

Cryptimage

guide de l'utilisateur

Table des matières

1. Introduction.....	2
2. Définition du discret 11.....	2
3. Définition du nagravision syster.....	2
4. Définition du videocrypt.....	3
5. Définition du MAC-Eurocrypt.....	4
6. Installer le logiciel.....	7
a. Windows.....	7
b. Linux, MacOSX.....	7
7. Utilisation de cryptimage.....	8
a. Mode.....	9
b. Fichiers.....	9
c. Options discret11.....	10
- Coder/décoder/décoder par corrélation de lignes.....	10
- Mot de 16 bits.....	10
- Audience.....	10
a. Audiences de 1 à 7.....	10
b. Le multicode.....	11
- Retards 1 et 2.....	11
- Bordure masquée.....	12
- Traiter le son, désactiver le son.....	12
- Seuil du blanc.....	12
- Démarrer à la trame.....	13
- Code clavier décodeur.....	13
d. Options nagravision syster.....	14
a. Options de codage.....	14
b. Options de décodage.....	16
e. Options videocrypt.....	17
a. Options de codage.....	17
b. Options de décodage.....	18
f. Options MAC-Eurocrypt.....	19
g. Options transcode.....	20
h. Rendu des couleurs.....	20
i. Options audio/vidéo.....	21
j. Informations.....	23
8. Utiliser cryptimage avec un décodeur matériel.....	23
a. Fixer un numéro de série dans la rom.....	24
b. Injecter un fichier vidéo à votre décodeur.....	25
9. Conseils.....	27
10. Bugs.....	28

1. Introduction

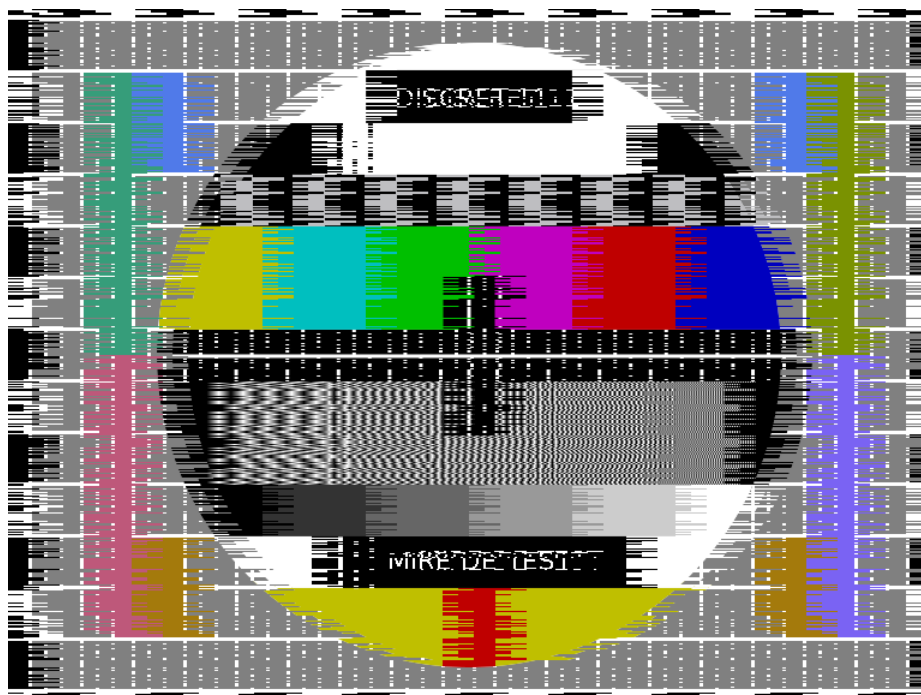
Cryptimage est un logiciel open source sous licence GNU GPL v3 permettant de reproduire parfaitement le procédé de cryptage et de décryptage « discret 11 » utilisé entre 1984 et 1995 par la chaîne de télévision française canal plus, ainsi que le procédé « nagravision syster » qui a succédé au discret 11 jusqu'en 2010, le procédé « videocrypt » utilisé par les chaînes du groupe britannique Sky, ainsi que d'autres chaînes européennes du bouquet satellite astra, et enfin le standard vidéo MAC associé au cryptage Eurocrypt.

Ce logiciel permet de convertir un fichier vidéo en une version cryptée (image et son), et permet aussi de décrypter un fichier vidéo qui a subi un cryptage en respectant la norme de ces systèmes de cryptage.

Outre la possibilité de reproduire sous forme de fichier numérique ces procédés de cryptage, sa seconde utilité est de permettre aux possesseurs de décodeurs discret 11 de les faire revivre en leur injectant ce fichier vidéo crypté.

2. Définition du discret 11

Le procédé discret 11 consiste à crypter l'image en retardant chaque ligne selon 3 valeurs au choix (0, 902 et 1804 millisecondes), les retards étant sélectionnés via un algorithme reposant sur une séquence pseudo-aléatoire, le son étant quant à lui rendu inintelligible en lui faisant subir une inversion de spectre autour de la fréquence 12800 hertz.



exemple de cryptage discret 11 sur une mire Philips PM5544

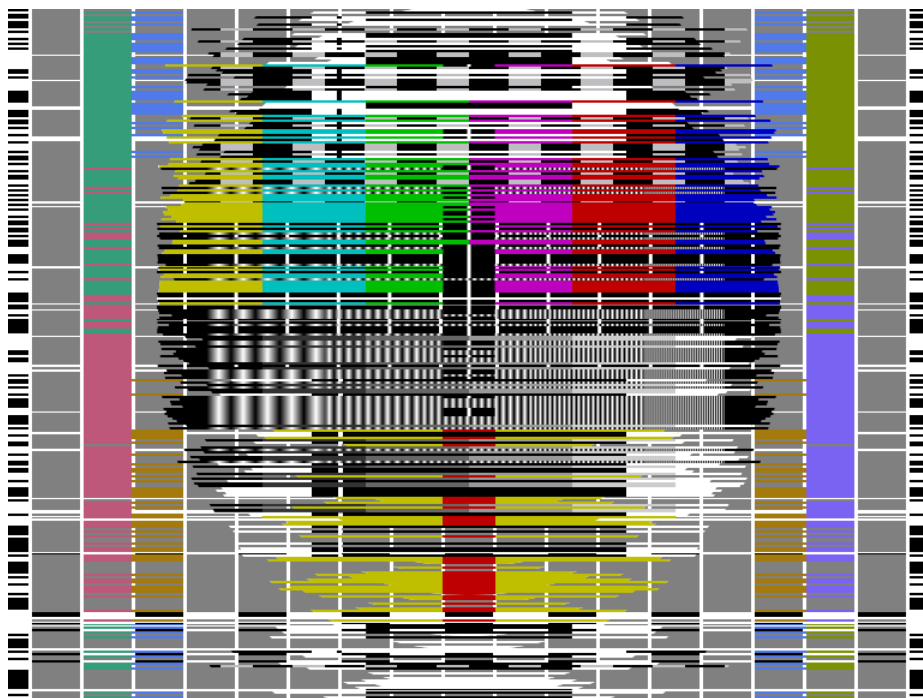
3. Définition du nagravision syster

Le nagravision syster (SYStème TERrestre) consiste à mélanger les lignes de manière verticale, de façon à rendre peu compréhensible l'image, les 2 demi-images d'une trame progressive voient leurs

287 premières lignes mélangées (la 288ième ligne n'est pas cryptée) , puis ensuite chaque demi-image voit ses 32 premières lignes reportées sur la demi-image précédente, cela donne le schéma suivant pour une demi image de 288 lignes qui a subi un cryptage :

- 255 premières lignes cryptées
- 32 lignes suivantes cryptées mais appartenant à la demi-image suivante
- la dernière ligne (288) n'est pas cryptée et appartient bien à la demi-image en cours

pour décrypter une trame complète il va falloir donc recomposer dans l'ordre les 287 lignes cryptées en prélevant 32 lignes d'une demi-image (lignes 256 à 287), puis les 255 premières lignes de la demi-image suivante afin de former une nouvelle demi-image décryptable, puis retrouver l'ordre original des lignes en utilisant un couple « offset, incrément » et une table primaire contenant 256 valeurs de 0 à 31 , cette table est parcourue 255 fois de manière circulaire via une adresse de départ (l'offset, valeur de 0 à 255) auquel on ajoute un incrément (valeur impaire comprise entre 1 et 127) , c'est de cette manière que chaque demi-image sera décryptée.

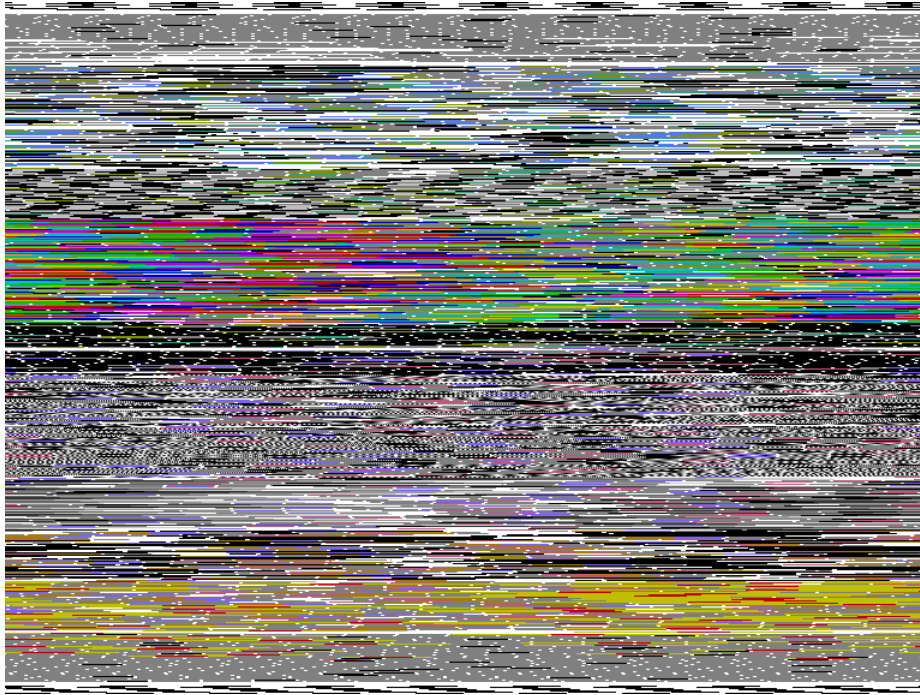


exemple de cryptage nagravision syster sur une mire Philips PM5544

4. Définition du videocrypt

Le videocrypt consiste à utiliser le principe du « cut and rotate », à chaque ligne un point de coupe est choisi (sur 256 possibilités), autour de ce point de coupe la partie droite de la ligne va à gauche et la partie gauche va à droite, ce processus est répété pour l'ensemble des lignes de l'image, donnant ainsi une image très embrouillée .

