Robin LOBEL Adrien MATTA

Captage, traitement et utilisation des ondes de compromissions

Dossier réalisé dans le cadre des TPE du Lycée Lakanal

Introduction :

1. *Définition et éléments de bases :*

Lors de l'utilisation d'un appareil électronique, les circuits qui le composent sont soumis à des variations de tensions, ces variations entraînent l'émission d'ondes électromagnétiques qui se propagent dans l'espace environnant et ce à des distances très importantes (plusieurs centaines de mètres).Lorsque ces ondes peuvent être captées et utilisées pour recréer les informations qui transitent dans le circuit, elles sont appelées ondes de compromissions car elles « compromettent » la confidentialité des données. Cela est vrai pour toute sorte d'appareils, tels que les magnétoscopes, télévisions, chaînes Hi-fi ou ordinateurs. On peut donc théoriquement capter les ondes de compromissions émises par des appareils dans le but d'avoir accès à des données de façon totalement furtive. Néanmoins l'amplitude de ces ondes décroît rapidement avec la distance, et ne peuvent être captées à plus de quelque centimètres que les ondes de fortes amplitudes initiales, or la plupart des appareils électroniques n'émettent que des ondes de faibles amplitudes ; cependant les écrans d'ordinateurs amplifient près de 500 fois les signaux émis par la carte vidéo avant d'afficher l'image, ils émettent donc des ondes d'une amplitude suffisante pour être captée.

2. *Mise en évidence du phénomène :*

On peut très simplement mettre en évidence l'existence de ces ondes ; en effet, si l'on branche un écran d'ordinateur à l'unité centrale avec un câble non blindé, il se produit un effet d'écho et il apparaît en addition la même image en décalage avec l'image d'origine. Le fil agit comme une antenne réceptrice, il capte les ondes émises par l'ordinateur et les transforme en signaux électriques envoyés dans l'écran.

3. *Objectif :*

L'objectif poursuivit par ce TPE est de mettre en évidence l'existence du phénomène de compromission, et de tenter de savoir dans quelles conditions et à quel coût il est possible de reconstituer les images se trouvant sur un écran d'ordinateur.

I.Historique du système Tempest

Les premières études concernant le phénomène de compromission des ondes électromagnétique remontent aux années 1950. C'est en espionnant les transmissions de messages Russes encryptés que la NSA s'aperçut de faibles cliquetis parasites dans la tonalité porteuse, qui étaient émanés par les électro aimants de la machine d'encodage. En construisant le dispositif approprié, il fut possible de reconstruire le texte en clair sans avoir à décrypter les transmissions.

Ce phénomène pris successivement les noms de NAG1A, puis FS222 dans les années 60, NACSIM5100 dans les années 70, et finalement TEMPEST à partir de 1980.

US Army Blacktail Canyon TEMPEST Test Facility logo

En 1985 un scientifique Hollandais, Wim van Eck, publia un rapport sur les expériences qu'il menait depuis Janvier 1983 dans ce domaine. Il montre qu'un tel système est réalisable avec peu de moyen, cependant il ne donne que très peu de données concernant les expériences elles même. Il n'aborde que l'aspect théorique du phénomène.
En 1986 et 1988 des rapports complémentaires furent publiés, suite à l'article de van Eck, mais sans apporter d'autres informations concernant les expériences.

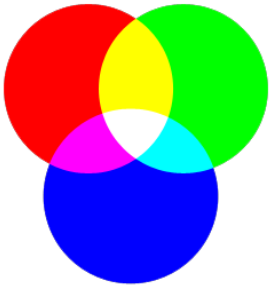
En 1998 John Young, un citoyen américain, demande à la NSA de publier des informations déclassifiés concernant le système TEMPEST. Voyant sa requête rejetée, il fait appel et obtient finalement en 1999 quelques documents, mais largement censurés.

Très peu d'informations sont disponible sur ce système. La plupart des documents ne font qu'exposer superficiellement le phénomène, sans rentrer dans les détails d'une expérience pratique.

