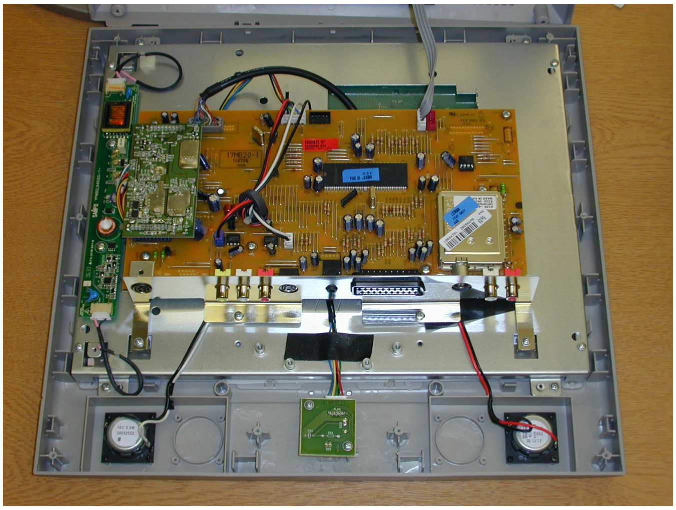

Fig. 3. Mikomi 15LCD25 LVDS link: the thick black cable near top center

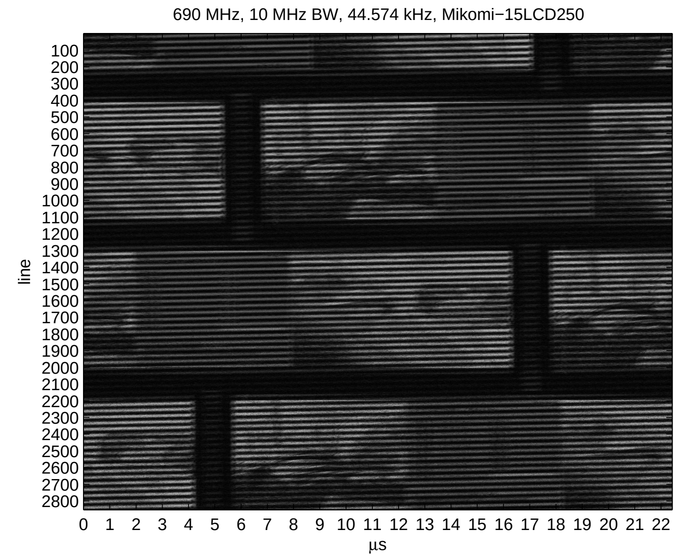

Fig. 4. Emissions of the Mikomi 15LCD25 while displaying a received terrestrial UHF PAL/I television program. The duration of the vertical blanking interval is not an integer multiple of the line duration, resulting in a horizontal jump after each frame. In the dark diagonal bands, the signal has left the receiver's IF bandwidth (see Fig. 5).

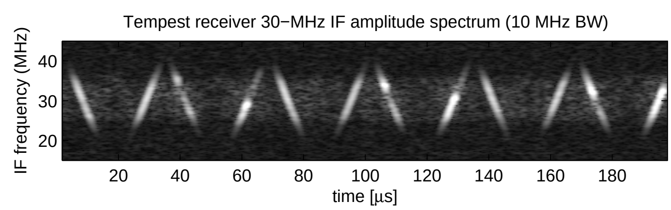

Fig. 5. IF spectrum of 15LCD25 emission (30 MHz IF $\hat{=}$ 690 MHz RF, 10 MHz bandwidth) showing triangle-wave frequency modulation of pixel clock.

To further characterize a promising signal, the 30 MHz IF output of the Tempest receiver was fed to a digital storage oscilloscope, which made at 125 MHz sampling frequency 200 ms long recordings, covering about 10 TV fields. For images like Fig. 4 and 7, these recordings were amplitude demodulated in Matlab (multiplication with complex 30 MHz phasor, low-pass filter, taking absolute value), interpolated according to equation (1), and converted into an 8-bit grey-scale raster image, using a manually adjusted line frequency f_h and trigger time $t_{0,0,0}$. No periodic averaging was used and y_d was increased to show several recorded frames below each other in a single image. The sample values were offset and scaled linearly for maximum contrast.

