`gr-tempest`: Spying Video Interfaces Through Electromagnetic Emanations

Federico Larroca

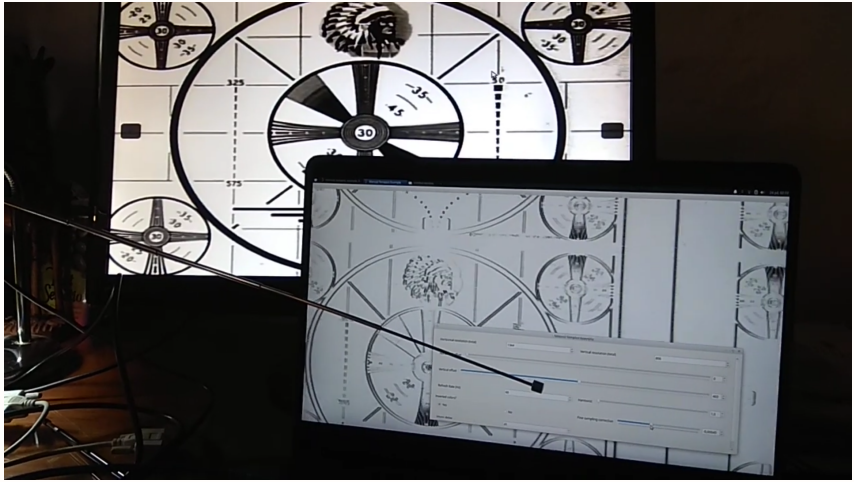
Instituto de Ingeniería Eléctrica, Facultad de Ingeniería, Universidad de la República, Uruguay

GNU Radio Conference

September 23rd 2021

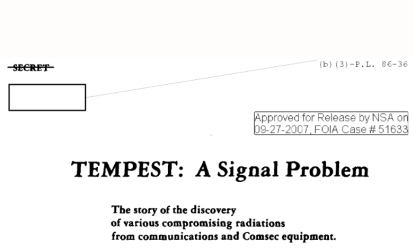
Agenda

Spying on a monitor using an antenna?



A brief history

- During World War II, US military used Bell's 131-B2 to encrypt teleprinter signals


~~SECRET~~

(b)(3)-P.L. 86-36

Approved for Release by NSA on 09-27-2007, FOIA Case # 51633

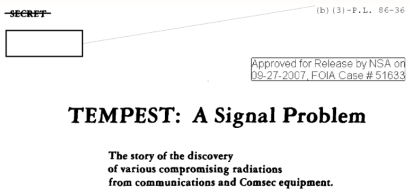
TEMPEST: A Signal Problem

The story of the discovery
of various compromising radiations
from communications and Comsec equipment.

- As accidentally discovered by Bell's researchers, it generated emissions such that the plaintext could be recovered tens of meters away

A brief history

- During World War II, US military used Bell's 131-B2 to encrypt teleprinter signals

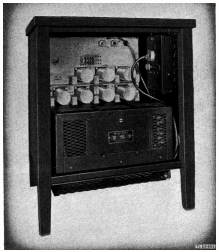

~~SECRET~~

(b)(3)-P.L. 86-36

Approved for Release by NSA on 09-27-2007, FOIA Case # 51633

TEMPEST: A Signal Problem

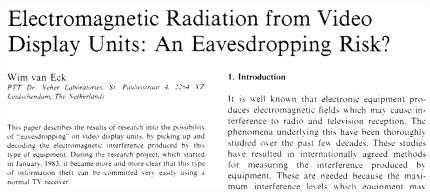
The story of the discovery
of various compromising radiations
from communications and Comsec equipment.



  - As accidentally discovered by Bell's researchers, it generated emissions such that the plaintext could be recovered tens of meters away
- This event triggered what then evolved into TEMPEST: how to spy on these emanations and how to protect sensitive information from potential eavesdroppers
  - However, most is classified and remained restricted to the military and government for several years

A brief history

- It was not until 1985 when Wim Van Eck published his paper on eavesdropping CRTs monitors



Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?

Wim van Eck
PTT Dr. Neher Laboratories, St. Paulusstraat 4, 2264 XZ Leidschendam, The Netherlands

This paper describes the results of research into the possibility of "eavesdropping" on video display units, by picking up and decoding the electromagnetic interference produced by this type of equipment. During the research project, which started in January, 1983, it became more and more clear that this type of information theft can be committed very easily using a normal TV receiver.

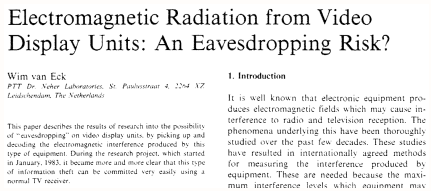
1. Introduction

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

- The reason why the term *Van Eck Phreaking* is sometimes used to refer to TEMPEST applied to video

A brief history

- It was not until 1985 when Wim Van Eck published his paper on eavesdropping CRTs monitors



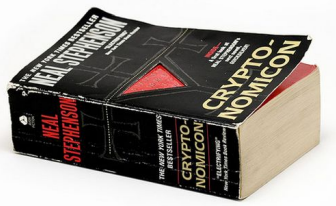
Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?

Wim van Eck
PTT Dr. Neher Laboratories, St. Paulusstraat 4, 2264 XZ Leidschendam, The Netherlands

This paper describes the results of research into the possibility of "eavesdropping" on video display units, by picking up and decoding the electromagnetic interference produced by this type of equipment. During the research project, which started in January, 1983, it became more and more clear that this type of information theft can be committed very easily using a normal TV receiver.

