Robin LOBEL
divide@3dvf.net

Adrien MATTA

Collection, Treatment, and Usage of Compromising Waves

translated by Dan Robey

Introduction :

1. *Definition and Initial Elements:*

When using an electronic instrument, its circuitry is subject to variations of voltages. These variations emit of electromagnetic waves, which are propagated in the surrounding space significant distances (several hundred meters). When these waves can be collected and used to recreate the information which was passing through the circuit, they are called compromising waves, because they "compromise" the confidentiality of the data. This is true for any kind of electronic machine, such as video cassette recorders, televisions, stereo systems, or computers.

One can theoretically collect the compromising waves emitted by apparatuses with access to the data in a completely furtive way. Nevertheless, the amplitude of these waves decreases quickly with distance, and only waves of strong initial amplitudes can be captured further than a few centimeters away. The majority of electronic apparatuses emit only waves of low amplitudes; however, computer screens amplify the signals emitted by the video card before nearly 500 times drawing the image, they thus emit waves with amplitude sufficient for being captured.

2. *Evidence of the Phenomenon:*

One can very simply find these waves; indeed, if one connects a computer screen to the central unit with an unshielded cable, there is an echo effect and it appears in addition to the original image out of sync with it. The wire acts like an antenna receptor, collecting the waves emitted by the computer and transforms them into electric signals sent to the screen.

3. *Objective :*

The objective is to show the compromising phenomenon, and to attempt to know under which conditions it occurs and how difficult it is to reconstitute the images found on a computer screen.

I.History of the Tempest system

The first studies concerning the phenomenon of compromising electromagnetic waves occured in the 1950s. Through spying on Russian encrypted message transmission, NSA discovered weak parasitic rattlings in the carrying tone, which were emanated by the electricity of the encoding machine. By building a device appropriately, it was possible to rebuild the plaintext without having decrypt the transmissions.

This phenomenon successively takes the names NAG1A, then FS222 in the 60s, NACSIM5100 in the 70s, and finally, TEMPEST beginning in the 1980s.

US Army Blacktail Canyon TEMPEST Test Facility logo

In 1985 a Dutch scientist, Wim van Eck, published a report on the experiences he had since January 1983 in this field. It shows that such a system is creatable with little means, however it gives very little detail about the experiences. It discusses only the theory of the phenomenon.
In 1986 and 1988, complementary reports were published, continuing van Eck's article, without bringing much other information concerning the experiences.

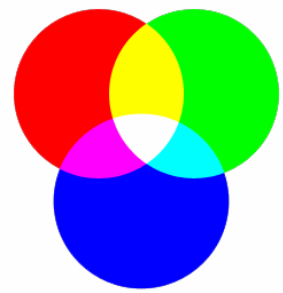
In 1998 John Young, an American citizen, requested the NSA to publish declassified information concerning the TEMPEST system. Seeing his request rejected, he appealed and finally in 1999 obtained some documents, but largely censured.

Very little information is available on this system. The majority of the documents do nothing but superficially expose the phenomenon, without returning in the details of a practical sort.

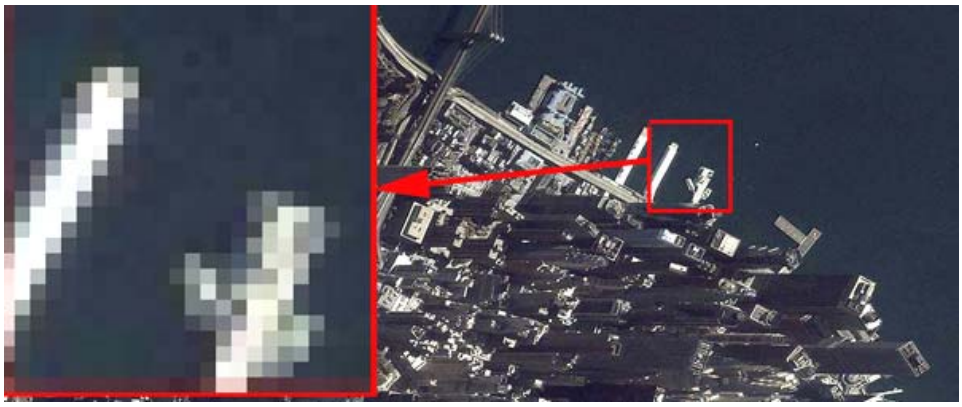
II.Theory of the Screens

1. Decomposition of an image :

The colors can be decomposed into three primary colors: Red, Green, and Blue. It is possible through the combination of these 3 colors to recreate any color, by varying these fundamental proportions.