Généralement le son n'est pas crypté même s'il fut envisagé à un moment de le faire.



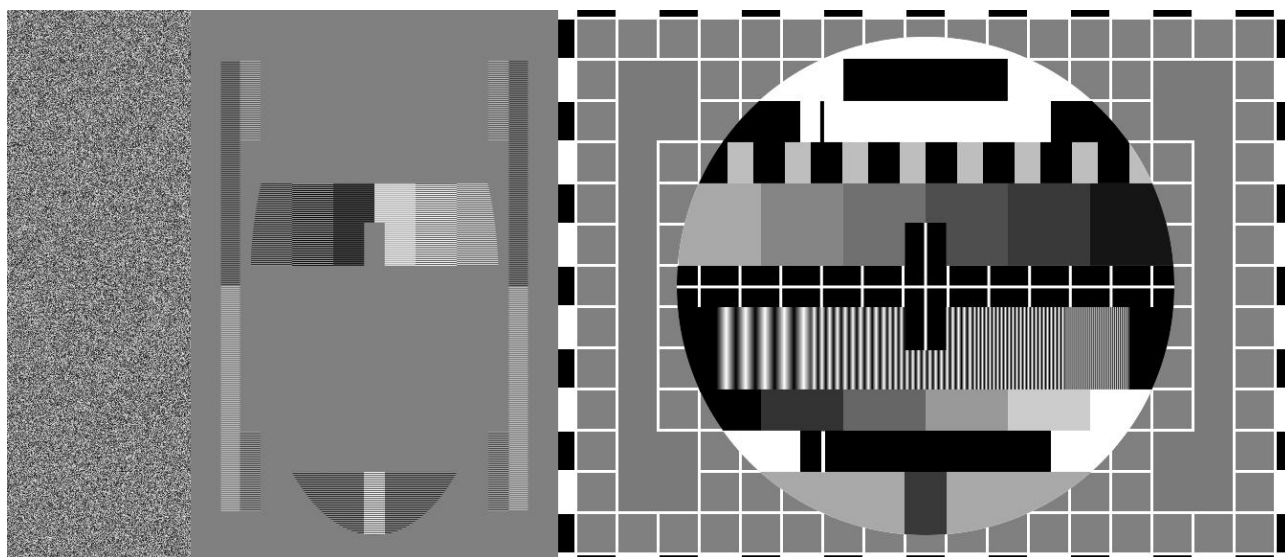
exemple de cryptage videocrypt sur une mire Philips PM5544

5. Définition du MAC-Eurocrypt

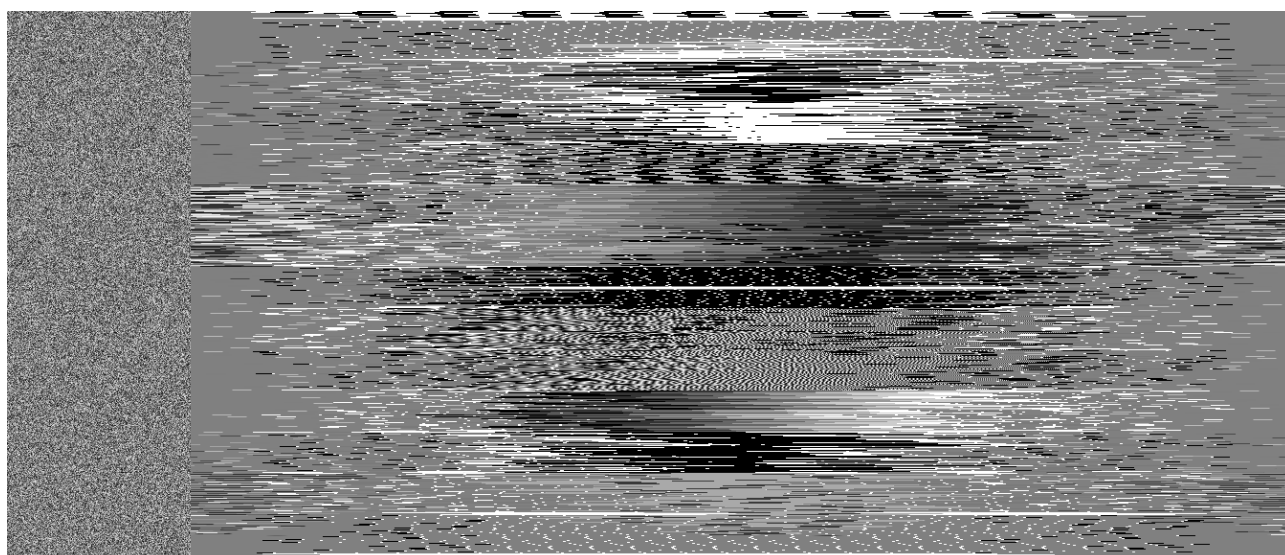
Le MAC (Multiplexed Of Analog Components) est un standard de vidéo développé dans les années 80, qui consiste à transmettre de manière séquentielle le son, puis la chroma et enfin la luma à chacune des 576 lignes de l'image, contrairement aux autres standards couleurs (PAL/SECAM/NTSC) la partie chroma n'est pas mélangée avec la luma, ce qui permet une bien meilleure qualité.

Pour la télévision à péage un mode de chiffrement est possible, avec l'Eurocrypt, basé sur le principe du « cut and rotate » similaire au videocrypt, avec deux variantes :

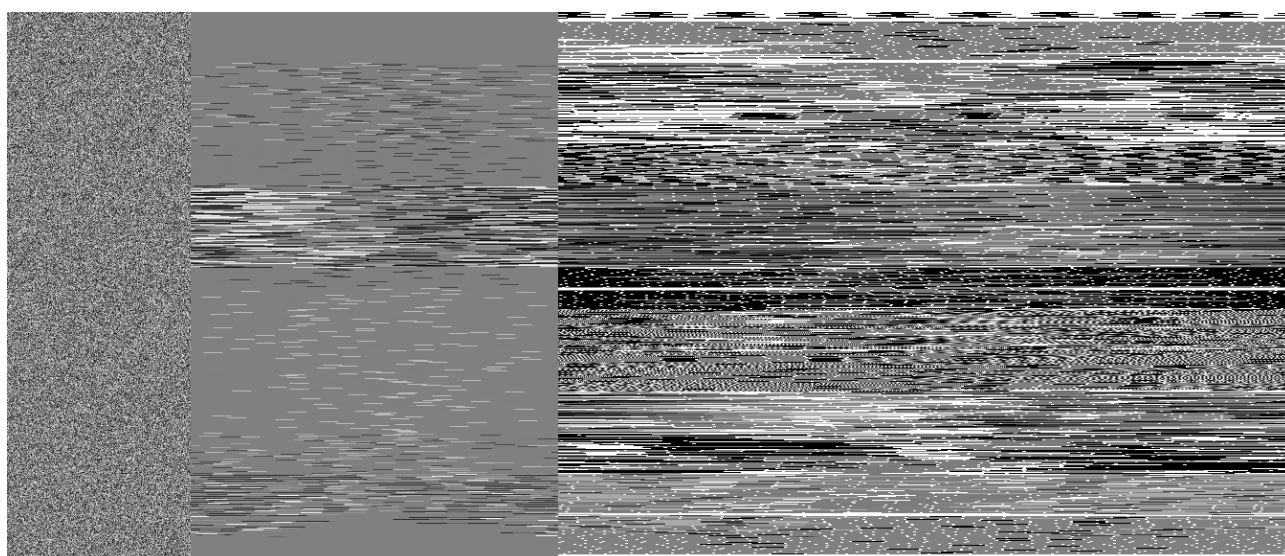
- single cut (simple coupe) où seule la partie chroma subit un point de coupe, avec la partie luma qui se retrouve au milieu des 2 parties de la chroma ayant subit une rotation,
- double cut (double coupe) où la partie chroma et la partie luma subissent tous les 2 une opération de « cut and rotate ».