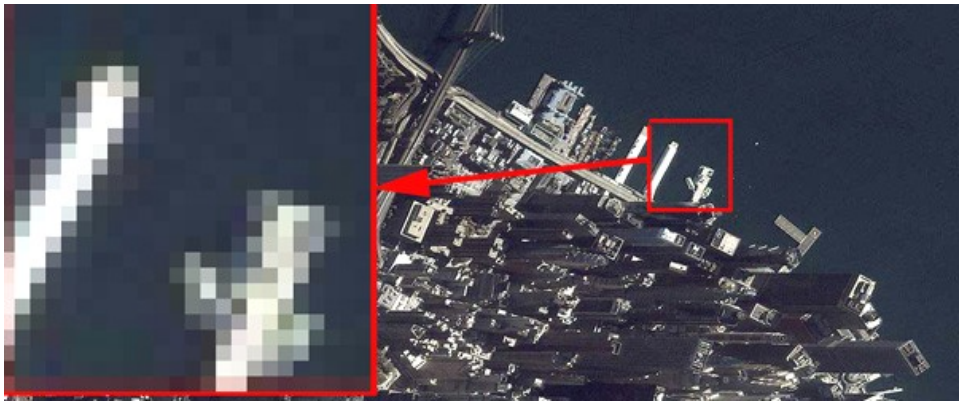
II.Théorie des écrans

1. Décomposition d'une image :

Les couleurs peuvent être décomposées en trois couleurs fondamentales : le Rouge, le Vert, et le Bleu. Il est possible par la combinaison de ces 3 couleurs de recréer n'importe quelle couleur, en variant les proportions de ces fondamentales.



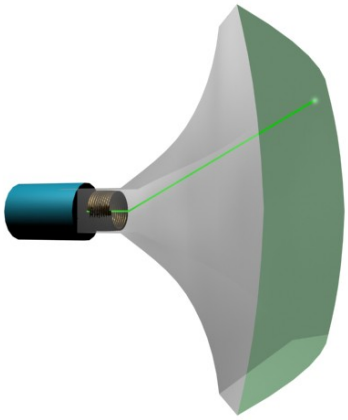
Une image est considérée comme un assemblage complexe de couleurs, sous la forme d'une grille de Pixels. Un Pixel est un point composé des 3 couleurs Rouge Vert Bleu.
Avec une grande densité de point, il est possible de restituer une image avec fidélité.



La résolution (finesse) de l'image se note X*Y, avec X le nombre de pixels horizontalement, et Y le nombre de pixels verticalement (ex : 640*480, 800*600, 1024*768…)

2. Restitution d'une image sur un écran :

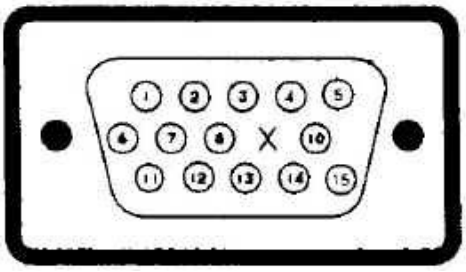
Un écran est composé de plusieurs modules :
Le tube cathodique sert à la restitution directe de l'image ;
Un faisceau d'électrons balaye une couche fluorescente à très grande vitesse pour afficher l'image. Le balayage se fait de gauche à droite et de haut en bas, à une fréquence de 50Hz à 100Hz sur la totalité de l'écran ; la couche fluorescente est excitée au passage de ces électrons et émet de la lumière. Cette couche est également phosphorescente, c'est-à-dire qu'elle continue à émettre de la lumière pendant un bref instant (de 10 à 20ms) après son excitation ; ainsi le phénomène de scintillement qui pourrait survenir est éliminé.



La luminosité des composantes fondamentales est déterminée par le débit d'électron, régulé par un wehlnet (composant électronique).
Le faisceau passe ensuite entre 2 bobines qui dévient sa trajectoire par électromagnétisme afin de réaliser le balayage de l'écran.

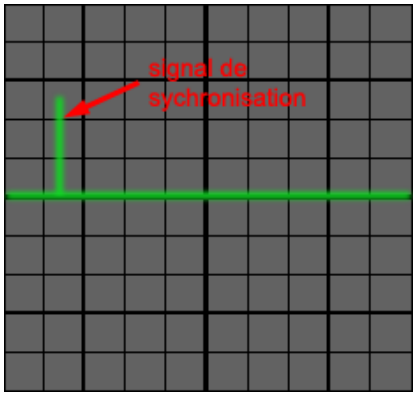
3. Codage du signal vidéo :

Le signal vidéo passe par plusieurs canaux ; 6 canaux pour le signal vidéo lui-même, c'est-à-dire les canaux Rouge, Vert, Bleu et leurs masses respectives, plus 2 canaux de synchronisation pour le balayage vertical et horizontal, et la masse commune au signaux de synchronisations..