As the experiments focused on the format and timing of the emanations, no systematic attempt was made to document the signal levels observed. Where electrical field strength values are given in the text, they were obtained separately using a calibrated log-periodic antenna (Schwarzbeck VUSLP 9111B) connected to a spectrum analyzer (Rohde & Schwarz FSV7) with integrated pre-amplifier, configured to use an RMS detector in zero-span mode with equal resolution and video bandwidth. Emission sources were identified using H-field probes (Langer EMV-Technik XF1 set).

LVDS signals were characterized with a differential oscilloscope probe and 5 GHz sampling frequency.

V. Experimental observations

Target 1: Mikomi 15LCD25

The first target is a low-cost (£130) 15-inch LCD television set with a 1024×768 panel.[1] Its circuit consists primarily of two chips (Fig. 3), a front-end video processor Micronas VCT 49X36 and a display controller labelled TSU36AWL-M-LF.

A circa 20 cm long cable with 18 wires and ground shield connects the main PCB with the display panel. Ten of these wires carry LVDS signals. One pair carries an ≈ 49 MHz clock signal, the other four pairs carry digital video data at $49\ \mathrm{MHz} \times 7 = 343$ Mbit/s per pair ($4 \times 343\ \mathrm{Mbit/s} = 1.37$ Gbit/s). The LVDS video signal has recognizable inactivity (constant level) during vertical and horizontal blanking intervals, which appear with 50 Hz and about 44.57 kHz frequency, respectively.

RF scans revealed wide center frequency ranges (in particular 580–830 MHz) with a 50-Hz periodic video signal. The signal was strongest near 690 MHz, where the field strength at 1.5 m antenna distance varied in the range 46–58 dBµV/m (at 40 MHz bandwidth, vertical polarization), the lowest values appearing during blanking intervals. (In comparison, the noise floor with the TV set switched off was 43 dBµV/m.)

Near-field probing and rearranged cabling suggested that these emissions originate in the display controller on the main PCB. Unplugging the LVDS display cable from the main PCB was alone not sufficent to substantially reduce these emissions as long as another cable was still passing the display controller in close proximity.

On closer investigation the received video signal turned out to have around 891.5 lines per frame, leading to a line rate of $50\ \mathrm{Hz} \times 891.5 = 44575$ kHz. An example rasterization is shown in Fig. 4.

This raster image shows clearly that the horizontal phase jumps by about half a line (11 µs) after each field of 891 lines. It also shows that this phase jump is not exactly half a

[1]PCB inscriptions suggest it was manufactured by Vestel in Turkey.

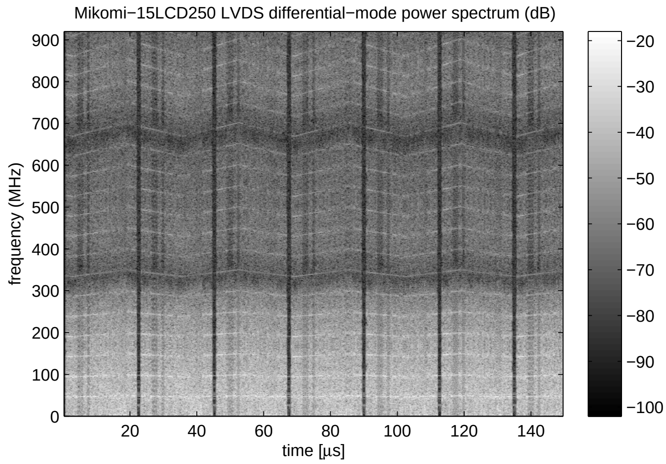

Fig. 6. Spectrogram of the differential data signal on one of the LVDS links in a Mikomi 15LCD25 TV set. The triangle waves are harmonics of the frequency-modulated 48–50 MHz pixel clock. The vertical gap every 22.4 µs is the horizontal blanking interval.

line, as after every second field, there is still a more than 1 µs large phase offset. As a result, a stable image cannot simply be reconstructed by rastering the received signal with a fixed horizontal deflection frequency, as is the case with the more regular video signals generated by personal computers.

Another deviation from computer-display practice, and also a potential problem for an eavesdropper, is that the pixel-clock frequency used on the LVDS link is not constant, but varies between 48.0 and 50.3 MHz. Its frequency increases and then decreases again linearly with time almost 30 000-times per second, in other words it is frequency modulated with a 29.5 kHz symmetric triangle waveform and a modulation index of about 2.3%. Deliberately frequency modulating a clock frequency with an ultrasonic signal helps to evade electromagnetic-interference regulations, such as CISPR 22. These judge emissions using a reference receiver with 120 kHz bandwidth and a "quasi-peak detector" with severely low-pass filtered AM-detector output. In this resolution bandwidth, the receiver will see only a small fraction of the moving clock signal and its harmonics at any time, and its detector will hardly react to the brief pulses caused when the clock frequency rapidly sweeps across.