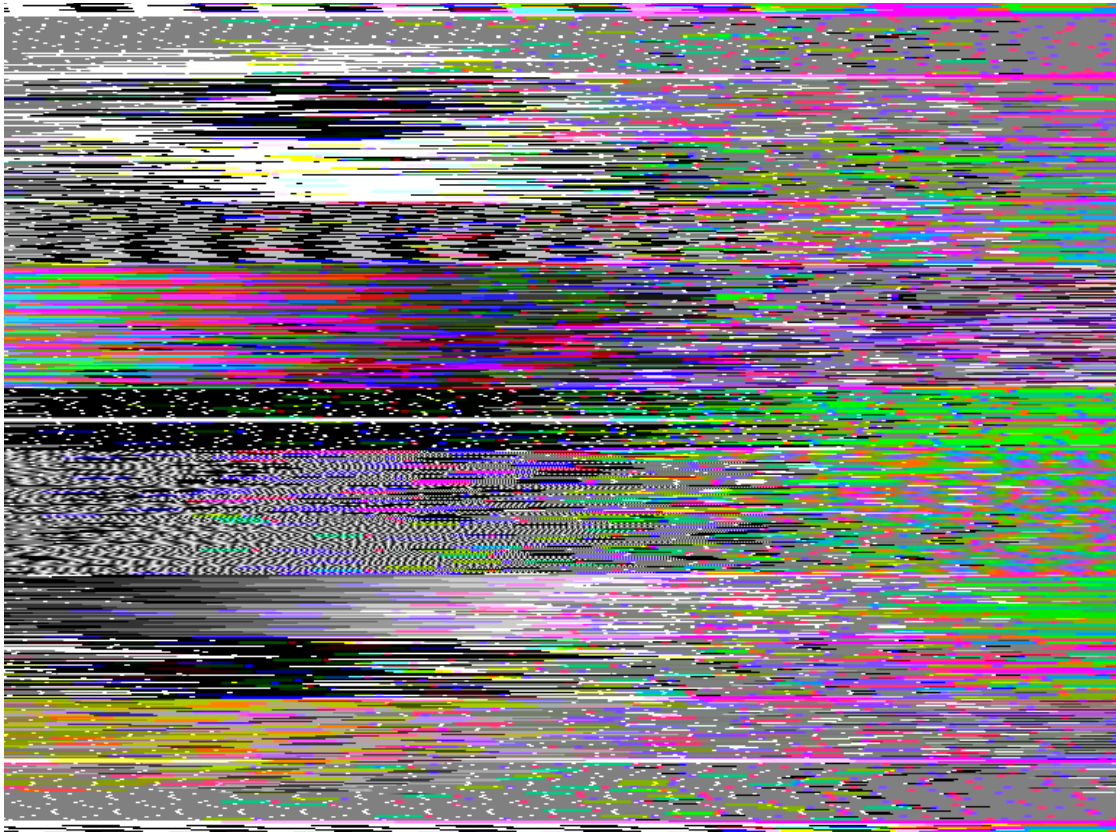
Encodage MAC sans cryptage Eurocrypt



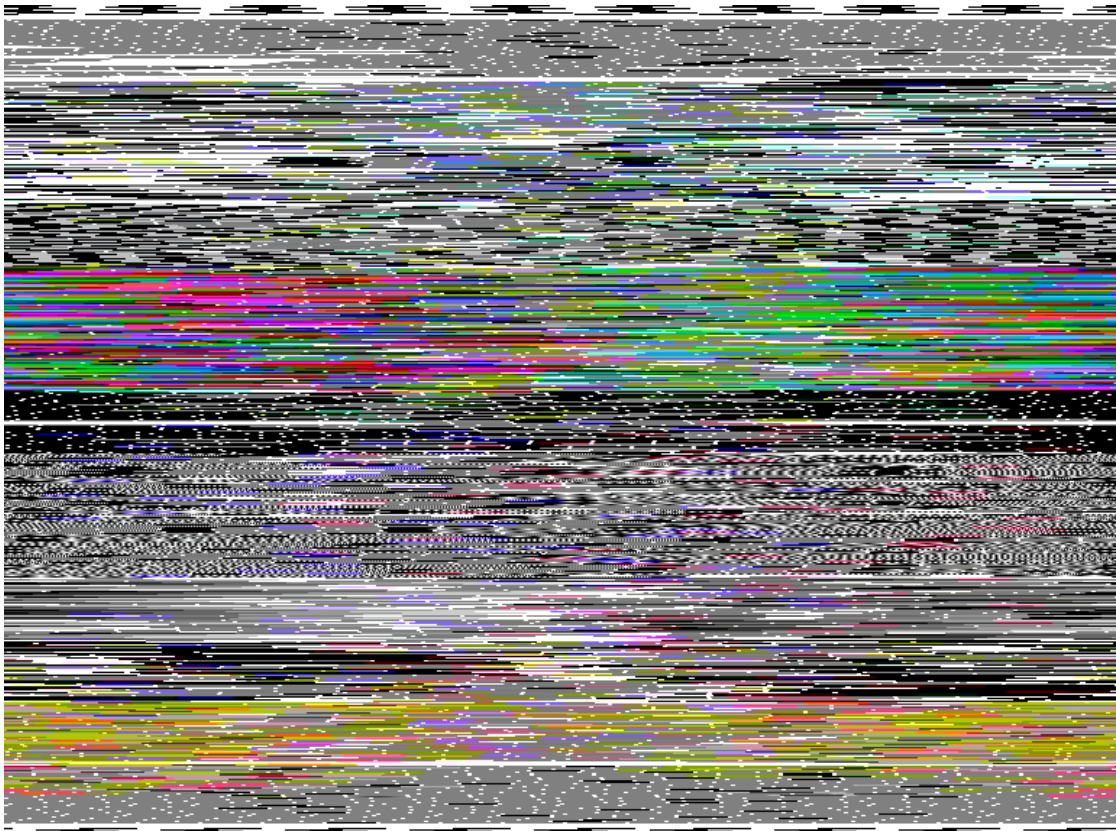
Encodage MAC avec cryptage Eurocrypt single cut (simple coupe)



Encodage MAC avec cryptage Eurocrypt double cut (double coupe)



Décodage d'un format MAC crypté « Eurocrypt simple cut » par un récepteur satellite/câble n'ayant pas les droits nécessaires pour le décodage Eurocrypt



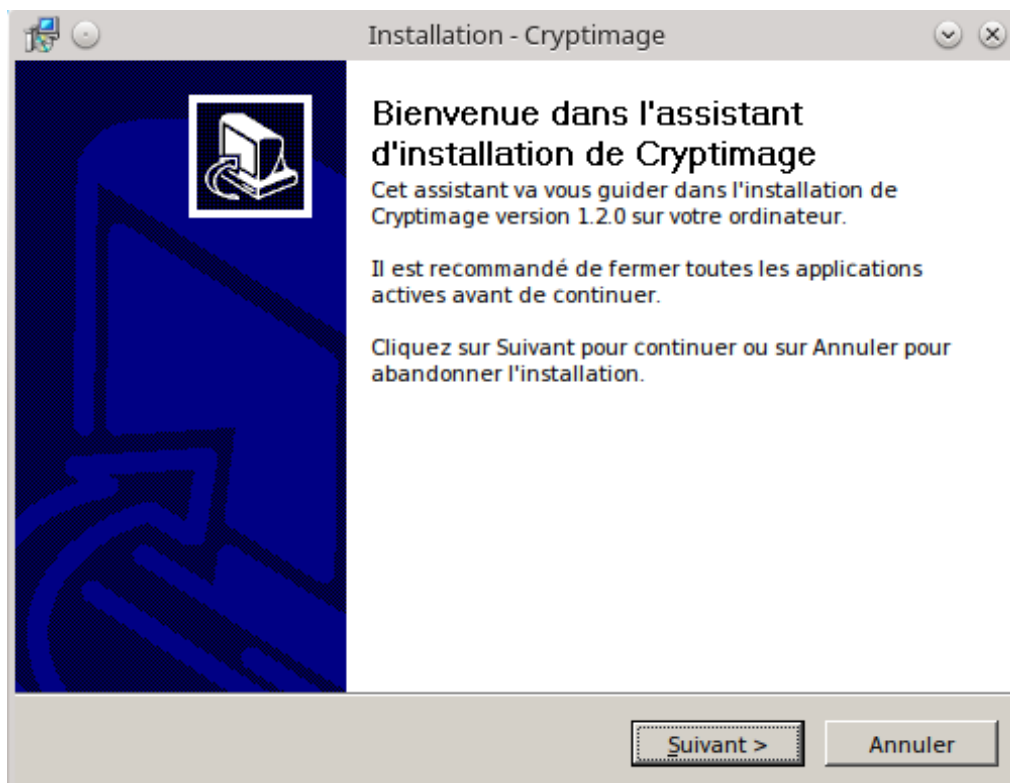
Décodage d'un format MAC crypté « Eurocrypt double cut » par un récepteur satellite/câble n'ayant pas les droits nécessaires pour le décodage Eurocrypt

6. Installer le logiciel

a. Windows

La manière la plus simple d'installer cryptimage (si vous êtes sous windows) est d'utiliser le fichier de type « setup.exe » disponible dans la section téléchargements du site officiel de cryptimage :

<http://ibsoftware.free.fr/cryptimage.php>



ce fichier setup installera le programme avec sa machine virtuelle java embarquée, créera un lien sur le bureau ainsi que dans le menu démarrer vers l'exécutable principal, installera la documentation et un lien pour désinstaller cryptimage.