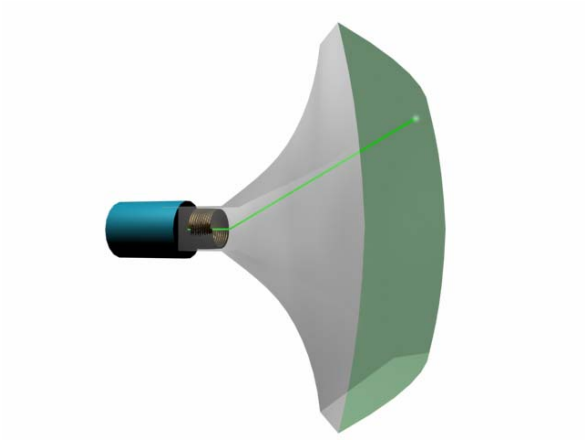
An image is considered a complex assembly of colors, in the shape of a grid of Pixels. A Pixel is a point composed of the three colors, blue, green, and red. With a large density of points, it is possible to restore an image with fidelity.



The resolution (smoothness) of the image describes X*Y, with X being the number of pixels horizontally, and Y the number of pixels vertically (ex: 640*480, 800*600, 1024*768…)

2. Reconstitution of an image on a screen:

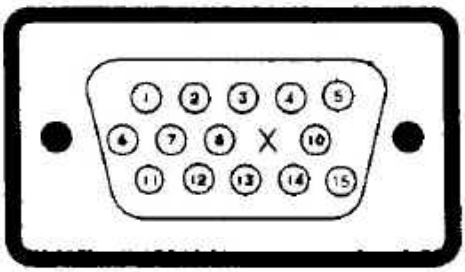
A screen is composed several modules:
The cathode ray tube serves the direct reconstruction of the image;
A beam of electrons sweeps a fluorescent layer at very high speed to post the image. Sweeping is done from right to left and from top to bottom, at a frequency of 50Hz 100Hz on the entire screen; the fluorescent layer is excited with the passage of these electrons and emits light. This layer is equally phosphorescent, it continues to emit light for a brief time (10 20ms) after its excitation; thus the flutter phenomenon which could occur is eliminated.



The luminosity of the fundamental components is determined by the throughput of electrons, regulated by a wehlnet (electronic component). The beam then passes between two reels which realign its trajectory through electromagnetism in order to sweep the screen.

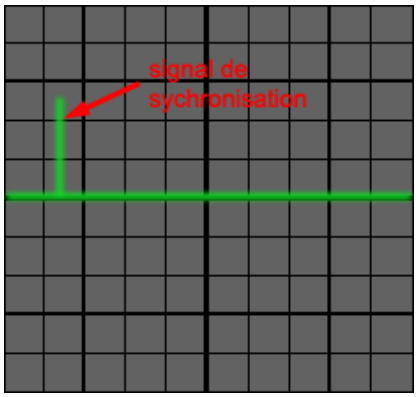
3. Coding of the video signal :

The video signal passes by several channels; six channels for the video signal itself, channels red, green, blue and their respective powers, plus two synchronization channels for the field and horizontal sweep, and the power common to synchronization signals.