1. Introduction

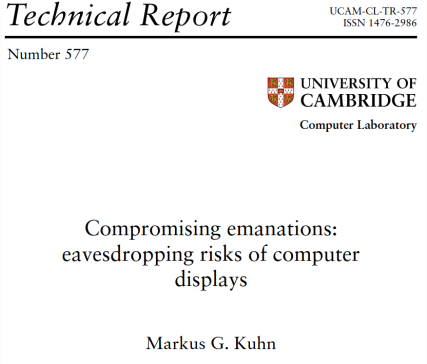
It is well known that electronic equipment produces electromagnetic fields which may cause interference to radio and television reception. The phenomena underlying this have been thoroughly studied over the past few decades. These studies have resulted in internationally agreed methods for measuring the interference produced by equipment. These are needed because the maximum interference levels which equipment may



- The reason why the term *Van Eck Phreaking* is sometimes used to refer to TEMPEST applied to video (most notably on Neal Stephenson's Cryptonomicon)

A brief history

- In 2003 Markus G. Kuhn published a technical report on how to spy (and protect) modern video displays (both analog and digital)



Technical Report

UCAM-CL-TR-577
ISSN 1476-2986

Number 577

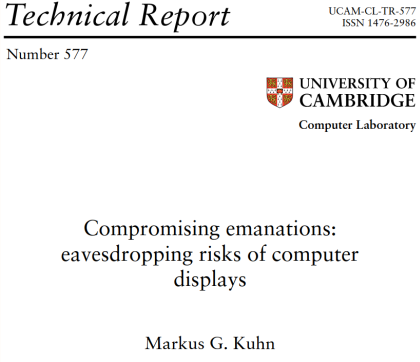
UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Compromising emanations: eavesdropping risks of computer displays

Markus G. Kuhn

A brief history

- In 2003 Markus G. Kuhn published a technical report on how to spy (and protect) modern video displays (both analog and digital)
- In 2014 the first SDR implementation was published: Martin Marinov's `TempestSDR`



Technical Report

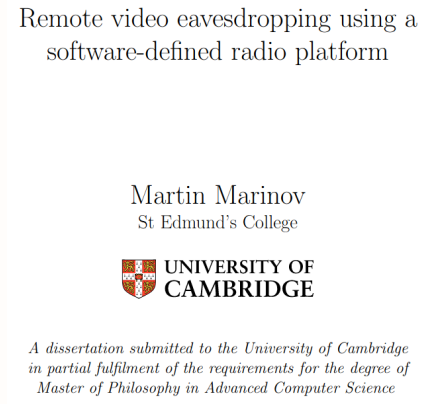
UCAM-CL-TR-577
ISSN 1476-2986

Number 577

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Compromising emanations: eavesdropping risks of computer displays

Markus G. Kuhn



Remote video eavesdropping using a software-defined radio platform

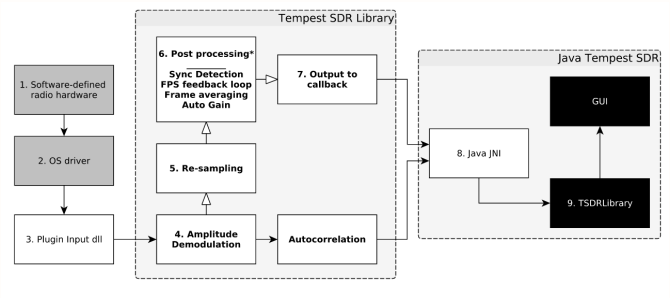
Martin Marinov
St Edmund's College

UNIVERSITY OF CAMBRIDGE

A dissertation submitted to the University of Cambridge in partial fulfilment of the requirements for the degree of Master of Philosophy in Advanced Computer Science

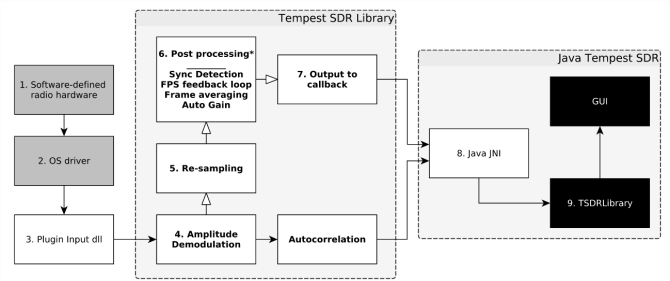
A brief history

- TempestSDR
  - Java-based GUI
  - Modules written in C for DSP
  - Plugins for SDR hardware



A brief history

- TempestSDR
  - Java-based GUI
  - Modules written in C for DSP
  - Plugins for SDR hardware

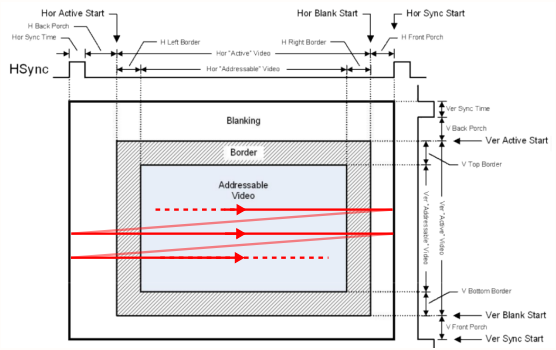


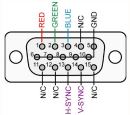
- In 2017-2018 we worked along Pablo Menoni with TempsestSDR for his master thesis
- In 2020, during the beginning of the pandemic, I developed and published gr-tempest, basically a TEMPEST implementation in GNU Radio
  - Take advantage of GNU Radio to address the problem:
    - Easier to code (mostly focus on the general_work function)
    - SDR hardware support
    - Several blocks (and functions) already implemented: filters, resamplers, video, etc.
  - Simpler experimentation and extensions