Le lancement de cryptimage s'effectue simplement via le raccourci «cryptimage.exe » sur le bureau ou depuis le menu démarrer, programmes, cryptimage.

b. Linux, MacOSX

Si vous êtes sous un autre système d'exploitation (linux, macOS) il vous faudra télécharger la version jar, puis installer la machine virtuelle java en allant sur le site de java :

<https://www.java.com/fr/>

une fois installé le lancement peut s'effectuer en double cliquant sur le fichier jar ce qui lancera la machine virtuelle java chargée d'exécuter cryptimage (si ce n'est pas le cas il faudra associer le processus java à l'ouverture des fichiers jar lors d'un clic sur ce type de fichier, consultez la documentation de votre système d'exploitation pour plus de détails),

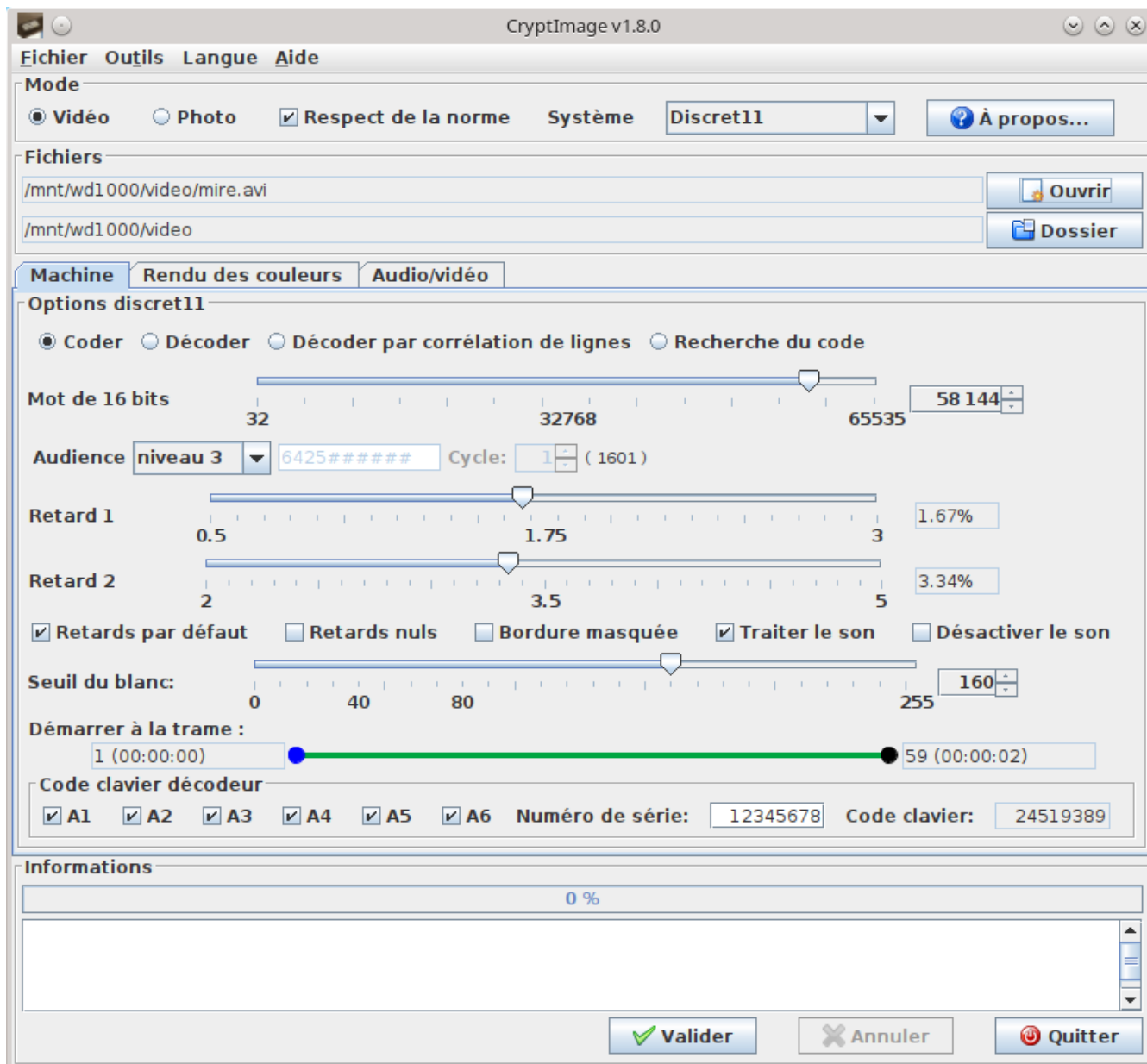
le lancement de cryptimage peut aussi s'effectuer depuis une console en tapant cette commande

depuis le dossier où se trouve le fichier jar :

```
java -jar cryptimage.jar
```

7. Utilisation de cryptimage

Au lancement de cryptimage vous aurez l'affichage de l'interface principale de configuration :

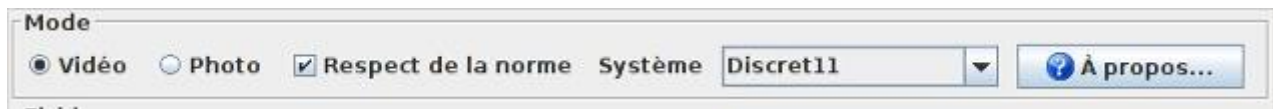


interface de cryptimage, le rendu peut être différent selon votre système d'exploitation

l'interface est découpée en 6 rubriques : « mode », « fichiers », « options discret11/nagravision system/videocrypt/MAC-Eurocrypt/transcode » (onglet « machine »), « rendu des couleurs », « options audio/vidéo » et « informations ».

En outre une barre de menu est présente, un menu « langue » permet de changer la langue de l'interface graphique, 6 langues au choix : allemand, anglais, espagnol, français, italien et polonais.

a. Mode



Ici vous pouvez sélectionner « vidéo » si vous voulez crypter/décrypter un fichier vidéo, ou bien sélectionner « photo » si vous voulez crypter/décrypter un fichier image.

Une case à cocher « respect de la norme » permet de spécifier si vous voulez un respect total de la norme discret11, si cette case est cochée alors l'image sera automatiquement redimensionnée au format 4/3 576 lignes, et la gestion des lignes TV 310 et 622 sera assurée (colorisation de ces lignes en blanc et en noir), si cette case n'est pas cochée alors le fichier crypté/décrypté conservera sa taille d'origine sans aucune colorisation des lignes TV 310 et 622, le mode « respect de la norme » est surtout utile pour ceux qui veulent alimenter un décodeur officiel (ou non officiel) discret11 ou ceux qui veulent une reproduction 100 % fidèle du système discret11.

À noter que pour le mode nagravision syster, videocrypt et MAC-Eurocrypt cette case sera cochée par défaut et grisée car ces 3 systèmes ne peuvent fonctionner qu'en mode « respect de la norme ».

Enfin une liste déroulante « système » permet de choisir le système : « discret11 », « nagravision syster », « videocrypt », « MAC-Eurocrypt » et « transcode ».

b. Fichiers



Cette partie vous permet de charger le fichier à traiter (bouton « ouvrir »), puis de définir le répertoire de travail où seront stockés les fichiers cryptés/décryptés (bouton « dossier »), par défaut si vous ne spécifiez pas de dossier de travail alors ce sera le dossier où se trouve le fichier chargé qui sera utilisé.

c. Options discret11

Ce panneau permet d'indiquer les réglages du codeur/décodeur logiciel discret11, ce panneau apparaîtra si la liste déroulante « système » est positionnée sur « discret11 » .

- Coder/décoder/décoder par corrélation de lignes

Ces boutons de sélection permettent de choisir le mode « codeur » (cryptage du fichier), le mode « décodeur » (décryptage du fichier) et le mode de décryptage par corrélation de lignes (ce mode n'est disponible que si la case « respect de la norme est cochée ») .

- Mot de 16 bits

il s'agit d'une valeur comprise entre 32 et 65535 qui sera ensuite utilisée par cryptimage pour calculer d'autres paramètres (mot de 11 bits selon le niveau d'audience, le code clavier) , tous les décodeurs matériels discret11 sont initialisés par ce mot de 16 bits (cette valeur étant déduite d'après le code clavier à huit chiffres tapé en façade, nous verrons ce point plus tard dans la documentation).

- Audience

a. Audiences de 1 à 7

Vous pouvez choisir 7 niveaux d'audience dans la liste déroulante, ainsi qu'un niveau spécial appelé « multicode », les 7 premiers niveaux d'audience permettent de générer automatiquement un mot de

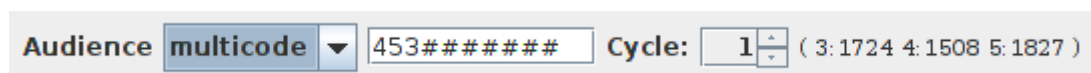
11 bits (valeurs de 1 à 2047), c'est grâce à ce mot de 11 bits que sera initialisé le générateur de valeurs pseudo-aléatoires du codeur/décodeur, des valeurs qui permettront de sélectionner le type de retard à appliquer à chaque ligne de l'image.

Cryptimage vous indique aussi entre parenthèses le mot de 11 bits utilisé en fonction du niveau d'audience sélectionné.

Le niveau d'audience 7 correspond à celui utilisé à l'époque par canal plus le dernier week-end du mois, c'est le « code universel » permettant aux décodeurs officiels de fonctionner même en l'absence d'un code clavier valide.

À noter qu'en mode « décodage » si la case « respect de la norme » a été cochée alors cryptimage sera capable de décoder la vidéo sans avoir besoin de spécifier le niveau d'audience dans l'interface, car cryptimage utilisera la fréquence de clignotement de la ligne TV 622 de l'image pour en déduire le niveau d'audience.

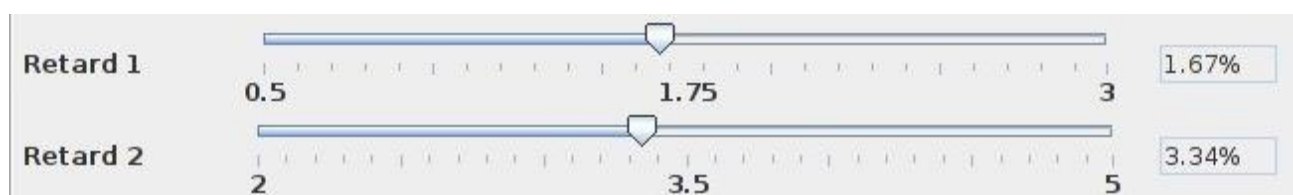
b. Le multicode



Vous pouvez aussi choisir d'utiliser le « multicode » présent dans la liste déroulante, le multicode vous donne la possibilité de spécifier jusqu'à 10 niveaux d'audience à utiliser, ces niveaux d'audience seront utilisés de manière cyclique (le paramètre « cycle » définit la durée en secondes de ces multiples niveaux d'audience), et entre parenthèses cryptimage vous informe encore des mots de 11 bits correspondant à ces niveaux d'audience du « multicode ».