Connecteur SUB-D HD – 1:Rouge, 2:Vert, 3:Bleu,
6:Masse Rouge, 7:Masse Vert, 8:Masse Bleu,
11 : Masse, 13 : Synchronisation horizontale, 14 : Synchronisation verticale

Les signaux de synchronisation, qui indiquent le passage à la ligne suivante ou le retour du faisceau au début de l'écran, sont de simples différences de potentiels de quelques volts. Ils ont lieux (pour un écran d'une résolution de 800*600 pixels avec un rafraîchissement de 70Hz) 70 fois par seconde pour les signaux de synchronisation verticaux, et 600*70=42000 fois par seconde pour les signaux de synchronisation horizontaux.



Les signaux vidéos sont des tensions de 0V a 0.7V, qui définissent l'intensité du point lumineux a l'endroit du balayage (cette tension est donc amenée à varier à chaque nouveau pixel de couleur différente ; pour un écran de résolution 800*600 avec un rafraîchissement de 70Hz, les changements de tensions peuvent aller à une fréquence de 800*600*70=34Mhz, soit 34 000 000 de fois par seconde).

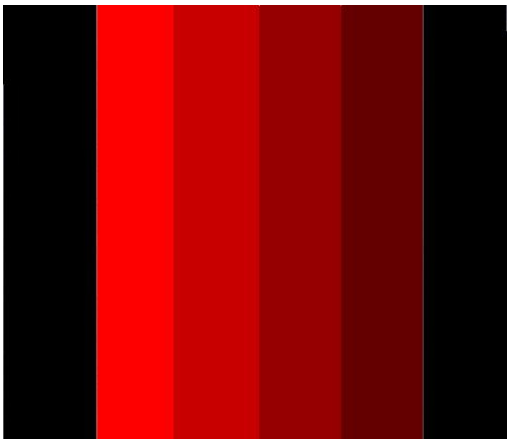
III. L'élaboration théorique du circuit :

1. *Les exigences du circuit :*

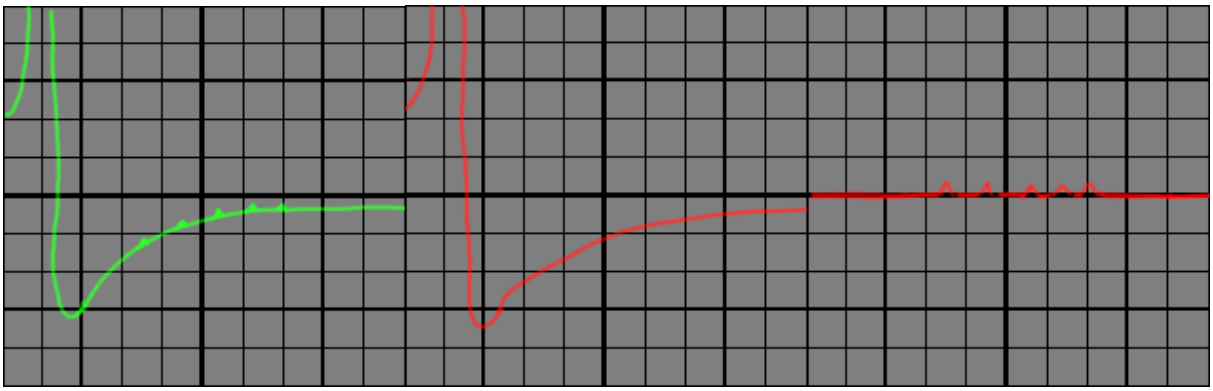
Plus haut nous avons vu la nature des signaux électriques véhiculant l'information vers l'écran, et que ces signaux étaient amplifiés pour afficher l'image. De cette amplification résulte l'émission d'ondes de compromissions de forte amplitude à la sortie, que nous cherchons à capter.