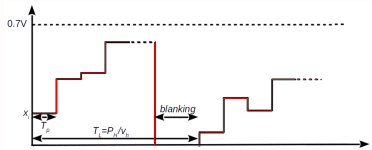
Agenda

VGA signal

- Let us first understand the VGA signal: it's basically a PAM with rectangular pulses
  - It may also be regarded as the output of a Zero-Order Hold (ZOH) DAC



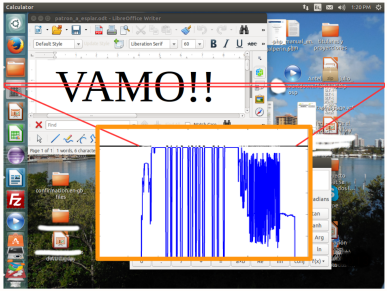




VGA Signal: spectrum (a little math)

Let x_i be the pixels' sequence, T_p the pixel duration and $p(t)$ the rectangular function with duration T_p:

$$x(t) = \sum_i x_i p(t - iT_p)$$

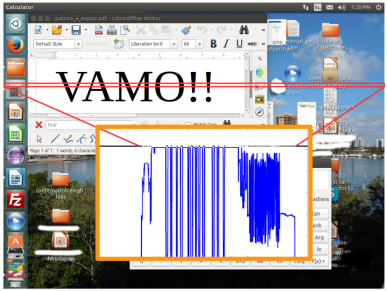


VGA Signal: spectrum (a little math)

Let x_i be the pixels' sequence, T_p the pixel duration and $p(t)$ the rectangular function with duration T_p:

$$x(t) = \sum_i x_i p(t - iT_p)$$

$$\Rightarrow X(f) = \sum_i x_i P(f) e^{-j2\pi f T_p}$$



VGA Signal: spectrum (a little math)

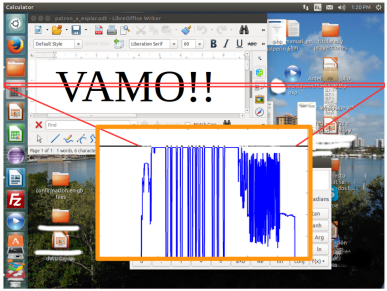
Let x_i be the pixels' sequence, T_p the pixel duration and $p(t)$ the rectangular function with duration T_p:

$$x(t) = \sum_i x_i p(t - iT_p)$$

$$\Rightarrow X(f) = \sum_i x_i P(f) e^{-j2\pi f T_p}$$

$$\Rightarrow X(f) = P(f) \sum_i x_i e^{-j2\pi f T_p}$$

$$\Rightarrow X(f) = P(f) X_s(f)$$



VGA Signal: spectrum (a little math)

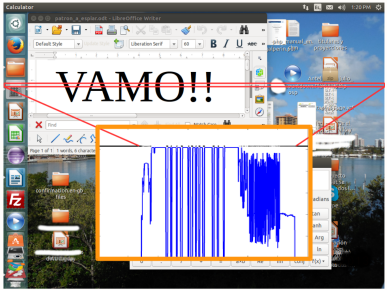
Let x_i be the pixels' sequence, T_p the pixel duration and $p(t)$ the rectangular function with duration T_p:

$$x(t) = \sum_i x_i p(t - iT_p)$$

$$\Rightarrow X(f) = \sum_i x_i P(f) e^{-j2\pi f T_p}$$

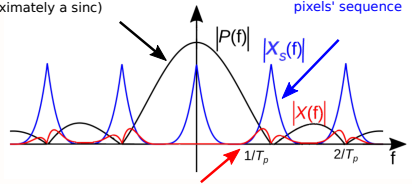
$$\Rightarrow X(f) = P(f) \sum_i x_i e^{-j2\pi f T_p}$$

$$\Rightarrow \mathcal{X}(f) = P(f)X_s(f)$$



Discrete Time Fourier Transform of the pixels' sequence

Fourier Transform of the pulse (approximately a sinc)



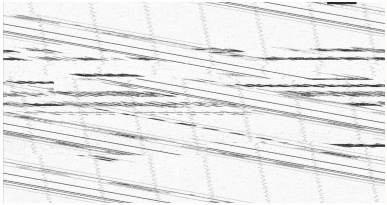
Resulting (and emitted) spectrum

“Demodulating” the VGA Signal

- I point my antenna to the VGA connectors, demodulate at a carrier of $f_c = 1/T_p$ (e.g. for 1024×768@60Hz it amounts to $1/T_p \approx 65\,\text{MHz}$), I consider its magnitude (to avoid frequency synchronization issues), and what do I get?

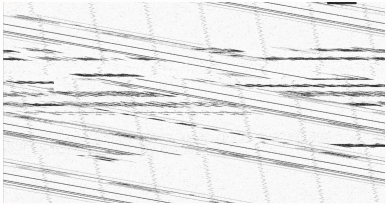
“Demodulating” the VGA Signal

- I point my antenna to the VGA connectors, demodulate at a carrier of $f_c = 1/T_p$ (e.g. for 1024×768@60Hz it amounts to $1/T_p \approx 65\,\text{MHz}$), I consider its magnitude (to avoid frequency synchronization issues), and what do I get?