Le « multicode » fut utilisé par canal plus à partir de 1987 pour contrer les décodeurs pirates, cette contre-mesure s'étant avérée au final inefficace elle fut rapidement retirée et la chaîne est revenue au « monocode », c'est à dire un seul niveau d'audience (un seul mot de 11 bits) lors du cryptage.

- Retards 1 et 2



Ces 2 curseurs permettent de spécifier les 2 types de retards en pourcentage de décalage de pixels (le retard « 0 » consistant à ne retarder aucune ligne), en règle générale vous n'aurez pas besoin de modifier ces 2 retards, les valeurs par défaut (1,67 % et 3,34%) permettant une bonne simulation du discret11, toutefois ceux qui ont des décodeurs non-officiels pourront modifier ces valeurs si leur matériel était mal étalonné en terme de décalage (lignes à retards électroniques éloignées des valeurs utilisées par le décodeur officiel).



Une case à cocher « retards par défaut » permet à tout moment de faire revenir les curseurs des retards aux réglages par défaut.

☐ Retards nuls

Cette case permet de mettre les 3 retards à zéro, permettant d'avoir une image toujours en clair, sauf les lignes 310 et 622 qui seront en mode « discret11 », cela permet à un décodeur matériel d'agir comme un codeur lorsqu'on lui donnera ce type de vidéo, il cryptera l'image au lieu de la décoder quand il verra les lignes 310 et 622 clignoter en mode « discret11 » .

- Bordure masquée

☐ Bordure masquée

Cette option permet de masquer les segments noirs de la bordure verticale gauche de l'image par des pixels de couleur prélevés plus loin dans la ligne en cours de cryptage, de manière à empêcher certains décodeurs pirates de fonctionner (notamment le décodeur « radio-plans » qui utilise la détection du noir en début de ligne pour en déduire le retard appliqué).

Cette mesure anti-piratage fut utilisée par canal plus dès 1985.

A noter que si cette case est cochée alors que le mode « décodage » est sélectionné alors cela aura pour effet de masquer aussi la bordure verticale droite .

- Traiter le son, désactiver le son

☒ Traiter le son ☐ Désactiver le son

La case « traiter le son » indique s'il faut coder/décoder le son de la vidéo, si cette case est cochée alors cryptimage cryptera/décryptera le son (en fonction du mode « codage/décodage » sélectionné).

La case « désactiver le son » fera en sorte que la vidéo générée ne contiendra aucune piste son (la vidéo sera muette).

- Seuil du blanc



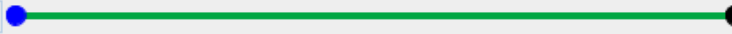
Ce curseur permet de régler le seuil de détection des lignes TV 310 et 622, en indiquant la valeur RVB à partir de laquelle le système considère ces lignes comme du blanc.

Ce réglage est utile lorsqu'on souhaite décoder un signal discret 11 issu de cassettes VHS en mauvais état, les lignes TV 310 et 622 pouvant alors être en mauvais état, en présentant une couleur bleutée plutôt que blanche, mettre le curseur à des valeurs inférieures à 80 permet d'améliorer le décodage.

En cochant la case « retards nuls » vous pourrez recréer une vidéo discret11 de ces cassettes VHS à l'identique, avec les lignes TV 310 et 622 restaurées, qui auront alors une couleur blanche parfaite (valeur RVB de 255).

- Démarrer à la trame

Démarrer à la trame :



Une vidéo se compose de trames, avec cryptimage vous avez la possibilité de dire au codeur/décodeur à partir de quelle trame il doit commencer et terminer son travail, il suffit de faire glisser les 2 marqueurs sur le numéro de trame à partir duquel le cryptage/décryptage doit commencer et se terminer.

- Code clavier décodeur

Code clavier décodeur

☒ A1 ☒ A2 ☒ A3 ☒ A4 ☒ A5 ☒ A6

Numéro de série:

Code clavier:

Cette section de l'interface est utile pour ceux qui possèdent un décodeur officiel discret 11 (celui fourni par canal plus aux abonnés entre 1984 et 1995), il vous permet de trouver le code clavier.

Ce code clavier est calculé en fonction du numéro de série de votre décodeur (qu'il faudra entrer dans le champ « numéro de série »), puis selon les autorisations de niveau d'audience (cases à cocher A1 à A6) et enfin en fonction du mot de 16 bits défini dans la section « options discret11 » .

d. Options nagravision syster

a. Options de codage

Options nagravision syster

☒ Coder ☐ Décoder

Options de codage

☒ Coder automatiquement table primaire 1 ▼

☐ Coder avec un fichier de paramètres Ouvrir

☐ Tatouer la ligne 288 ☐ Changer l'offset et l'incrément à chaque demi-trame

☒ Traiter le son ☐ Désactiver le son

Démarrer à la trame :

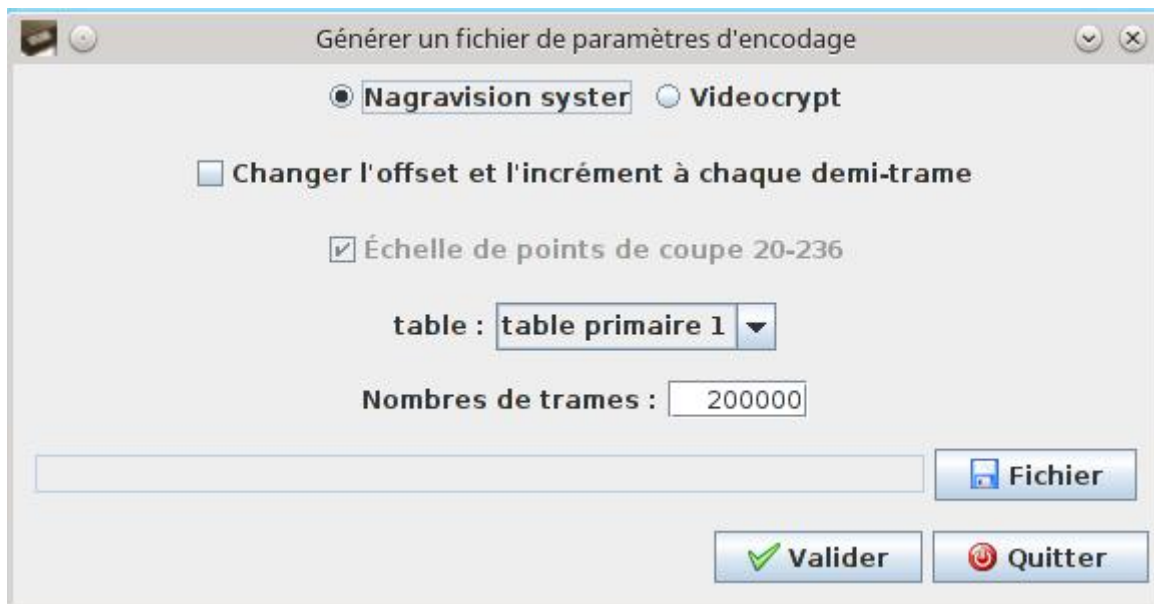
1 (00:00:00) 59 (00:00:02)

Ce panneau apparaît lorsque la liste déroulante « système » est positionnée sur « nagravision syster » et que le bouton « coder » est sélectionné .

Ces options vous permettront de créer des fichiers vidéos et des photos cryptées en nagravision syster.

Il existe deux manières de coder en nagravision syster via 2 boutons dans cette interface :

- « **coder automatiquement** » en fonction d'une table primaire, le programme générera de manière aléatoire un offset et un incrément pour chaque demi-image du fichier vidéo.
- « **coder à l'aide d'un fichier d'encodage** » , c'est un fichier texte (portant l'extension « enc ») qui décrit pour chaque trame progressive le couple offset/incrément à utiliser pour les demi-images composant cette trame, ce fichier indique aussi quel type de table primaire à utiliser, un tel fichier peut se générer via le menu « outils, générer un fichier de paramètres d'encodage » :



pour que ce fichier d'encodage soit valide il faut qu'il possède un nombre de lignes au moins égal au nombre de trames progressives constituant la vidéo à crypter .

Il existe 2 types de table primaire sélectionnables :

- **table primaire 1** : utilisée par plusieurs chaînes du satellite et du câble, les chaînes en PAL, ainsi que par canal+ jusqu'en septembre 1997.
- **table primaire 2** : utilisée uniquement par canal+ de septembre 1997 jusqu'à l'extinction de la diffusion hertzienne analogique de canal+ en France fin 2010.

En plus de ces deux options de codage vous pouvez « tatouer » la ligne 288 (qui n'est pas cryptée) en cochant la case « **tatouer la ligne 288** » afin d'y placer à l'image sous forme de bits le type de table utilisé (codé sur 2 bits), l'offset et l'incrément (codés chacun sur 8 bits), chaque bit utilise 8 pixels à l'image, ce tatouage est placé en bas à gauche de l'image, sur les deux dernières lignes de l'image (numéros de ligne 575 et 576 sur une trame progressive 768x576 lignes) .

Ce tatouage vous permettra si la case est cochée d'avoir un décodage automatique par simple lecture de ce tatouage par cryptimage .