A chaque différence de potentiel à la sortie du circuit d'amplification est émis une onde électromagnétique, d'amplitude proportionnelle. L'amplitude de cette onde décroît avec la distance du fait de la répartition de l'énergie électromagnétique sur le front d'onde sphérique.

Un exemple d'onde électromagnétique en fonction de l'image affichée :



L'écran affiche une dégradé de rouge pur entouré de bandes noires



Une observation à l'oscilloscope nous montre que le signale est déformé (image de droite) par l'amortissement de l'onde lié au signal de synchronisation horizontal (au centre) ; remarquons que le signal « oscille » sur l'axe des ordonnées à cause des perturbations liées au secteur. Nous voulons récupérer le signal vidéo (à gauche).

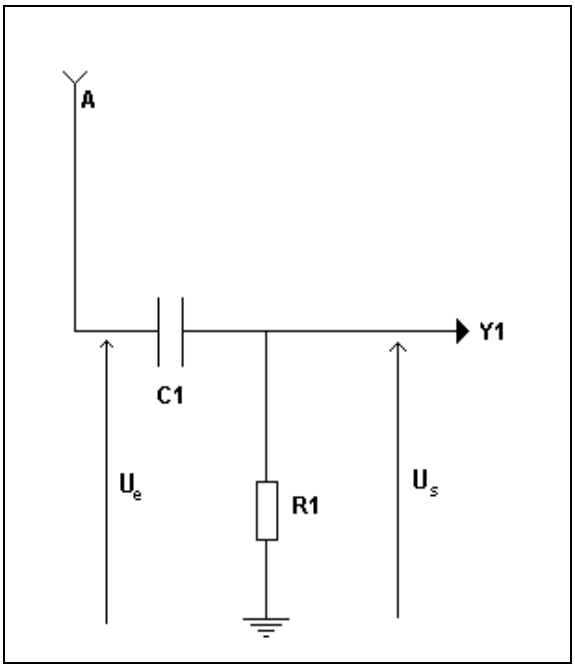
D'après ce que nous avons montré précédemment, ce signal n'est pas exploitable directement par un écran, car nous avons besoin d'un signal positif dont la tension varie entre 0V et 0.7V.

Le montage à réaliser doit donc permettre d'annuler l'effet causé par le signal de synchronisation et le secteur mais également d'amplifier le signal.

2. *Le filtrage des signaux :*

Dans le but d'éliminer les signaux parasite nous mettons en place, entre l'antenne réceptrice et l'écrans, un circuit passe-bande. Il existe deux types de circuit passe-bande, les passe-haut et les passe-bas qui laissent passer respectivement, les fréquences supérieures à leur fréquence de coupure ou les fréquences inférieures à leurs fréquences de coupure.

Dans notre cas nous avons besoin d'un circuit passe-haut, puisque la fréquence des signaux vidéo (plusieurs dizaines de MHz) est supérieure à celle des signaux de synchronisations (quelques dizaines de KHz pour les signaux de synchronisations horizontaux).



Le montage en dérivation d'un condensateur et d'une résistance permet la création d'un filtre passe-haut.

En effet tout signal périodique peut être considéré comme la somme de signaux sinusoïdaux et par conséquent, le filtre passe-haut peut « supprimer » les composantes dont les fréquences sont inférieures à la fréquence de coupure comme suivent :
Lorsqu'il est soumit à une tension sinusoïdale, le condensateur se charge, puis lors du changement de sens de variation de la sinusoïde, celui-ci se décharge, néanmoins, si la période de la tension est supérieur au temps de charge du condensateur, celui-ci agit comme un coupe-circuit et empêche le passage du signal. On peut faire varier la fréquence de coupure en ajustant les valeurs de C et de R.On pose $\tau = RC$, si τ augmente, le temps de charge du condensateur augmente et donc la fréquence de coupure diminue.