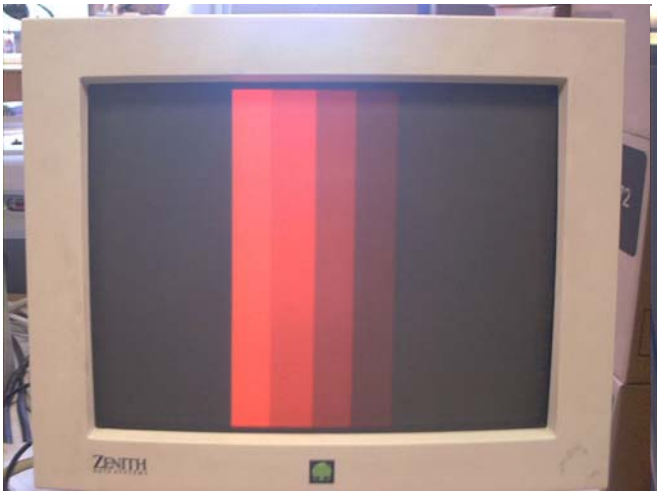


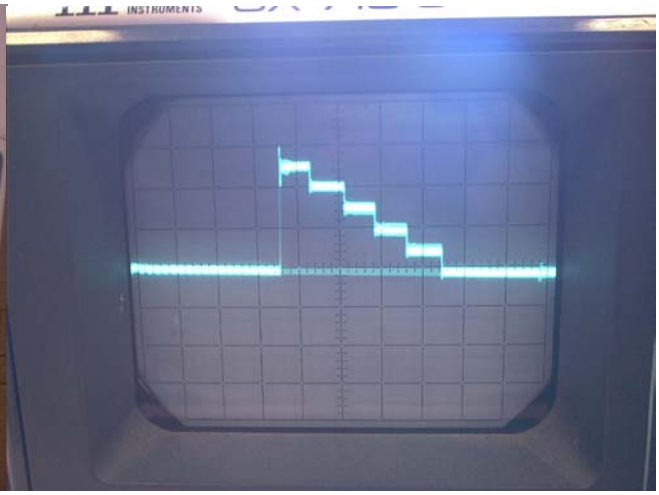
Connector SUB-D HD – 1:Red, 2:Green, 3:Blue,
6:Red Strength, 7:Green Strength, 8:Blue Strength,
11 :Strength, 13 : Horizontal Sync, 14 : Vertical Sync

The synchronization signals, which indicate the passage to the following line or the return of the beam to the beginning of the screen, are simple differences of potentials of a few volts. They take place (for a screen of a resolution of 800*600 pixels with 70Hz refresh) 70 times a second for the vertical synchronization signals, and 600*70=42000 time a second for the horizontal synchronization signals.



The video signals are voltages of 0V to 0.7V, which define the intensity of the luminous point at the sweeping point (this voltage is thus able to vary to each new pixel of different color; for a screen of resolution 800*600 with refresh rate of 70Hz, the changes of voltage can reach a frequency of 800*600*70=34Mhz, that is to say 34,000,000 times a second).





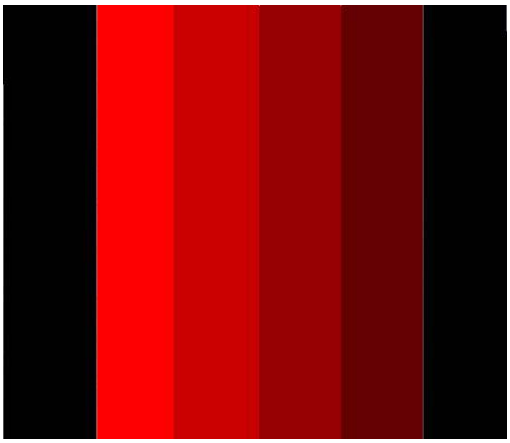
III. Theoretical Development of the Circuit