The effects of the frequency modulation of the pixel-clock signal become apparent in two ways in Fig. 4:

Firstly, the frequency modulation also phase modulates the clock signal, which is apparent from the jittery edges within a single field. The start and end point of the active line varies by about 0.2 µs, or 1% of the mean line period, in comparison to a constant-frequency horizontal-sync signal.

Secondly, the entire frequency spectrum of the LVDS signal is scaled up and down slightly. Fig. 4 was received with a bandwidth of 10 MHz at a center frequency of 690 MHz, which is almost exactly twice the bit frequency of the data signal ($2 \times 7 \times 49\ \mathrm{MHz} = 686$ MHz). However, as this double-bitrate frequency varies between $2 \times 7 \times 48.0\ \mathrm{MHz} = 672$ MHz and $2 \times 7 \times 50.3\ \mathrm{MHz} = 704$ MHz, across 32 MHz, it will spend only some of the time within the 10 MHz receiver band. Where it is outside, the raster image shows dark bands distorting the displayed image. A look at a spectrogram of the receiver's 30 MHz IF output (Fig. 5) shows how the received signal moves up and down with a frequency of about 30 kHz, and sweeps about 30 MHz of the spectrum this way. Similarly, Fig. 6 shows a spectrogram of the signal recorded with a differential probe from one of the LVDS pairs, which shows the same frequency modulation.

The horizontal banding can be reduced by increasing the IF bandwidth of the eavesdropping receiver and can be made to disappear if the bandwidth is at least about 5% of the center frequency. It could also be avoided with a special-purpose receiver that tracks this frequency modulation with its tuning frequency (using a suitable phase-locked loop design).

An open question remains, whether there is any fixed phase relationship between the triangle-wave signal that frequency modulates the pixel-clock, and any of the other characteristic frequencies, or whether an eavesdropper would have to adjust and track all of these frequencies independently. Another uncertainty faced by an eavesdropper are the exact scaling factor (e.g., 4/3) and interpolation algorithm that the display controller uses to convert the 576 lines of the broadcast image into the 768 lines of the display, and how it deals with interlacing.

Target 2: Toshiba 42WLT66

The "HD-Ready" Toshiba 42WLT66 42-inch set has a 1366×768-pixel display, with both TV and VGA inputs.

Recognizable video signals with 50 Hz and 56.7475 kHz (1134.95 lines) were found over a wide range of RF tuning frequencies, including 256, 288, 375, 447, 511, 765, and 830 MHz. Fig. 7 shows that the horizontal sync signal at which the flat-panel is driven makes an $\approx$1 µs phase jump in the vertical blanking interval after every second field, but the pixel clock is far more stable than with the previous target. While contours are clearly visible, the non-monotonic relationship between the brightness of the TV image and the resulting AM demodulator output of the eavesdropping receiver severely alters the image content, as is to be expected with eavesdropping any digital video signal [3].

Target 3: Toshiba 42C3030D

While the Toshiba Regza 42C3030D is another "HD-Ready" 42-inch television set with 1366×768 pixels resolution, in external appearance and technical data very similar to the previous target, its compromising video emanations use very different parameters: a much lower line frequency of 47.400 kHz and a smaller phase jump in the horizontal sync signal after each second field. The signal received was noticeably weaker and distorted by rapidly moving dark bands, again most likely an artifact caused by EMC-motivated frequency modulation of the clock frequency.

The two core chips are a DVB-T front-end video processor Toshiba TC90403FG and a Genesis FLI8548H-LF video controller which feeds the LVDS cable consisting of five twisted pairs, one with a 72 MHz clock signal and four $72\ \mathrm{MHz} \times 7 = 500$ Mbit/s data links (2 Gbit/s combined).