On en déduit que la fréquence de coupure f_c est inversement proportionnelle à $\tau = RC$ .On a :

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

On peut ainsi déduire l'allure de la tension en sortie du dispositif en fonction de la tension d'entrée :

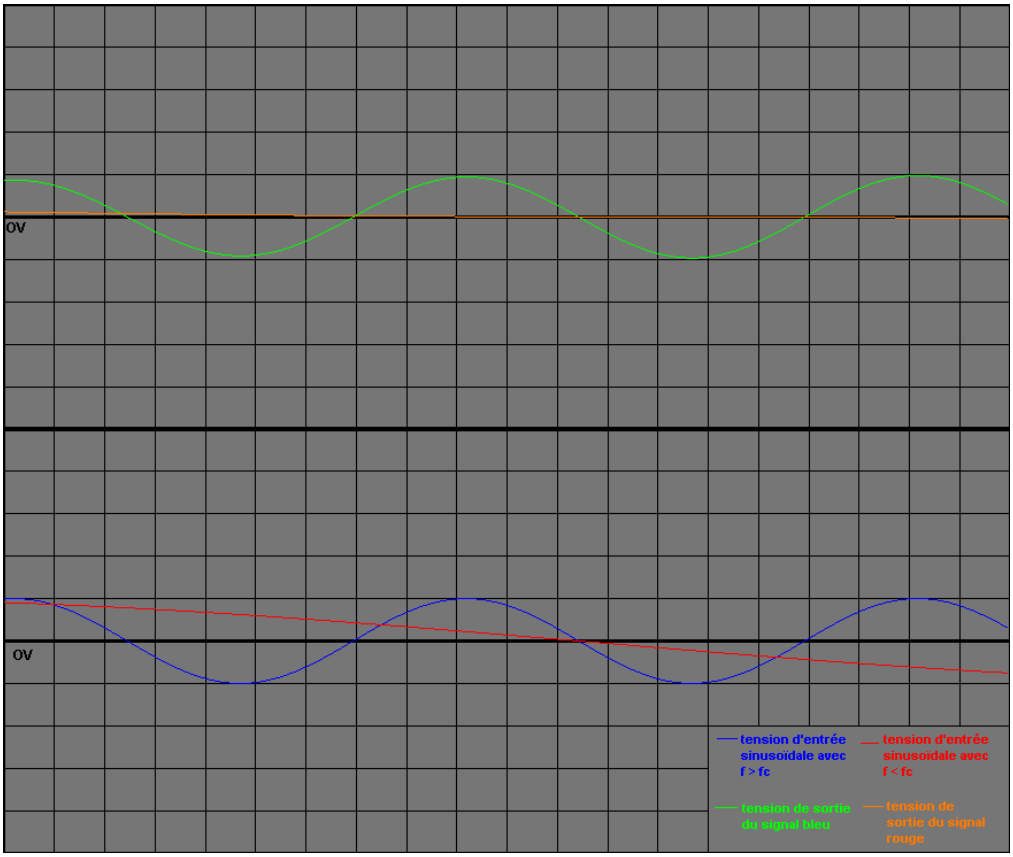
Si la fréquence d'entrée f_e est supérieure à la fréquence de coupure, le condensateur se charge positivement puis négativement, on peut ainsi écrire l'équation de la tension aux bornes du circuit RC :

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

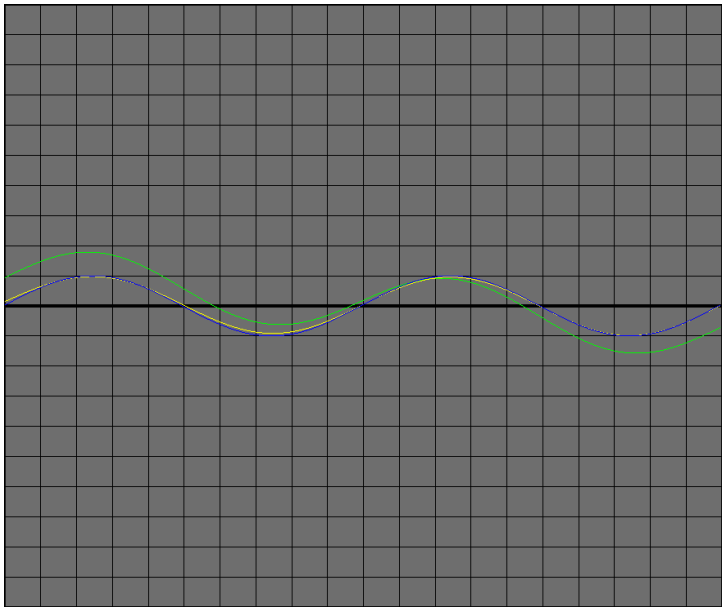
Si la fréquence d'entrée f_e est inférieure à la fréquence de coupure, le condensateur se charge puis ne se décharge pas car il arrive à son régime maximum avant que la tension change de sens de variation, la tension vacille légèrement, de quelques millièmes de volts, on peut ainsi écrire l'équation de la tension aux bornes du circuit RC :