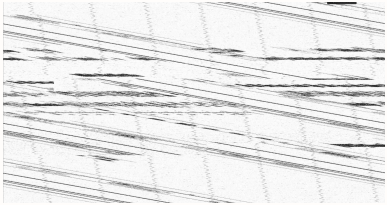
“Demodulating” the VGA Signal

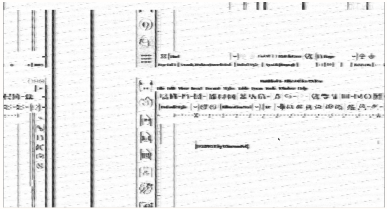
- I point my antenna to the VGA connectors, demodulate at a carrier of $f_c = 1/T_p$ (e.g. for 1024×768@60Hz it amounts to $1/T_p \approx 65\,\text{MHz}$), I consider its magnitude (to avoid frequency synchronization issues), and what do I get?
- One of the most challenging aspects of the problem is time synchronization. We may take advantage of repetitions: one line is very similar to the next one, and a frame is very similar to the next one.



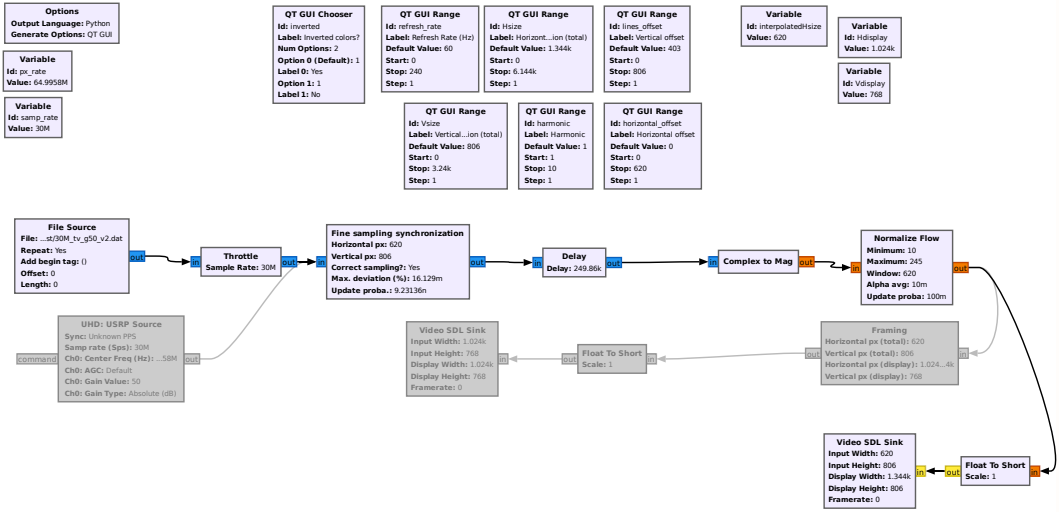
“Demodulating” the VGA Signal

- I point my antenna to the VGA connectors, demodulate at a carrier of $f_c = 1/T_p$ (e.g. for 1024×768@60Hz it amounts to $1/T_p \approx 65\,\text{MHz}$), I consider its magnitude (to avoid frequency synchronization issues), and what do I get?
- One of the most challenging aspects of the problem is time synchronization. We may take advantage of repetitions: one line is very similar to the next one, and a frame is very similar to the next one.