1. *Requirements of the Circuit :*

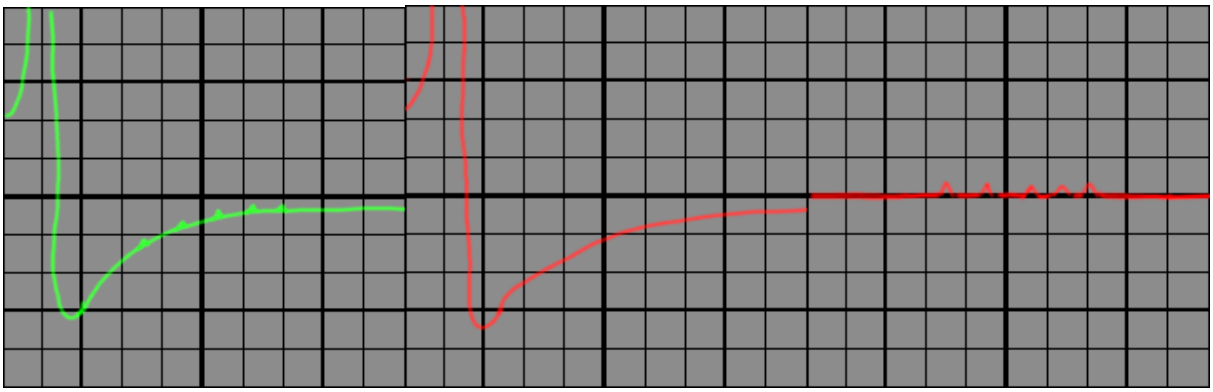
Above we saw the nature of the electric signals bringing information to the screen, and that these signals were amplified to draw the image. This amplification brings the emission of compromising waves of high amplitude, which we seek to collect.

With each difference of potential at the exit of the amplification circuit an electromagnetic wave is emitted of proportional amplitude. The amplitude of this wave will decrease with the distance because of the distribution of the electromagnetic energy on the face of spherical wave.

An example of electromagnetic wave is the attached image:



The screen draws a degradation of pure red surrounded by black bands.



An observation the oscilloscope shows us that the signal is deformed (right-hand image) by the damping of the wave connected to the horizontal synchronization signal (center); notice that the signal "oscillates" on the prescribed axis from disturbances connected to the power. We want to recover the video signal (left).

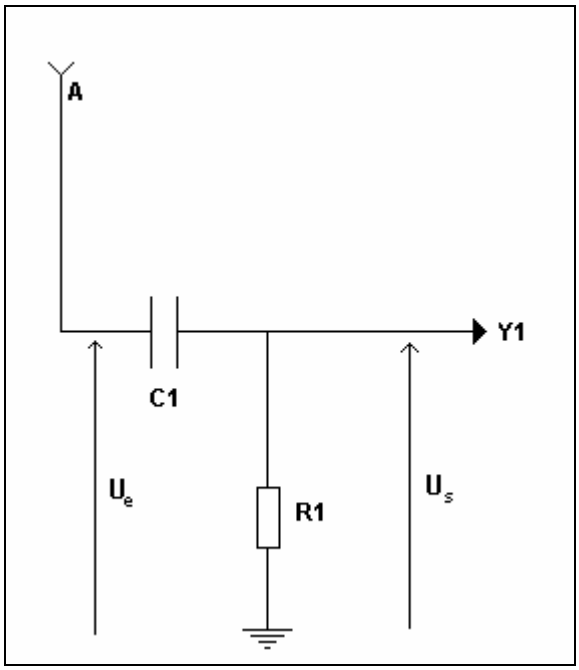
After what we have just shown, this signal is not exploitable directly by a screen, because we need a positive signal whose voltage varies between 0V and 0.7V.

The assembly to create must thus make it possible to cancel the effect caused by the synchronization signal and the power but equally to amplify the signal.

2. *Filtering the signals :*

With the aim of eliminating the parasitic signals we set up, between the antenna receptor and the screens, we use a band-pass circuit. There are two types of band-pass circuits, the high-pass ones and the low-pass ones which let pass respectively, the high frequencies or the low frequencies.

In our case, we need a high-pass circuit, since the frequency of the video signals (several tens of MHz) is greater than that of the synchronization signals (a few tens of Khz for the horizontal synchronizations signals).



The assembly derived from a capacitor and a resistor allows the creation of a high-pass filter.