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

On peut donc tracer la tension aux bornes du circuit RC, en fonction de la fréquence de la tension d'entrée :



Ainsi si la tension d'entrée est la somme de deux (ou plus) signaux, l'un de fréquence supérieure à la fréquence de coupure et l'autre de fréquence inférieure à la fréquence de coupure, il ne ressort que le signal de fréquence supérieure à la fréquences de coupure :

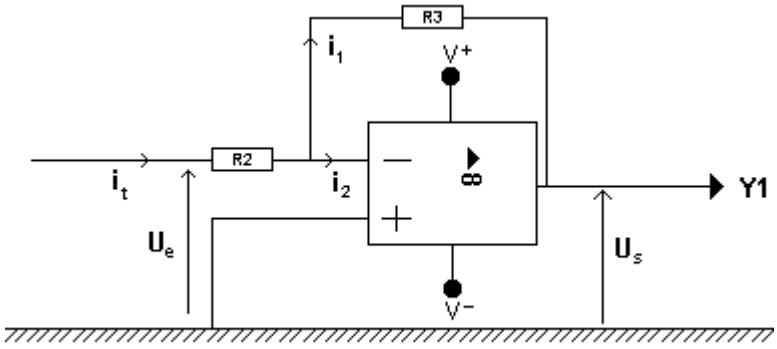


On remarque que le signal de sortie (jaune) est « presque » le même que le signal de fréquences supérieure à la fréquence de coupure (bleu). Il est légèrement déformé. En vert, le signal d'entrée, somme de deux signaux de fréquences différentes.

En sortie de circuit RC, on obtient donc un signal n'ayant conservé que les informations vidéo. Celles-ci ne sont alors pas encore exploitable, il faut pour cela les amplifier.

3. *L'amplification :*

Pour avoir un signal exploitable, il nous faut un signal compris entre 0V et 0.7V, il faut donc l'amplifier mais tout en gardant la proportion des signaux entre eux, pour cela nous devons donc multiplier la tension sortie du circuit RC par un facteur k. Pour cela nous choisissons l'emploi d'un circuit basé sur un Amplificateur Opérationnel (A.O) en montage dit « inverseur ».



Un circuit inverseur qui amplifie la tension d'entrée par un coefficient k.

Dans un tel circuit, nous voyons que la loi d'Ohm s'applique à la résistance R_2, celle-ci fait donc diminuer la tension entrant dans l'amplificateur opérationnel, la tension U_r est donc inférieure à la tension U_e, la tension U_s est donc inversement proportionnelle à la valeur de la résistance R_2.
La résistance R_3 est en dérivation avec l'AO ; plus elle sera de valeur importante, moins de courant la traversera, et donc plus de courant traversera l'AO, sachant qu'on a $i_1 < i_2$ .On en déduit que la tension de sortie est proportionnelle à la valeur de la résistance R_3.

On remarque que le montage est inverseur (entrée sur la borne négative et masse à la borne positive) le signal de sortie est donc multiplié par un coefficient négatif, ainsi on en déduit que :

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

Ainsi en réglant les valeurs de R_2 et R_3 nous faisons varier la tension aux bornes d'entrées de l'amplificateur opérationnel, celui-ci va ensuite, par l'intermédiaire de son alimentation stabilisée (branchée sur les borne V^+ et V^-) pouvoir multiplier la tension du signal d'entrée.

4. La synchronisation des signaux :

Les signaux récupérés sont désynchronisés, l'écran ne peut donc pas les restituer de façons cohérente, il faut donc envoyer à l'écran une synchronisation « artificielle », pour cela, on peut utiliser deux méthodes :

- générer des signaux à l'aide de deux GBF (un pour la synchronisation horizontale et l'autre pour la synchronisation verticale).
- récupérer les signaux émis par la carte graphique d'un ordinateur en fonctionnement.