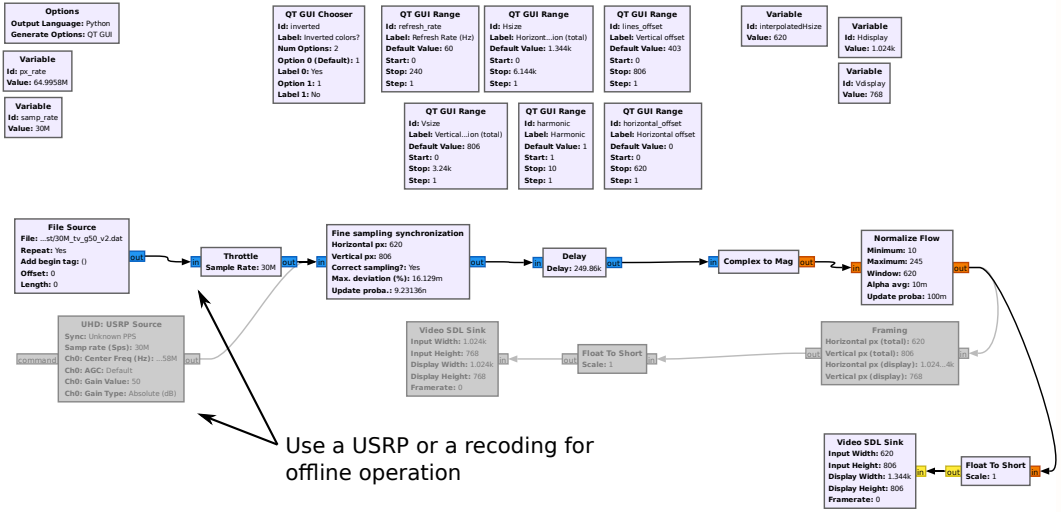




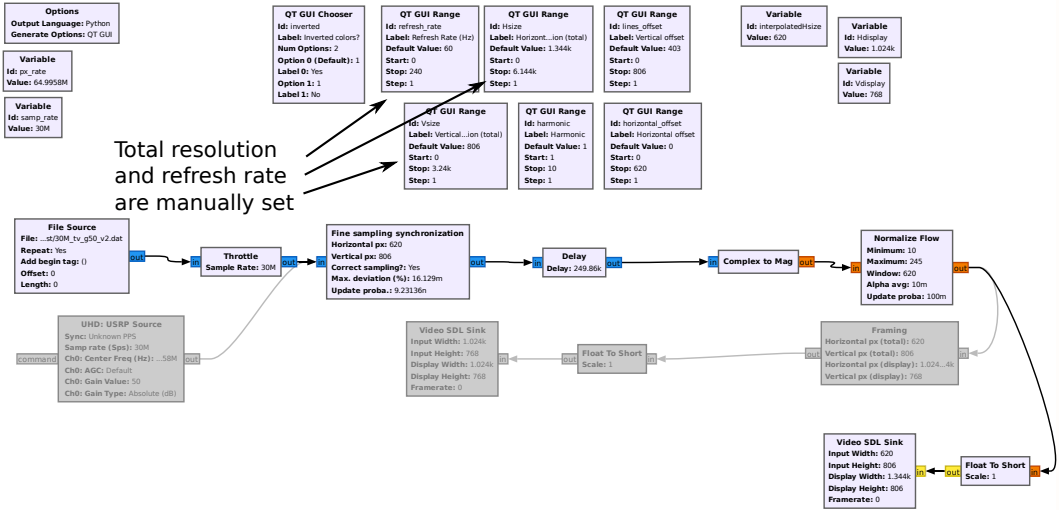
gr-tempest: simplest flowgraph



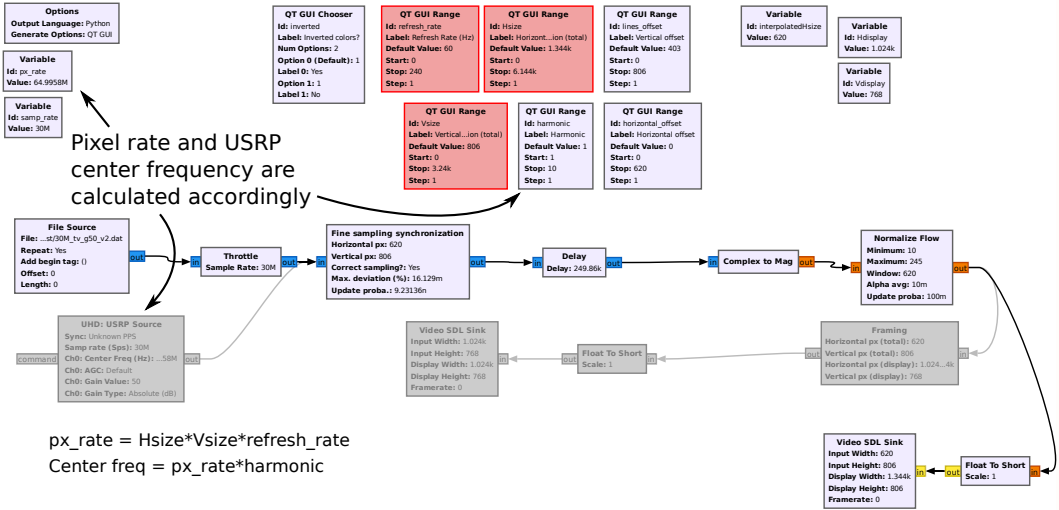
gr-tempest: simplest flowgraph



gr-tempest: simplest flowgraph

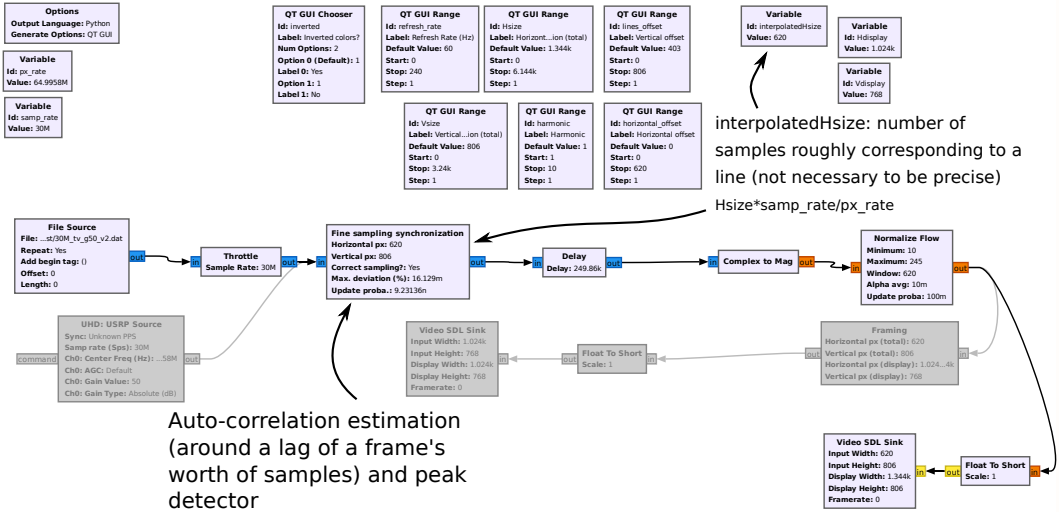


gr-tempest: simplest flowgraph

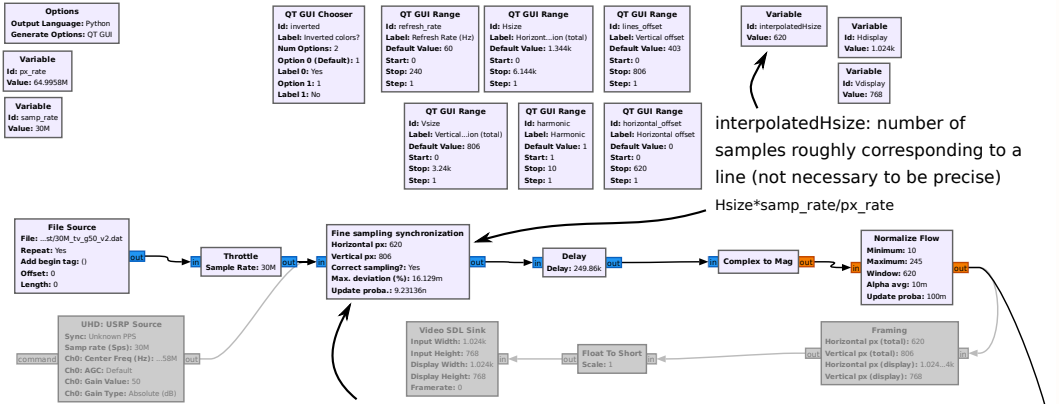


px_rate = Hsize*Vsize*refresh_rate
Center freq = px_rate*harmonic

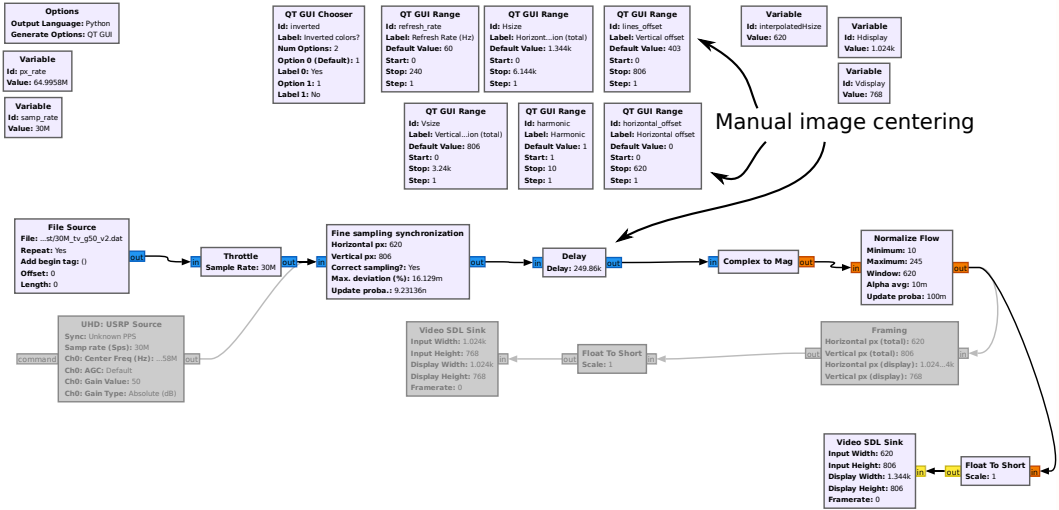
gr-tempest: simplest flowgraph



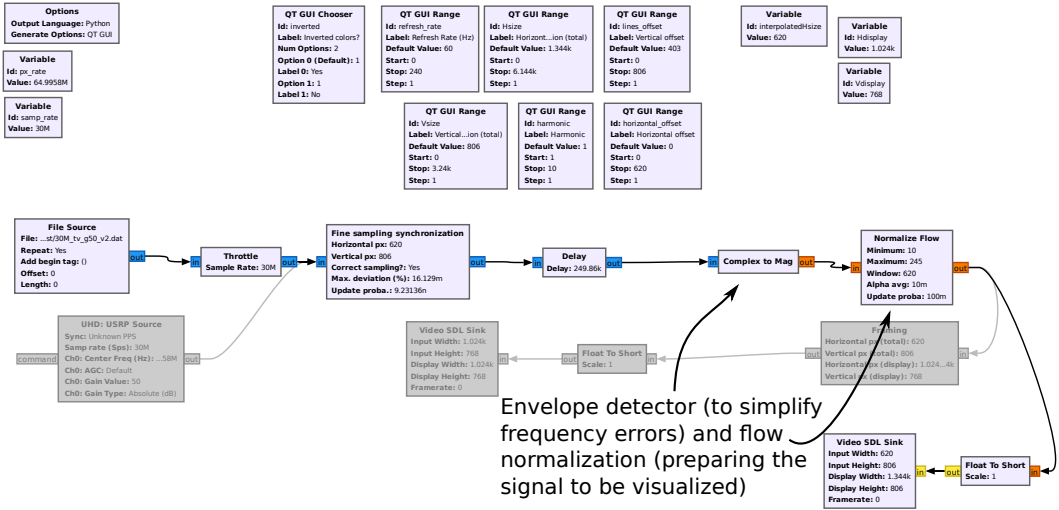
gr-tempest: simplest flowgraph



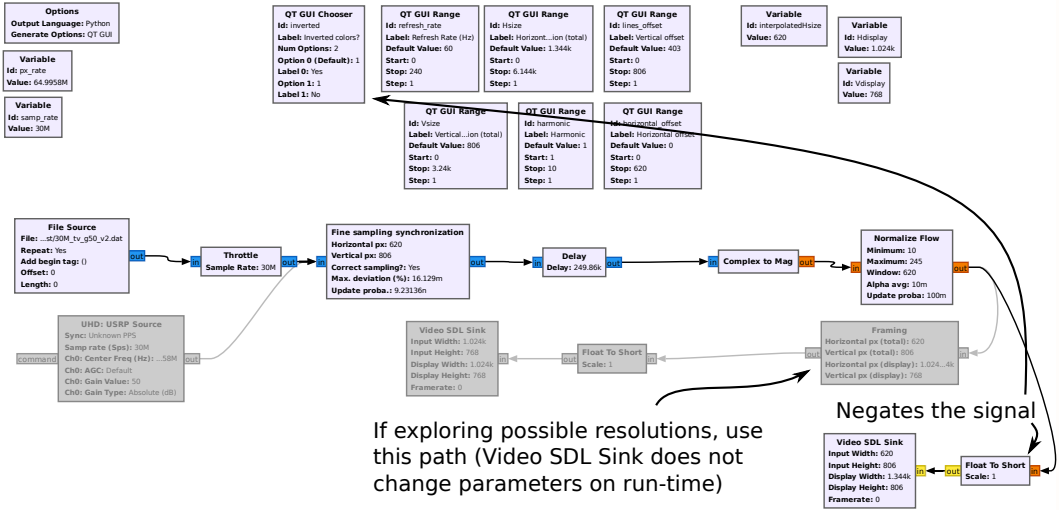
gr-tempest: simplest flowgraph



gr-tempest: simplest flowgraph



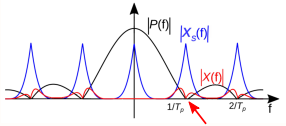