Indeed, any periodic signal can be considered as the sum of sinusoidal signals, and consequently, the high-pass filter can "remove" the components whose frequencies are lower than the cut frequency as follows:

When it is subjected to a sinusoidal voltage, the capacitor takes care, then during the change of direction of variation of the sinusoid, this one discharges, nevertheless, if the period of the voltage is a greater at the load time of the capacitor, this one acts like a circuit breaker and impedes the passage of the signal. One can vary the cut frequency by adjusting the values of C and of R. If τ =RC, if τ ro increases, the load time of the capacitor increases and thus the cut frequency decreases. One can deduce that the cut frequency FC is inversely proportional to τ =RC . We have:

$$f_c = \frac{1}{2\pi.RC}$$

One can deduce thus the voltage waveform exiting the device according to the entry voltage:

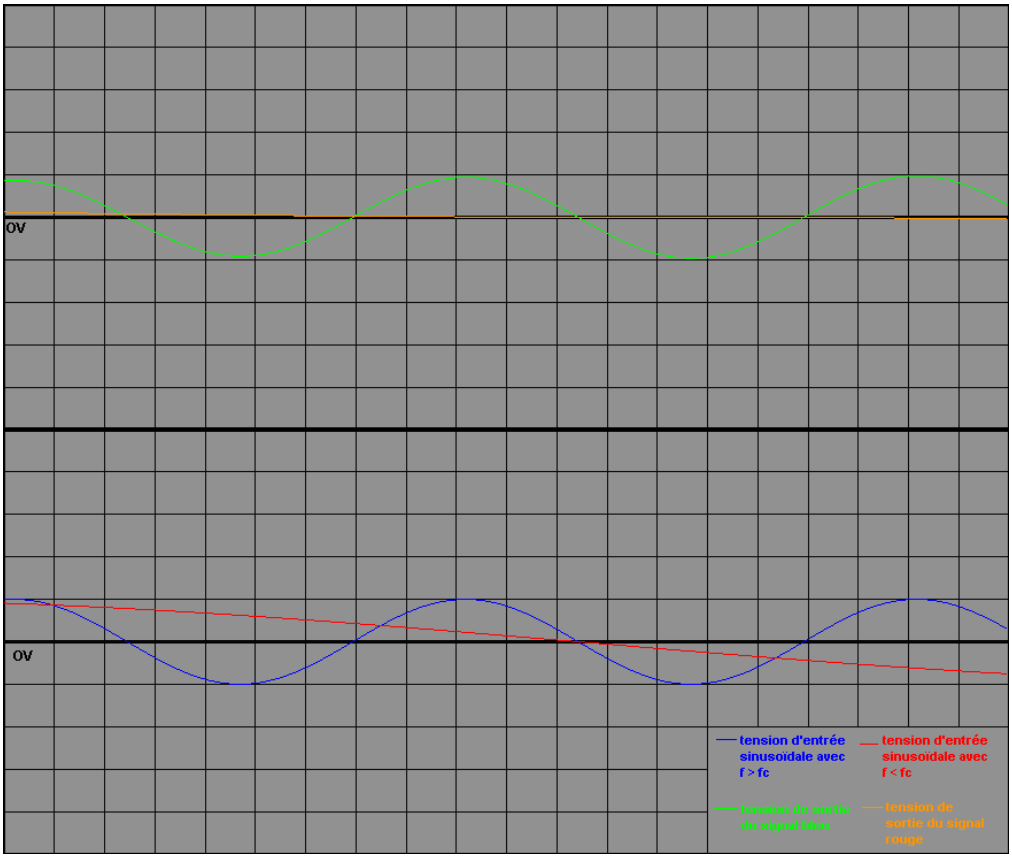
If the entry frequency of f_e Fe is greater than the cut frequency, the capacitor charges itself positively then negatively, one can thus write the equation of the terminal voltage of RC circuit:

$$U_s = \sin(f_e t).(1-e^{-t/\tau})$$

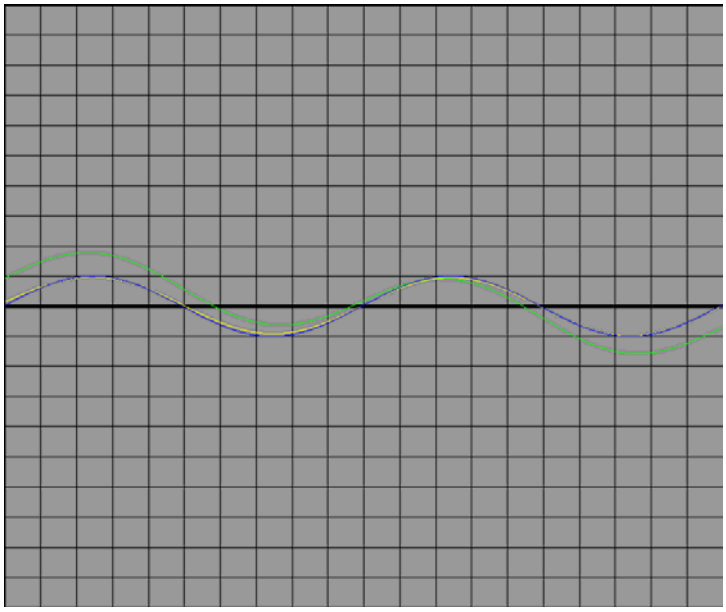
If the entry frequency Fe is less than the cut frequency, the capacitor charges then does not discharge because it arrives at its maximum regime before the voltage changes direction of variation, the voltage wavers slightly, of some milliohms of volts, one can write thus the equation of the terminal voltage of RC circuit:

$$U_s = \sin(f_e t).(e^{-t/\tau})$$

One can also trace the terminal voltage of the RC circuit according to the frequency of the entry voltage:



If the entry voltage is the sum of two (or more) signals, one of frequency more than the cut frequency and the other of frequency less than the cut frequency, it brings out only the signal of frequency greater than the cutoff frequencies:

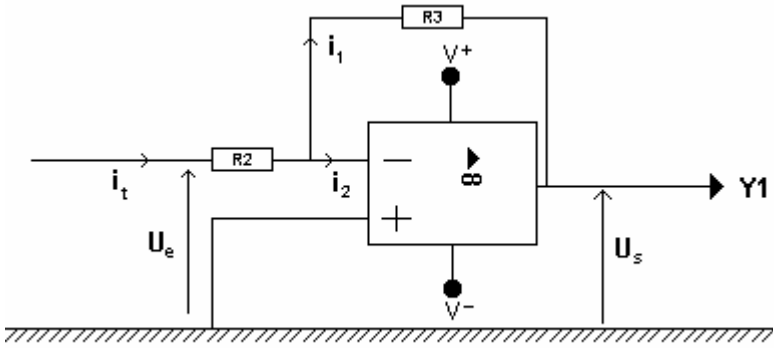


The output signal (yellow) is "almost" the same that the signal of frequencies greater than the cut frequency (blue). It is slightly deformed. In green, the signal of entry, nap of two signals of frequencies different.

At the exit of the RC circuit, one obtains a signal having only video information remaining. These are not yet exploitable, they must be amplified.

3. *Amplification :*

To have an exploitable signal, we need a signal ranging between 0V and 0.7V, it should be amplified while keeping the proportion of the signals between them, for that we must thus multiply the voltage left RC circuit by a factor K For that we choose the use of a circuit based on an Operational Amplifier (op-amp), an "inverter."



A NOT-circuit which amplifies the voltage of entry by a coefficient K.

In such a circuit, we see that Ohm's law applies to the resistance R2, this one decreasing the voltage entering the amplifier operational, the voltage U_r is thus less than the voltage U_e, the voltage U_s is thus inversely proportional the value of the resistance R_2.
The resistance R_3 R3 is in derivation with the op-amp; ; the more it will be of significant value, less current will cross it, and thus more current will cross the op-amp, knowing that one has $i_1 < i_2$. The output voltage is proportional the value of the resistance R_3.

One notices that the circuit is an inverter. The output signal is multiplied by a negative coefficient, so we can deduce:

$$\boxed{k = -\frac{R_3}{R_2}}$$

By regulating the values of R_2 and R_3 we vary the terminal voltage of the entire op-amp, this one goes then, to the intermediate of its supply stability (on the V^+ and V^- terminals) to be able to multiply the voltage of the entire signal.