La première solution paraît la plus appropriée car elle permet des changements pour adapter les signaux de synchronisation aux signaux reçus.

5. Les résultas escomptés :

Du fait qu'une onde n'est émise qu'à chaque différence de tension dans l'écran, l'image obtenue ne pourra pas être la reproduction fidèle de la première mais permettra l'accès aux informations affichées sur l'écran source. On obtient donc en théorie une image de ce type :

IV. Réalisation expérimentale :

1. *Le choix des valeurs pour le passe-haut :*

Comme nous l'avons vu plus haut, nous voulons supprimer les effets des signaux de synchronisation ; ceux ci se répétant à une fréquence d'environ 70*600=42KHz (pour un écran en 800*600*70Hz, en tenant compte des signaux de synchronisation horizontaux) nous choisissons une valeur de fréquence de coupure f_c un peu plus grande de manière à avoir une marge de sécurité, et d'éliminer un maximum de signaux parasites. On choisit donc une fréquence de coupure voisine de 160 KHz :

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

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

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

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

Nous devons donc choisir un rapport RC voisin de 10^{-6} s ; or les condensateurs ont des valeurs maximums de l'ordre du micro Farad (µF), la résistance employée devra donc être de l'ordre du kilo Ohm (kΩ).

2. *Le choix des valeurs pour l'amplification :*

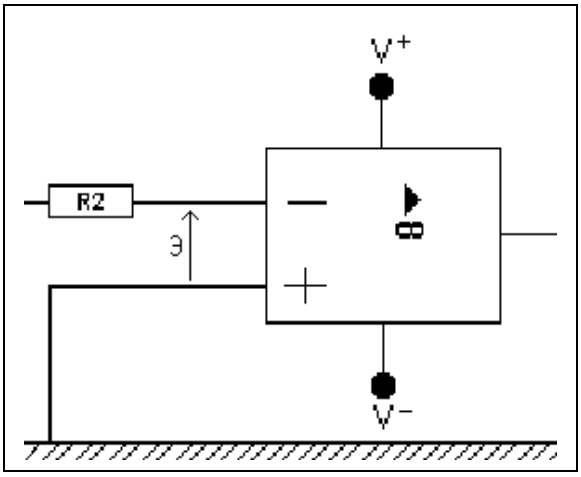
a. choix d'un modèle d'amplificateur opérationnel :

Pour notre utilisation nous avons besoin d'un amplificateur opérationnel capable de supporter de très importantes fréquences voisine de 50 MHz, nous avons par sécurité choisit un A.O. gérant jusqu'à 60 MHz, il s'agit donc d'un A.O. spécialement conçut pour les montage vidéo, le modèle sélectionné est le AD844AN ; celui-ci nécessite pour un fonctionnement normal une alimentation stabilisée a 5V et une tension d'entrée maximum de 5 µV.

b. Choix des valeurs des résistances :

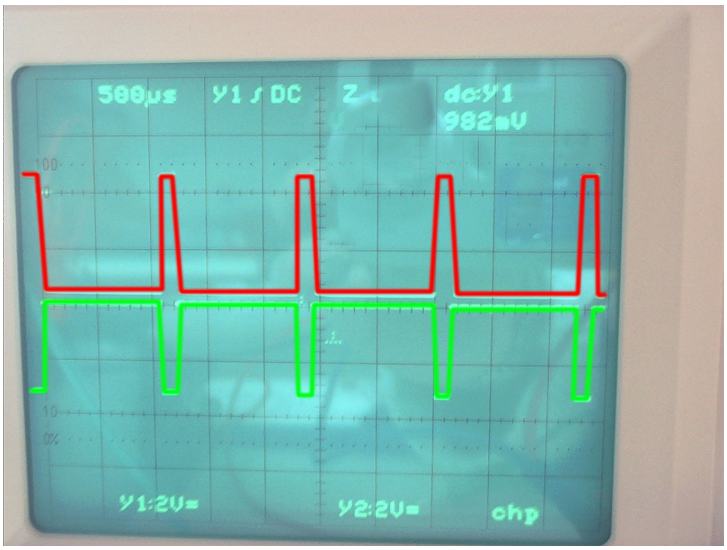
• Notre modèle d'amplificateur opérationnel nous oblige à prendre une résistance de très forte valeur de manière à avoir une tension d'entrée de 5 µV. Pour avoir un ordre de grandeur nous menons le raisonnement suivant :

Une tension est une différence d'état électrique, donc la différence entre deux potentiels ; plus l'écart est faible, plus la tension est faible !