gr-tempest: simplest flowgraph

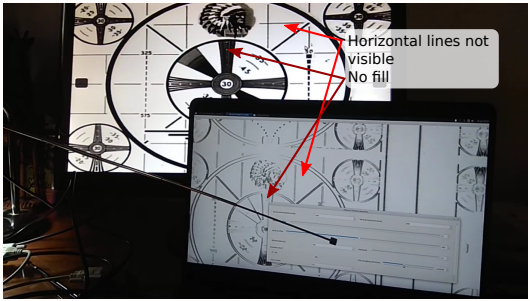


If exploring possible resolutions, use this path (Video SDL Sink does not change parameters on run-time)

Practicalities

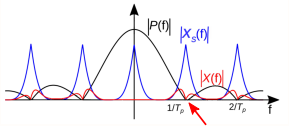
- The null in the center frequency results in a sort of horizontal border detector



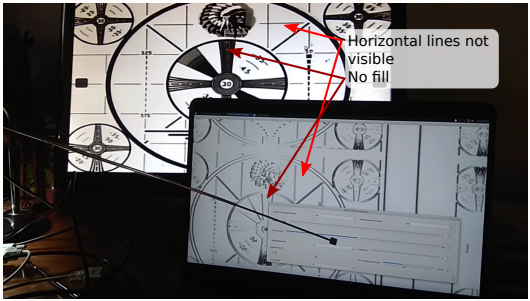


Practicalities

- The null in the center frequency results in a sort of horizontal border detector

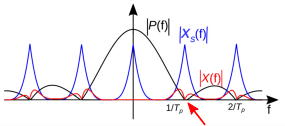


- A somewhat large bandwidth is necessary: at least 20 MSps.
  - Sample losses complicates the visualization (image centering) and results in "jumps"
- Expect interference, which further complicates the problem.