4. Signal Synchronization :

The signals recovered are desynchronized, the screen cannot thus restore them coherently, it is thus necessary to send the screen an "artificial" synchronization, for that, one can use two methods:

- generating the assistance signals of two LFG (low frequency generator) for horizontal synchronization and the other for vertical synchronization.
- recover the signals emitted by the graphics board of a computer under operation. The first solution seems more appropriate because it allows changes to adapt the signals of synchronization to the received signals.

5. Expected Results:

Owing to the fact that a wave is only emitted at each difference of voltage in the screen, the image obtained cannot be a faithful reproduction of the original, but will allow the access to information attached to the screen source. One thus obtains in theory an image of this type:

IV. Experimental Realization :

1. *The choice of the values for the high-pass:*

As we saw above, we want to remove the effects of the signals of synchronization; those which repeat at a frequency of approximately 70*600=42KHz (for a screen in 800*600*70Hz, by taking account of the signals of horizontal synchronization) we choose a value of cut frequency FC a little larger to have a margin of security, and to eliminate a maximum of interfering signals. One thus chooses a cut frequency close to 160 KHz:

$$f_c = \frac{1}{2\pi RC}$$

$$RC = \frac{1}{2\pi f_c}$$

$$RC = \frac{1}{2\pi . 160000}$$

$$RC = 10^{-6} s$$

We must thus choose a RC ratio close to 10^{-6} s ; however the capacitors have maximum values of the order of the micro Farad (μF), the resistance used will thus be on the order of the kilo Ohm (kΩ).

2. *The Choice of Amplification Values :*

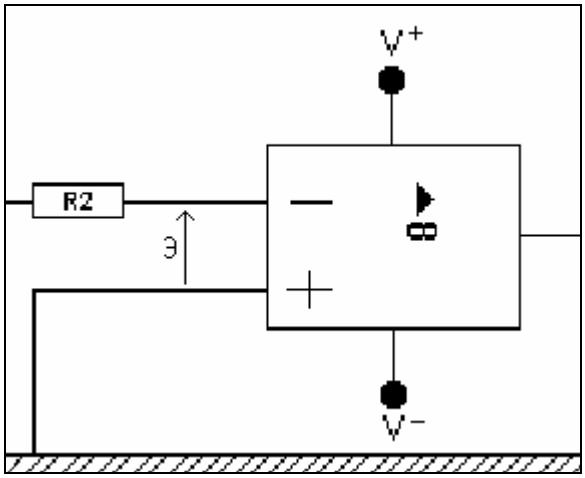
a. choice of an operational amplifier model:

For our use we need an operational amplifier able to support very significant frequencies neighbor of 50 MHz, we have by security chosen an op-amp managing until 60 MHz, it thus acts of a op-amp specially constructed for the assembly video, the model selected is the AD844AN; this one is necessary for a normal operation a fuel stabilized at 5V and a maximum voltage of 5 μV.

b. Choice of resistance values :

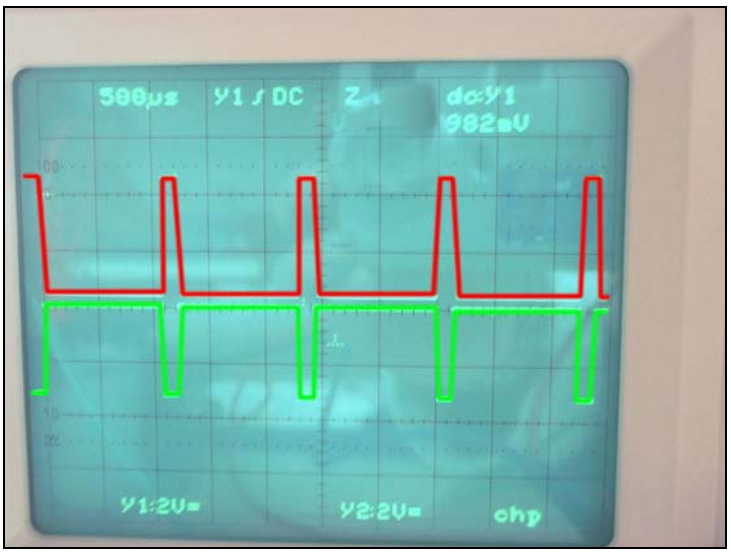
• Our model of operational amplifier forces us to use a very strong resistance value to have an entry voltage of 5 μV. to have an order of magnitude we carry out the following reasoning:

A voltage is a difference of electric state, therefore the difference between two potentials; the weaker the difference is, the weaker the voltage is!



Our objective thus is to choose a resistance enabling us to have a voltage of 5µV ; however the wire of the positive terminal is linked to the power, its potential is from zero; we thus need a potential of 5µV in the negative terminal of the wire, but this value is extremely low before the entry potential (about 0.1V). By taking a resistance very large we will obtain a strong voltage on the terminal of the resistance (Ohm's law) and thus a low potential on the lower terminal. We thus choose a resistance variable R2 of 1 Ω (Ohm).

• We saw above the amplification energy ratio; knowing that we want to amplify between 1 to 100 times, we thus need a resistance R3 of about 10 to 100 Ω.

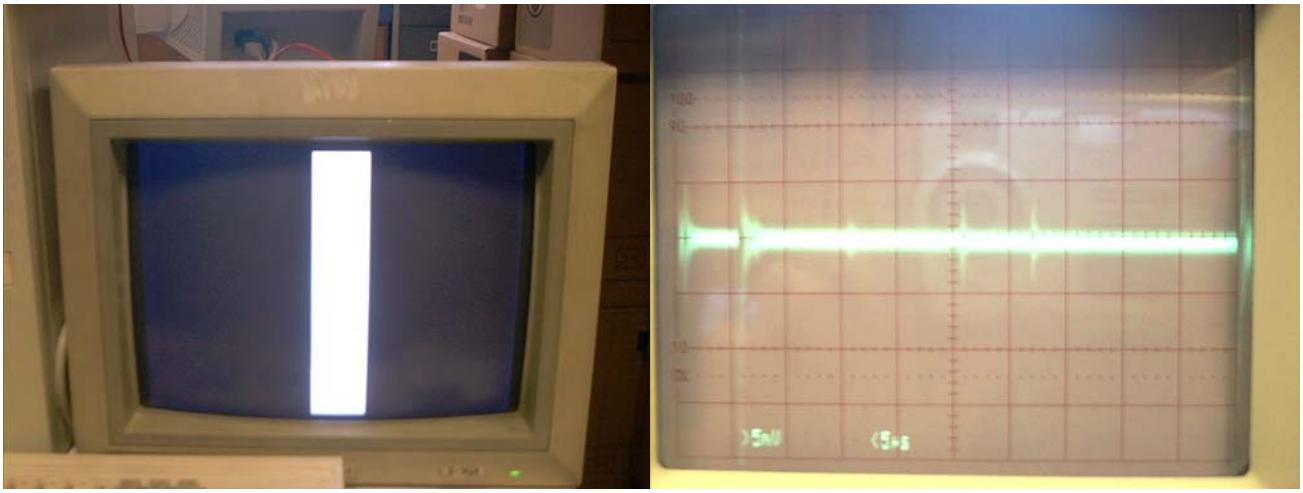


The original signal (green, -3V) and after amplification (in red, +5V)

V. Experimental Results:

When we wrote this file, our experiments were still not completed (although we now possess all now the elements to complete the work).

The most encouraging results that we obtained are visible here:



On left the original image, right, the two central peaks captured by the corresponding electromagnetism to the beginning and the end of the white band.

The signal on the right has been obtained with the high-pass filters, which proves its effectiveness. We only need to amplify this signal and to transmit it to a 2em screen, that we will synchronize with the assistance of 2 LFG, to obtain a phantom image similar the original image.

We had some problems with the amplifier operational (concerning in particular the resistances) but those have been resolved (as the image of the preceding page shows).