Notre objectif est donc de choisir une résistance nous permettant d'avoir une tension 3 de 5 µV ; or le fil de la borne positive est relié à la masse, son potentiel est donc de zéro ; il nous faut donc un potentiel de 5 µV dans le fil à la borne négative, or cette valeur est extrêmement faible devant le potentiel d'entrée (de environs 0.1V), en prenant une résistance très grandes nous obtiendrons alors une forte tension au borne de la résistance (loi d'Ohm) et donc un faible potentiel à la borne moins, nous choisissons donc une résistance variable R_2 de 1 Ω (Ohm).

•Nous avons vu plus haut l'expression du rapport d'amplification, sachant que nous voulons amplifier dans une tranche de 1 à 100, il nous faut donc une résistance R_3 de l'ordre de 10 à 100 Ω.

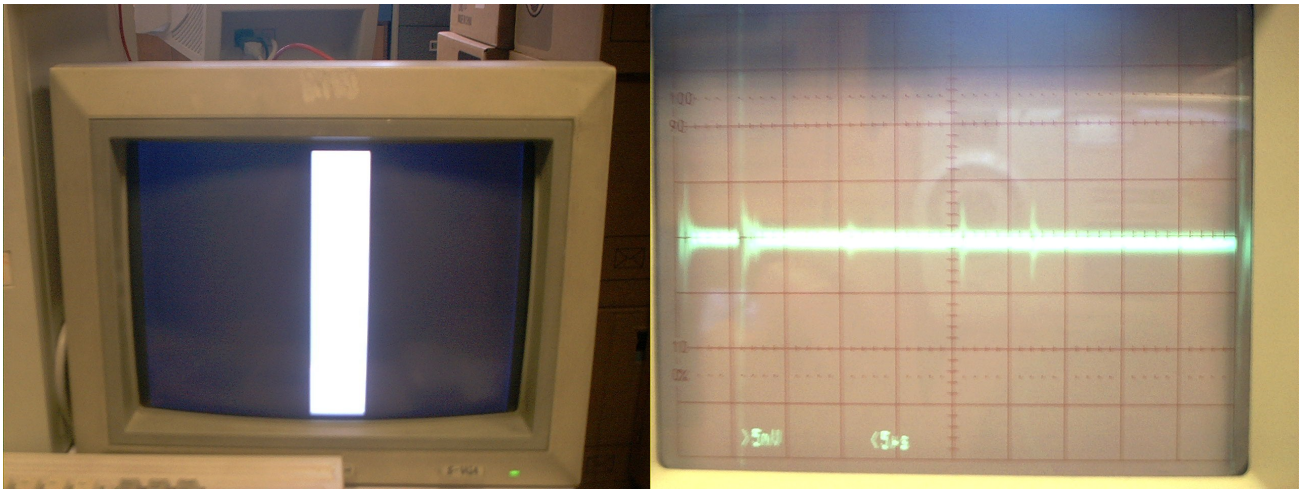


Le signal original (et vert, -3V) et après amplification (en rouge, +5V)

V. Résultats expérimentaux :

A l'heure où nous rédigeons ce dossier, notre expérience n'a pas été encore achevée (bien que nous possédions maintenant tous les éléments pour la mettre en œuvre complètement).

Les résultats les plus encourageant que nous ayons obtenus sont visibles ici :



A gauche l'image originale ; à droite, les 2 pics centraux captés par électromagnétisme correspondent au début et à la fin de la bande blanche.

Le signal de droite a été obtenu grâce au filtre passe haut, ce qui prouve son efficacité. Il ne nous reste plus qu'à amplifier ce signal et à le transmettre à un 2em écran, que nous synchroniserons à l'aide de 2 G.B.F., pour obtenir une image fantôme, similaire à l'image originale.

Nous avions quelques problèmes avec l'amplificateur opérationnel (concernant notamment les résistances) mais ceux-ci ont été résolus (comme en atteste l'image de la page précédente).