Television set	x_d	y_d	$\frac{f_\mathrm{v}}{\mathrm{Hz}}$	$\frac{f_\mathrm{h}}{\mathrm{kHz}}$	x_t	y_t	$\frac{f_\mathrm{p}}{\mathrm{MHz}}$
Mikomi 15LCD25	1024	768	50.0	44.5740	≈ 1140	891.48	49.2 ± 1.2
Samsung LE19R71B	1440	900	41.8	44.0256	≈ 1550	1053	$2 \times (34.2 \pm 0.8)$
Toshiba 42WLT66	1366	768	50.0	56.7475	?	1135	(not measured)
Toshiba 42C3030D	1366	768	50.0	47.4000	≈ 1530	948.0	72.5 ± 0.9

TABLE I
SUMMARY: DISPLAY RESOLUTIONS AND LVDS TIMING PARAMETERS IN FOUR EXAMINED TV SETS, ALL FED WITH A 50 HZ PAL/I TV SIGNAL

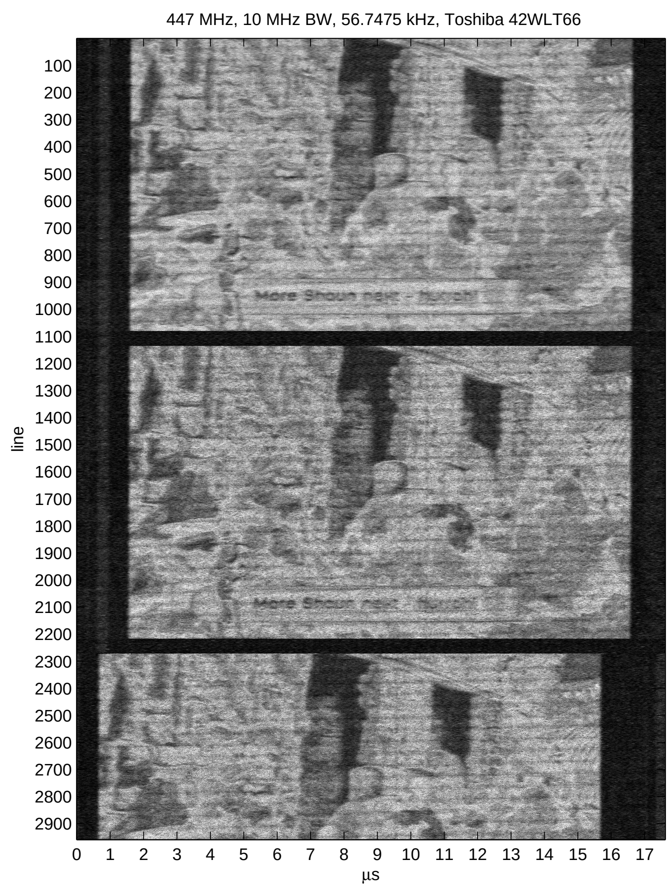

Fig. 7. Toshiba 42WLT66 emissions while receiving BBC1 (PAL).

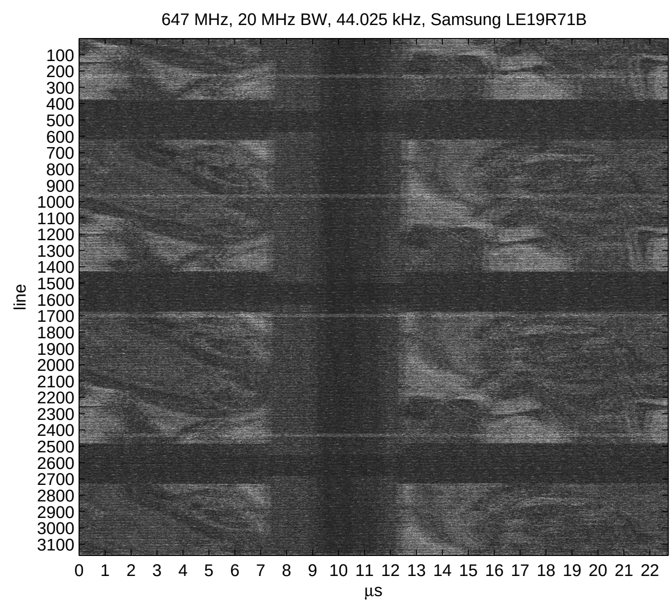

Fig. 8. LVDS emissions of the Samsung LE19R71B while displaying a received TV image, which became visible only after an RF choke ring was removed from the LVDS connection.