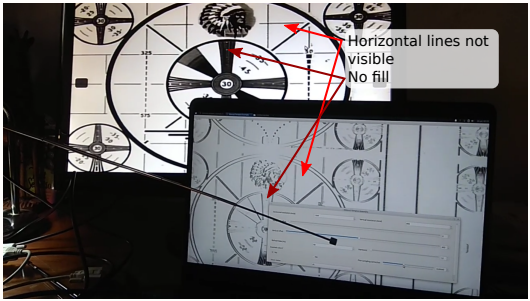


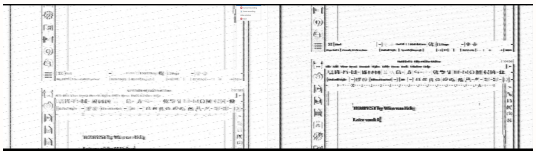
Practicalities

- The null in the center frequency results in a sort of horizontal border detector



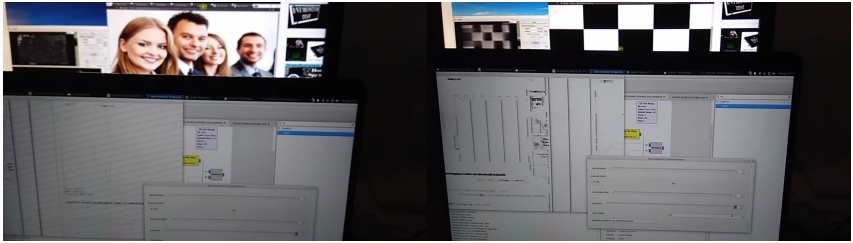
- A somewhat large bandwidth is necessary: at least 20 MSps.
  - Sample losses complicates the visualization (image centering) and results in "jumps"
- Expect interference, which further complicates the problem.





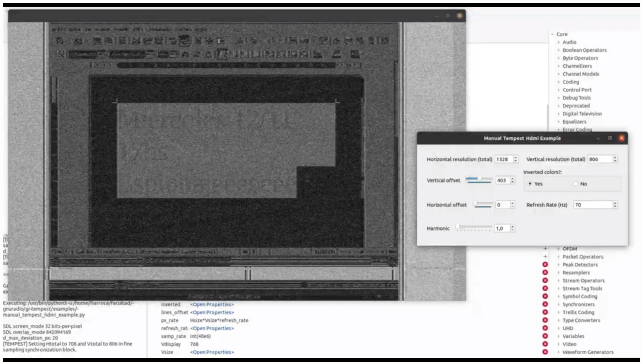
Practicalities

- If no high-gain antenna is available, a cheap adapter will do the trick



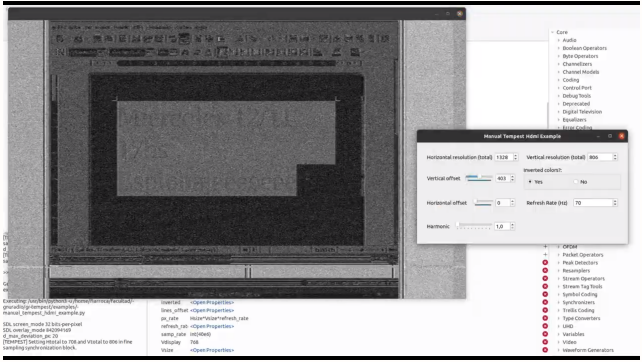
Practicalities

- What about digital (HDMI or DVI)?



Practicalities

- What about digital (HDMI or DVI)?