Enfin une case « **changer l'offset et l'incrément à chaque demi-image** » permet de faire varier l'offset-incrément à chaque demi-image, si décochée l'offset et l'incrément seront changés que toutes les 2 demi-images.

b. Options de décodage

Options nagravision syster

☐ Coder ☒ Décoder

Options de décodage

☒ Décoder avec un fichier de paramètres

☐ Décoder via le tatouage de la ligne 288

☐ Décoder via la corrélation de lignes ☐ Reverse decoding

☒ Traiter le son ☐ Désactiver le son

Démarrer à la trame :

Ce panneau apparaît lorsque la liste déroulante « système » est positionnée sur « nagravision syster » et que le bouton « décoder » est sélectionné .

Vous avez 3 façons de décoder du nagravision syster :

- « **décoder à l'aide d'un fichier de décodage** » : c'est un fichier texte décrivant quelle table primaire utiliser et quel couple offset/incrément utiliser pour chaque demi-image, un tel fichier porte l'extension « dec » **et est généré automatiquement** par cryptimage lorsqu'on crypte un fichier en nagravision syster.

- « **décoder via le tatouage de la ligne 288** » : le décodage se fera automatiquement si un tel tatouage est présent sur la ligne 288 de chaque demi-image, si vous avez pensé à cocher la case « tatouer la ligne 288 » lors de l'étape de codage alors vous pourrez utiliser cette option de décodage.

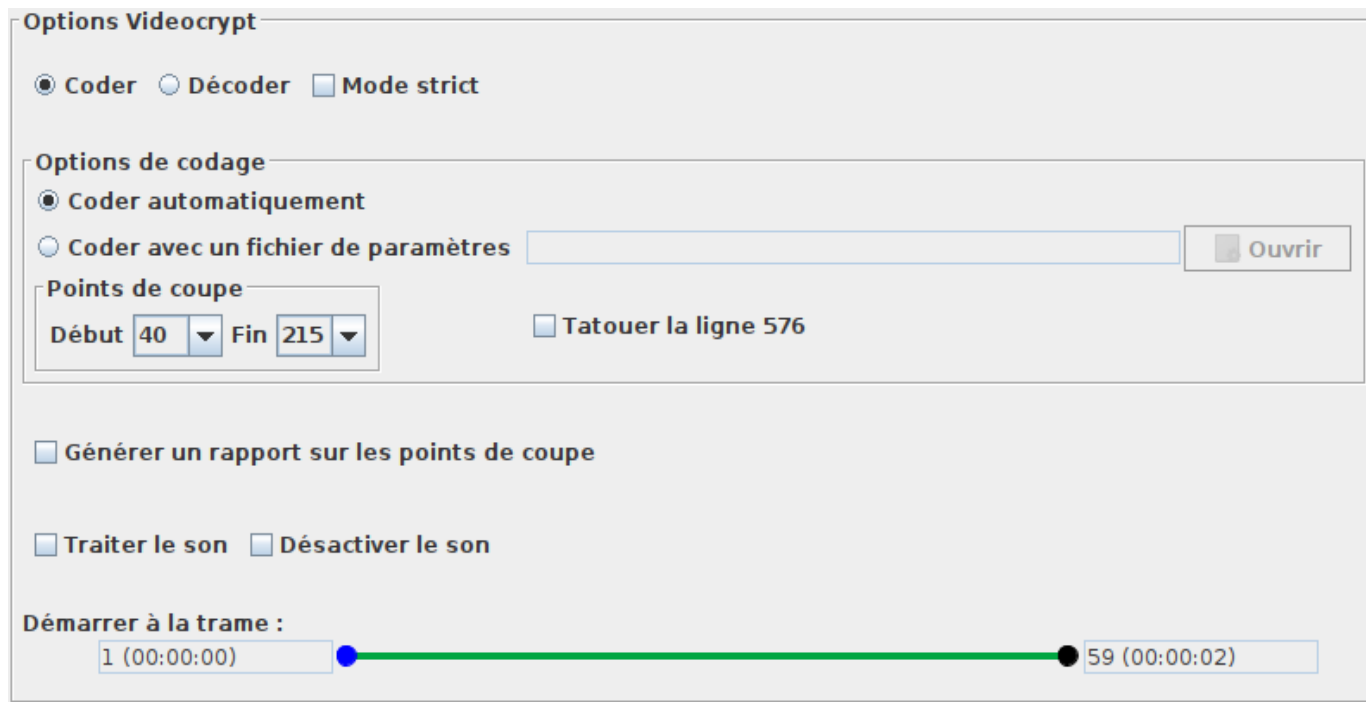
- « **décoder via la corrélation de lignes** » : le décodage se fera en testant les 32768 possibilités de décryptage et en déduira la bonne combinaison offset/incrément, si vous choisissez cette option il faudra alors indiquer via la liste déroulante quelle table primaire utiliser, cette méthode de décodage par corrélation de lignes est assez lente mais donne d'assez bons résultats .

À noter que comme pour le discret11 vous disposez des mêmes options pour la gestion du son (cases à cocher « traiter le son » et « désactiver le son ») et celle du choix du début de la trame pour l'activation du codeur/décodeur (curseur « démarrer à la trame »).

À des fins de débogage une case à cocher « reverse decoding » permet de décoder une vidéo qui a été « codée » par un décodeur syster (au moyen du logiciel SDR hacktv, via l'envoi d'informations VBI pour forcer un décodeur syster à s'activer et à décoder une vidéo en clair, permettant d'obtenir une vidéo cryptée en syster à « l' envers »).

e. Options videocrypt

a. Options de codage



Options Videocrypt

☒ Coder ☐ Décoder ☐ Mode strict

Options de codage

☒ Coder automatiquement

☐ Coder avec un fichier de paramètres

Points de coupe

Début Fin

☐ Tatouer la ligne 576

☐ Générer un rapport sur les points de coupe

☐ Traiter le son ☐ Désactiver le son

Démarrer à la trame :

Ce panneau apparaît lorsque la liste déroulante « système » est positionnée sur «videocrypt » et que le bouton « coder » est sélectionné .

Il existe deux manières de coder via 2 boutons dans cette interface :

- « **coder automatiquement** » le programme générera de manière aléatoire les points de coupe.
- « **coder à l'aide d'un fichier d'encodage** », c'est un fichier texte (portant l'extension «vid») qui contient des valeurs (« seed ») destinées à initialiser le générateur de valeurs pseudo-aléatoires qui permettront pour chaque image de générer des points de coupe. Un tel fichier peut se générer via le menu « outils , générer un fichier de paramètres d'encodage ». Cette option permet d'utiliser tout le temps les mêmes points de coupe, utile si on veut que tous les fichiers utilisent le même modèle pour les points de coupe.

Une liste déroulante «**points de coupe**» permet de restreindre les points de coupe à un intervalle de son choix, les valeurs par défaut étant « 40-215 » afin que le rendu soit proche de celui des chaînes de TV de l'époque qui utilisaient le videocrypt.

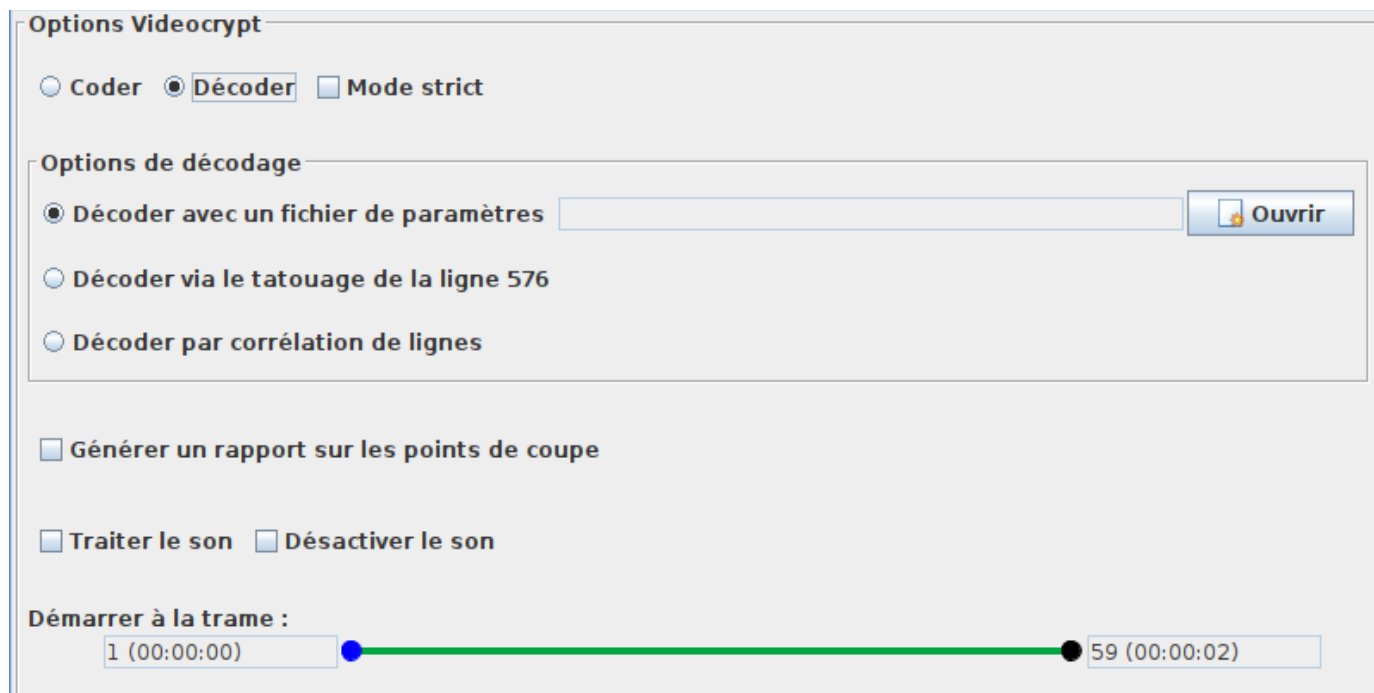
Une case à cocher « **Tatouer la ligne 576** » permet de tatouer la dernière ligne de l'image afin d'y placer l'échelle de point de coupe et la valeur « seed » permettant d'initialiser le générateur de valeurs pseudo-aléatoires, en vue d'un décodage automatique.