Television set	$\frac{\min f_\mathrm{p}}{\mathrm{MHz}}$	$\frac{\max f_\mathrm{p}}{\mathrm{MHz}}$	$\frac{f_\mathrm{p}}{\mathrm{MHz}}$	$\frac{f_\mathrm{FM}}{\mathrm{kHz}}$
Mikomi 15LCD25	48.0	50.3	$49.2 \pm 2.3\%$	29.5
Samsung LE19R71B	33.4	35.0	$34.2 \pm 2.3\%$	15.7
Toshiba 42C3030D	71.6	73.4	$72.5 \pm 1.2\%$	29.3

TABLE II
SUMMARY: FREQUENCY MODULATION OF LVDS CLOCKS

Target 4: Samsung LE19R71B

Finally, the Samsung LE19R71B is a mid-range (£350) 19-inch TV set with a 1440×900 pixel panel. It had the weakest emissions from the LVDS link, barely recognizable at more than 1–2 m distance in our (unshielded) laboratory. It was the only examined device that featured a ferrite choke around all LVDS links, which appears to substantially reduce common-mode currents and resulting compromising emanations. Its 11 cm LVDS cable was also the shortest.

Only after removing this ferrite ring the LVDS emanations became as prominent as with the others (Fig. 8). The frame rate of 41.8 Hz was exactly 1053-times lower than the line rate of 44.0256 kHz. Unlike the other TV sets, the raster signal emitted by this LVDS interface did not show a regular phase jump after every frame or field. However, the image does make an apparently random horizontal phase jump in irregular intervals, in the order of one per second. The LVDS clock signal of 34.2 MHz was triangle-wave frequency modulated with a peak deviation of 0.8 MHz. The data rate on the remaining six twisted pairs was $34.2\ \mathrm{MHz} \times 7 \approx 240$ Mbit/s.

The main chips are a Micronas VCT 49X3R front end video processor and a video controller labelled SE6181LA-LF. The design showed more EMI countermeasures, such as added metal shielding, than the other TV sets.

There was a very weak second emitted video signal at a line frequency of 31.250 kHz (exactly twice the PAL line frequency). Only about 9 µs of the 32 µs that are available at this rate for each line seem to be actually used to transfer image data. This narrow strip showed the same scene motion as the displayed image, but is split into 8–9 distinct vertical stripes, which appear to encode different parts of the image (Fig. 9). The link between the two main chips is an obvious candidate source for this second signal.

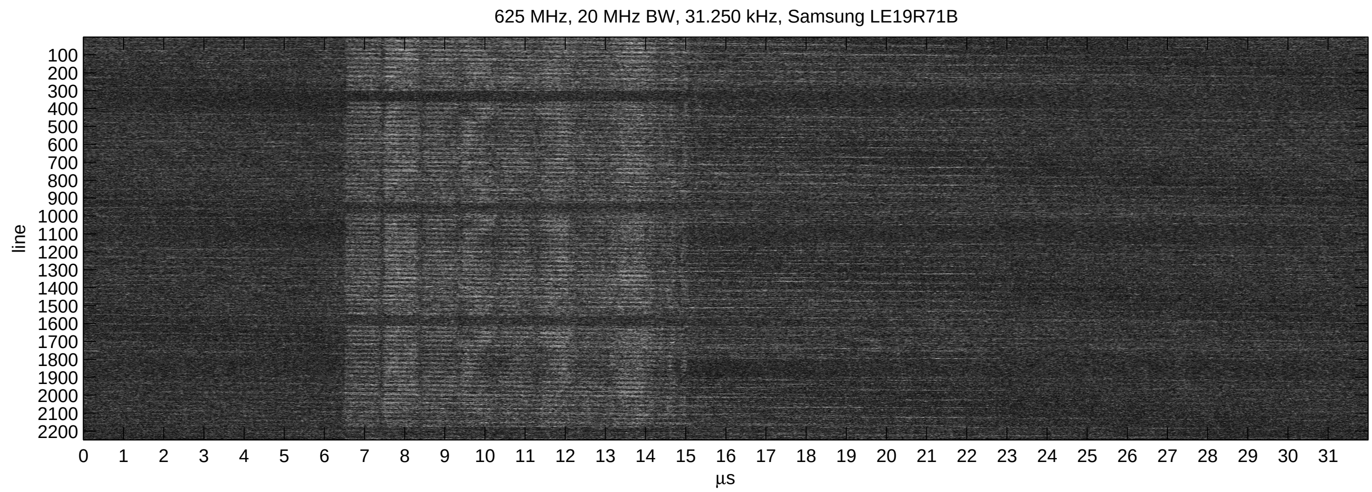

Fig. 9. Non-LVDS emissions of the Samsung LE19R71B (displaying TV image).

VI. Conclusions

Considering that all examined television sets were fed with the same TV standard (PAL/I), the results show a surprising diversity of internally-used video frequencies on the LCD TV market. Of the four television sets examined, no two shared the same internal line rate (Table I).