- Each color has an 8 bit depth and is encoded into 10 bits (Transition-minimized differential signaling or TMDS):
  - The same flowgraph works except we have to demodulate at 10 times the pixel rate
  - Due to the encoding, the image is qualitatively different (e.g. it has fill)

Agenda

Future

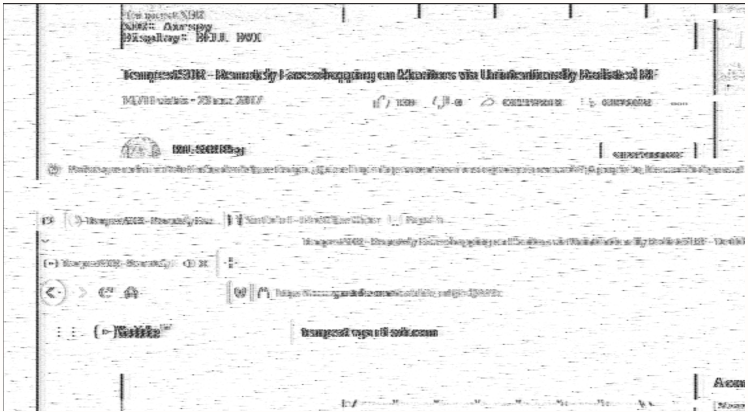
- What if I don't know the monitor's resolution?

Future

- What if I don't know the monitor's resolution?
- Do we really need to work at such a high sample-rate?
  - We may sacrifice frames instead of resolution (we don't really need a 60 Hz refresh rate)

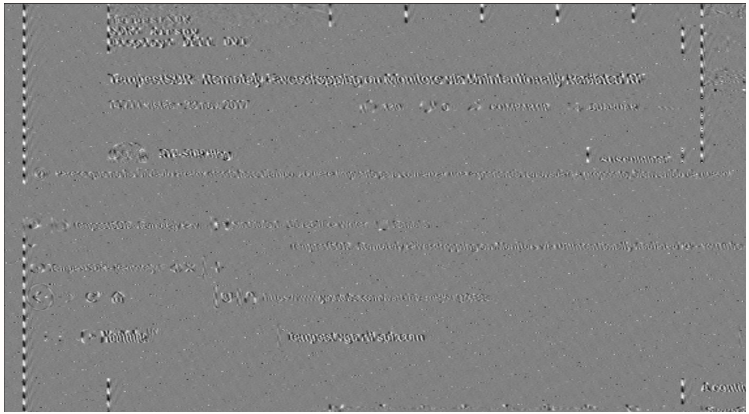
Future

- What if I don't know the monitor's resolution?
- Do we really need to work at such a high sample-rate?
  - We may sacrifice frames instead of resolution (we don't really need a 60 Hz refresh rate)
- Why consider only the magnitude of the signal?
  - Taking the magnitude distorts the signal



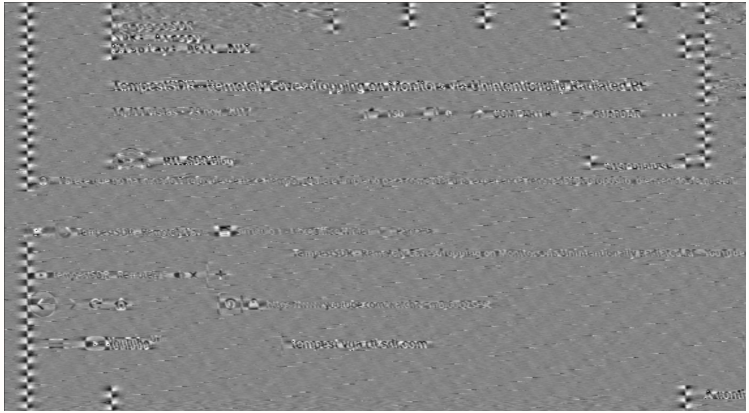
Future

- What if I don't know the monitor's resolution?
- Do we really need to work at such a high sample-rate?
  - We may sacrifice frames instead of resolution (we don't really need a 60 Hz refresh rate)
- Why consider only the magnitude of the signal?
  - Taking the real part reveals some details (but what about the frequency error?)



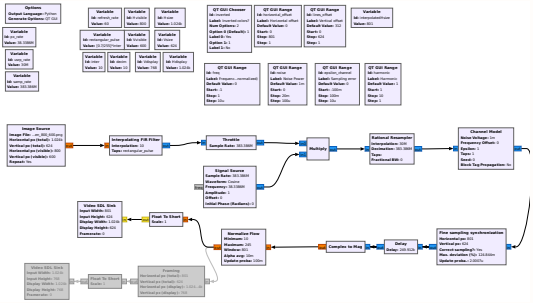
Future

- What if I don't know the monitor's resolution?
- Do we really need to work at such a high sample-rate?
  - We may sacrifice frames instead of resolution (we don't really need a 60 Hz refresh rate)
- Why consider only the magnitude of the signal?
  - Equalizing reveals further details (blind equalization?)



Future

- What if I don't know the monitor's resolution?
- Do we really need to work at such a high sample-rate?
  - We may sacrifice frames instead of resolution (we don't really need a 60 Hz refresh rate)
- Why consider only the magnitude of the signal?
- And in the digital case, where equalization is not really possible?
  - First steps in using deep learning to reconstruct the image. **Do not throw away one of the channels!**
  - We provide a signal simulator that should ease constructing a training set



Thanks!

¿Questions?

Federico “Larroca” La Rocca

✉ flarroca@fing.edu.uy
@fedelarrocca
https://github.com/git-artes/gr-tempest

We also share several recordings.

Special thanks to Pablo Menoni along whom I understood TEMPEST