La case à cocher « mode strict » permet de reproduire les marges droite et gauche particulière du videocrypt.

Vous avez enfin la possibilité de générer un rapport texte au format CSV décrivant pour chaque ligne de l'image les points de coupe qui ont été choisis, le fichier texte pouvant être très volumineux il sera découpé en plusieurs fichiers toutes les 113 images ($113 \times 576 = 65088$ lignes), car certaines

versions de tableur ne peuvent gérer que 65536 lignes au maximum.

b. Options de décodage



Options Videocrypt

☐ Coder ☒ Décoder ☐ Mode strict

Options de décodage

☒ Décoder avec un fichier de paramètres

☐ Décoder via le tatouage de la ligne 576

☐ Décoder par corrélation de lignes

☐ Générer un rapport sur les points de coupe

☐ Traiter le son ☐ Désactiver le son

Démarrer à la trame :

1 (00:00:00) 59 (00:00:02)

Ce panneau apparaît lorsque la liste déroulante « système » est positionnée sur « videocrypt » et que le bouton « décoder » est sélectionné .

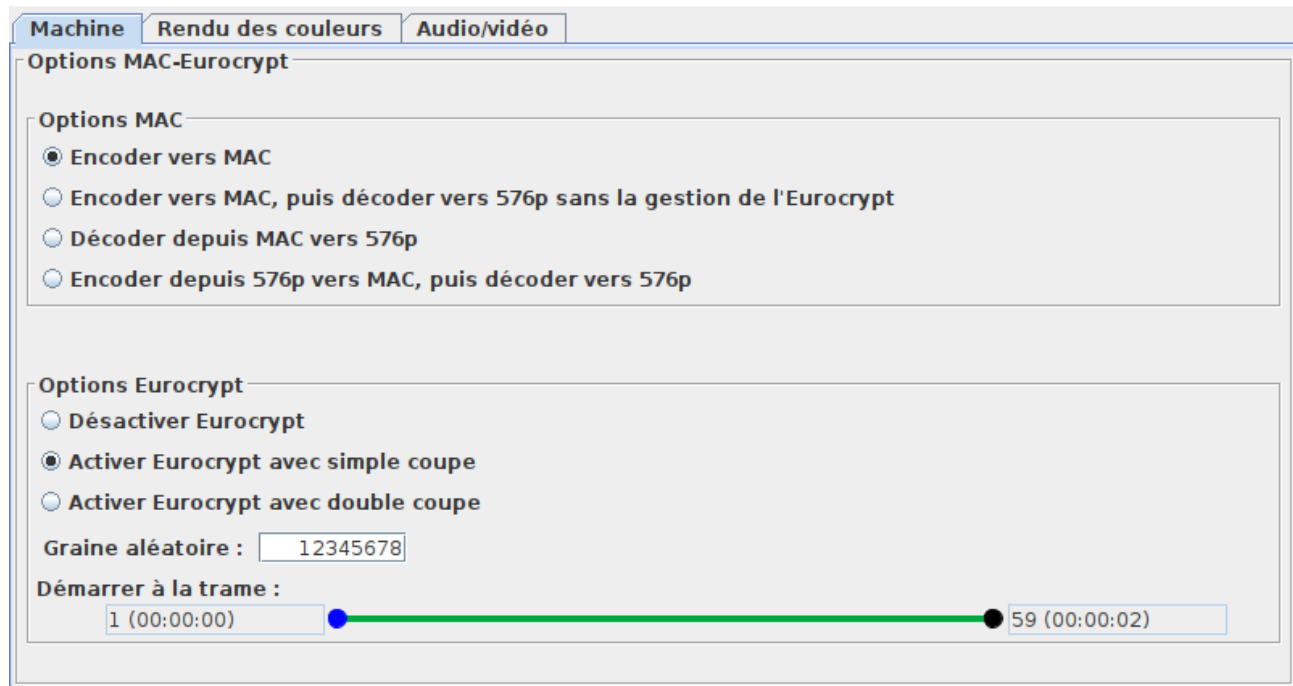
Vous avez 3 façons de décoder :

- « **décoder à l'aide d'un fichier de paramètres** » : c'est un fichier portant l'extension « vid » et est généré automatiquement par cryptimage lorsqu'on crypte un fichier en videocrypt.
- « **décoder via le tatouage de la ligne 1** » : permet un décodage automatique par lecture du tatouage sur la première ligne de l'image, si l'option de tatouage avait été choisie lors de l'étape du codage.
- « **décoder via la corrélation de lignes** » : le décodage se fera automatiquement via un algorithme spécial de corrélation de ligne qui recherchera le point de coupe le plus probable. Cet algorithme est très lent (3 secondes par image).

À noter que comme pour le discret11 vous disposez des mêmes options pour la gestion du son (cases à cocher « traiter le son » et « désactiver le son ») et celle du choix du début de la trame pour l'activation du codeur/décodeur (curseur « démarrer à la trame »).

f. Options MAC-Eurocrypt

L'option MAC-Eurocrypt permet d'encoder les images au format MAC (Multiplexed of Analog Components), où le son, la chroma et la luma sont transmis de manière séquentielle. Optionnellement un mode de cryptage « Eurocrypt » peut être activé.



- « **Encoder vers MAC** » avec option « **Désactiver Eurocrypt** » : les 192 premiers pixels de l'image contiendront le son au format numérique, les 384 suivants la partie chroma de l'image, avec la partie V ($R - Y$) sur une ligne, et sur la suivante la partie U ($B - Y$), et enfin la luma (Y) occupe les 768 pixels restants de l'image.

L'image en sortie aura donc un format de 1344 x 576 pixels.

- « **Encoder vers MAC** » avec option « **Activer Eurocrypt avec simple coupe** » : un encodage vers le format MAC est effectué, puis la partie chroma subit une rotation « cut and rotate », tous les pixels de la chroma à gauche du point de coupe sont déplacés après le dernier pixel de la zone luma.

- « **Encoder vers MAC** » avec option « **Activer Eurocrypt avec double coupe** » : un encodage vers le format MAC est effectué, puis la partie chroma subit une rotation « cut and rotate », et la partie luma subit aussi une rotation « cut and rotate ».

- « **Encoder vers MAC, puis décoder vers 576p sans la gestion de l'Eurocrypt** » avec option « **Désactiver Eurocrypt** » : un encodage vers le format MAC est effectué, puis un décodage vers le format 576p est effectué dans la foulée, sans se préoccuper de traiter un éventuel cryptage Eurocrypt, l'objectif de cette option étant de simuler le rendu d'un signal MAC crypté sur un terminal satellite/câble où aucun abonnement n'a été souscrit.

- « **Décoder depuis MAC vers 576p** » : cette option permet de retrouver l'image d'origine 768 x 576 pixels à partir d'une image encodée en MAC 1344 x 576 pixels, combinée aux options Eurocrypt elle permet en plus de décoder aussi l'Eurocrypt.

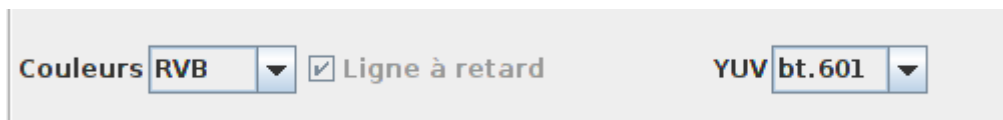
- « **Encoder depuis 576p vers MAC, puis décoder vers 576p** » : cette option permet de retrouver l'image en clair 768 x 576 pixels à partir d'une image embrouillée 768 x 576 pixels.

- « **Graine aléatoire** » : représente le nombre utilisé pour initialiser le générateur de valeurs pseudo-aléatoires, qui sert à créer les points de coupe pour le codage et décodage Eurocrypt.

g. Options transcode

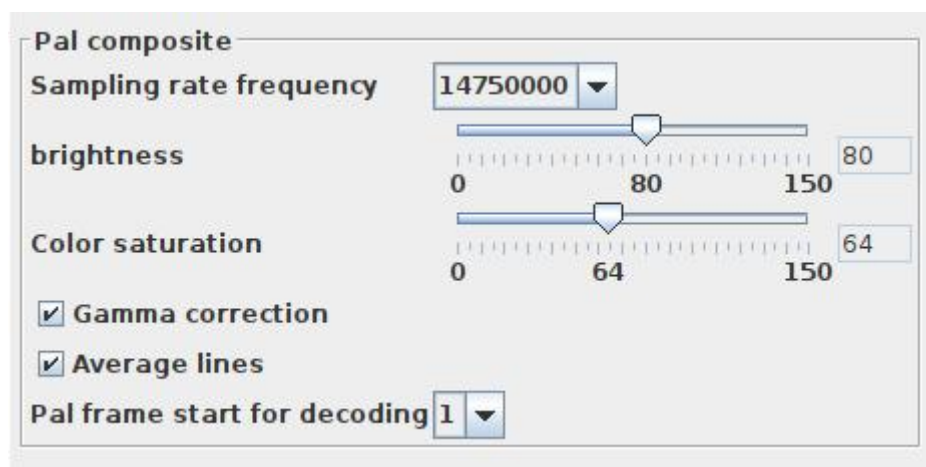
L'option transcode permet de convertir les images sans les crypter/décrypter, utile pour tester les modes PAL/Secam.

h. Rendu des couleurs



Un onglet « rendu des couleurs » permet de choisir le rendu de couleur qu'auront les fichiers générés par cryptimage.