But there are further complications for a video-signal eavesdropper. One is that the line rate is not always an integer-multiple of the frame rate; there tend to be model-specific phase jumps in the horizontal synchronization of the emitted signal after each field, after each second field, or at seemingly random points. In addition, the borders of the horizontal blanking interval can jitter substantially. This shows a very loose phase coupling of the input and output hsync signals of the scan-rate conversion chips used. It is caused primarily by the frequency modulation of the output clock signal as an EMC measure (Table II), but might also be compounded by the fact that in most cases the front-end and back-end chips have their own clock oscillators.

Each of these observations means a substantial complication for anyone who wants to separate a compromising LVDS signal of an LCD TV from background noise through periodic averaging. The high diversity of the timing parameters and the jitter on the synchronization signals also makes it difficult to envisage an automatic TV detector predicting from a broadcast TV signal the LVDS emanations of a TV set, in order to detect them at a distance using cross-correlation techniques, especially if the operation of the TV set is driven by its own crystal oscillators and only loosely phase-locked with the frame rate of a broadcast signal. Moreover, simple EMC measures, such as careful layout and ferrite rings, can substantially reduce compromising emanations from display controllers and LVDS links.

References

[1] W. van Eck, "Electromagnetic radiation from video display units: an eavesdropping risk?," Computers & Security, Vol. 4, pp. 269–286, 1985.

[2] M. G. Kuhn, "Compromising emanations: eavesdropping risks of computer displays," Chapter 3: Analog video displays. Technical Report UCAM-CL-TR-577, University of Cambridge, Computer Laboratory, December 2003.

[3] M. G. Kuhn, "Electromagnetic eavesdropping risks of flat-panel displays," 4th Workshop on Privacy Enhancing Technologies, 26–28 May 2004, Toronto, Canada, Proceedings, LNCS 3424, pp. 88–105, Springer-Verlag. http://www.cl.cam.ac.uk/~mgk25/pet2004-fpd.pdf

[4] DMT 1.0, Rev. 12, "Monitor timing specifications," VESA-2008-10, Video Electronics Standards Association.

[5] CVT 1.1, "Coordinated Video Timings," VESA-2003-9, Video Electronics Standards Association.

[6] R. Drinkwater, M. Killow, "Measurement of local oscillator emissions from a range of domestic television receivers in accordance with the requirements of British Standard EN 55013," Project No. 466, final report, Radio Technology & Compatibility Group, Radio Communications Agency, United Kingdom, April 1998.

[7] K. Martin, S.A.L. Ward, "Television detector vans," British Telecommunications Engineering, Vol 3, pp. 180–186, October 1984.

[8] B. Wild, K. Ramchandran, "Detecting primary receivers for cognitive radio applications," First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, Baltimore, MD, USA, November 2005.

[9] M. Enev, S. Gupta, T. Kohno, S. N. Patel, "Televisions, video privacy, and powerline electromagnetic interference," Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS'11), Chicago, IL, USA, October 2011, pp. 537–550.

[10] M. G. Kuhn, "Optical time-domain eavesdropping risks of CRT displays," Proceedings 2002 IEEE Symposium on Security and Privacy, Berkeley, California, 12–15 May 2002, IEEE Computer Society, pp. 3–18, ISBN 0-7695-1543-6.

[11] "Interfaces for digital component video signals in 525-line and 625-line television systems operating at the 4:2:2 level of Recommendation ITU-R BT.601 (Part A)," ITU-R Recommendation BT.656-4, 1998, International Telecommunication Union, Geneva.

[12] ANSI/TIA/EIA-644-A, "Electrical characteristics of low voltage differential signaling (LVDS) interface circuits".

[13] S. Poniatowski, "An introduction to FPD Link," National Semiconductor, Application Note 1032, July 1998.

[14] "Industry standard panels – Mounting & top level interface requirements, Version 2," Video Electronics Standards Association (VESA), Sep. 2001.

[15] "VESA TV Panels Standard, Version 1," Video Electronics Standards Association (VESA), March 2006.

[16] "VESA DisplayPort Panel Connector Standard, Version 1," Video Electronics Standards Association (VESA), January 2007.

[17] "RSDS 'Intra-panel' interface specification, Revision 1.0," National Semiconductor, May 2003.

[18] C. Zajac, S. Poniatowski, "A new intra-panel interface for large size / high resolution TFT-LCD applications." Texas Instruments, SNLA177.

[19] M. G. Kuhn, "COVISP – Compromising video signal processor." http://www.cl.cam.ac.uk/~mgk25/covisp/