- **RVB** : les couleurs ne seront pas modifiées, elles seront identiques au fichier source.
- **Pal** : les couleurs subiront une transformation en tenant compte des spécificités du standard Pal, notamment des inversions de phase, les composantes U et V seront moyennées par groupe de 2 lignes si la case « ligne à retard » est cochée. Ce mode n'est pas actif pour le discret11.
- **Pal composite** : version beaucoup plus réaliste du rendu pal, avec un panneau de commande dédié :



ce mode se décompose en 3 variantes :

- **encode et decode** : produit une image couleurs PAL.
- **encode seulement** : produit une image noir et blanc comportant l'information de chrominance PAL sous forme de motifs en points et en hachures.
- **decode seulement** : produit une image en couleurs PAL à partir d'une image noir et blanc comportant la chrominance codée sous forme de motifs en points et en hachures (image noir et blanc générée par le mode « encode seulement »).

- **Secam** : les couleurs subiront une transformation, les composantes U et V de chaque ligne seront déterminées en fonction de la ligne précédente, en cas de rupture d'alternance « V-U » (rouge, bleu) les lignes passeront en noir et blanc ou seront fixées au rouge, bleu ou violet selon le contexte.

Une liste déroulante « YUV » permet de spécifier la matrice de couleurs à utiliser lors d'une conversion RVB - YUV, « bt.601 » pour les fichiers à définition standard, « bt.709 » pour les fichiers haute définition, et « spécial » quand ces deux réglages ne donnent pas satisfaction.

Compte tenu de la complexité des traitements en pal et secam (conversion RVB-YUV, rotation de phase) la vitesse de génération des fichiers sera plus lente dans ces modes de rendu par rapport au RVB.

i. Options audio/vidéo

Options audio/vidéo

☐ 720x576 ☒ 768x576 ☐ 944x626 Audio ☐ Mode lecteur ☐ Horodatage

Options 4/3

☒ Letterbox ☐ Pan and scan ☐ Étirer

Décalage X Décalage Y ☐ Joindre

Codec Bitrate 1 20000 10836

Extension Nb frames 1 59 59 (00:00:02)

Ces options concernent le fichier vidéo généré, vous pouvez choisir la résolution du fichier (uniquement si vous avez coché la case « respect de la norme »), le codec vidéo de compression, le conteneur du fichier (son extension), le codec audio et son bitrate, la fréquence d'échantillonnage (44100 ou 48000 Hz) , le taux de compression vidéo (bitrate), le nombre de trames sur lesquelles il faut créer ce fichier (permet de limiter votre fichier à une certaine durée indiquée entre parenthèses).

En outre vous avez la possibilité d'horodater le nom du fichier vidéo, la date, l'heure, les options discret11, le code clavier seront ajoutés automatiquement au nom du fichier vidéo créée.

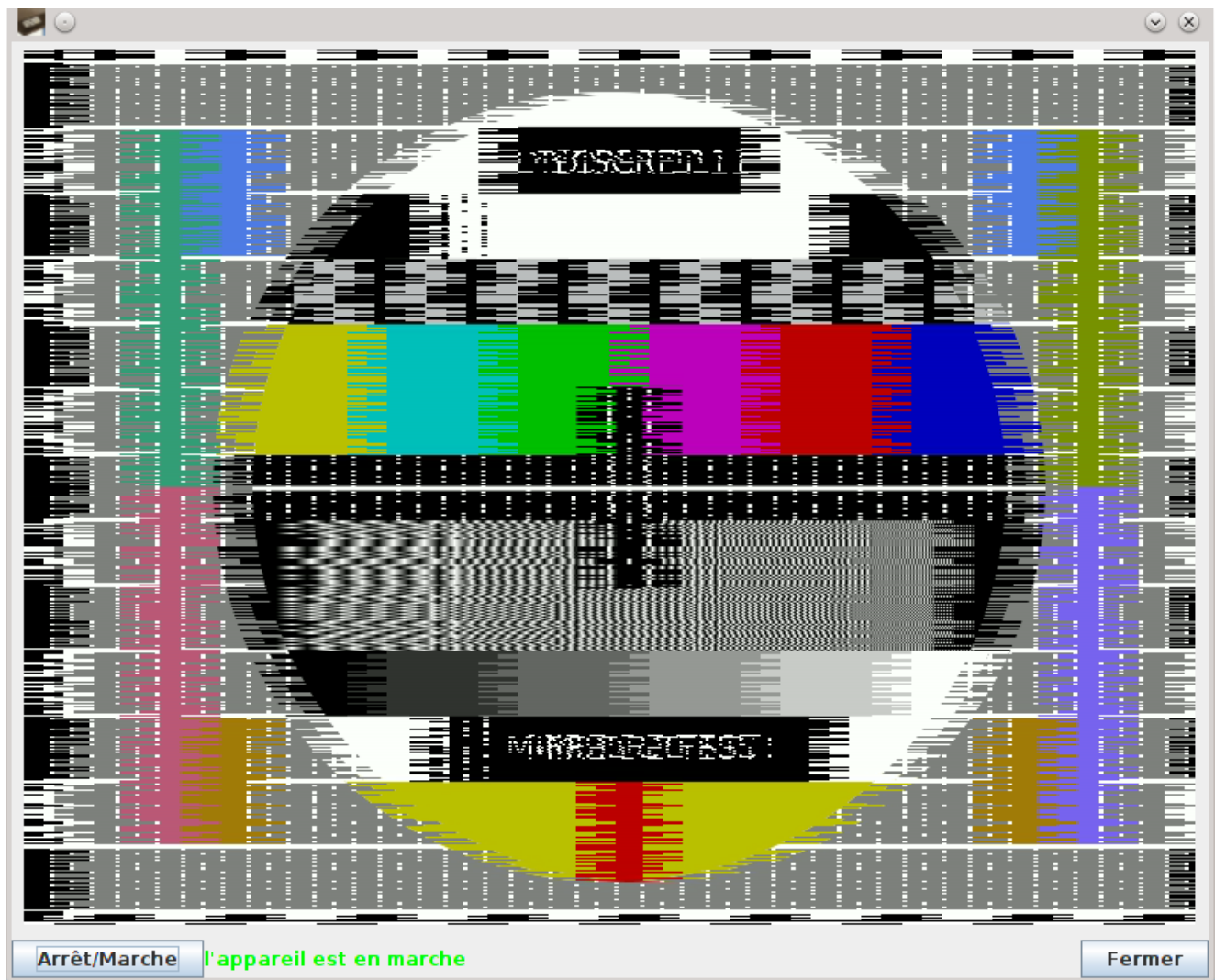
Une option «pan and scan » permet de recadrer en mode 4/3 sans bandes noires horizontales une image en entrée, une option « Étirer » permet de redimensionner au format 4/3 en étirant horizontalement et verticalement les pixels, et enfin une option « letterbox » qui redimensionne au format 4/3 en préservant le ratio de la vidéo d'origine, en ajoutant si nécessaire des bandes noires,

tous ces modes 4/3 ne fonctionnent qu'en mode « cryptage ».

Vous avez la possibilité de décaler l'image pixel par pixel, sur le plan horizontal et vertical, au moyen des options « décalage X » et « décalage Y ».

Une case à cocher « mode lecteur » vous permet de désactiver la création du fichier vidéo sur le disque, cela ouvrira une nouvelle fenêtre qui fera office de lecteur vidéo afin d'avoir un aperçu visuel du codage/décodage, dans ce mode aucun son n'est émis, il s'agit uniquement d'un aperçu visuel, un bouton « on/off » permet de désactiver/activer le codeur/décodeur.

Une case à cocher « joindre » permet de générer un fichier vidéo avec à gauche l'image d'origine et à droite l'image transformée.



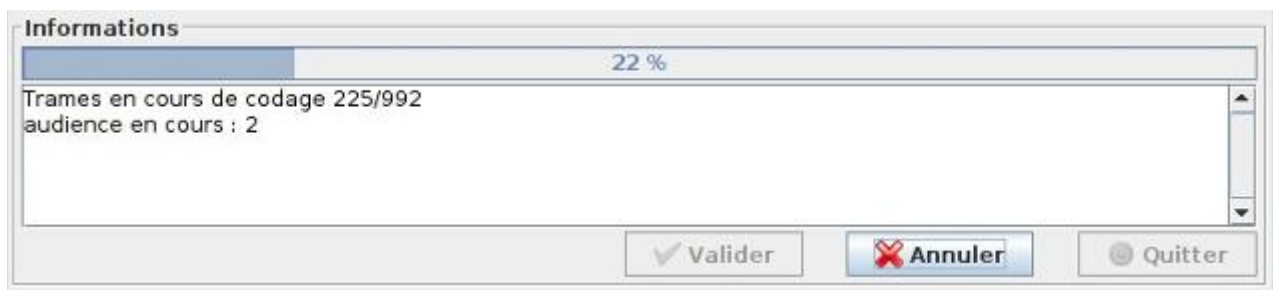
fenêtre du mode lecteur

j. Informations



Cette partie de l'interface vous permet de suivre la progression du traitement du fichier vidéo, via une barre de progression avec un pourcentage, une zone de texte pour afficher les messages d'information et les éventuels messages d'erreurs.

Le bouton « valider » permet de lancer le traitement du fichier vidéo, le bouton « annuler » d'annuler les opérations, le bouton « quitter » de fermer cryptimage.



informations de progression d'un cryptage d'un fichier vidéo

À la fin de la génération du fichier un rapport texte sera généré dans le répertoire de travail, il contiendra les différents paramètres discret11 qui ont servi à la génération de ce fichier.

Enfin la plupart des options de l'interface sont sauvegardées dans un fichier de configuration (cryptimage.conf) stocké dans le répertoire de l'utilisateur (« documents and settings » sous windows, dossier « home » sous linux) dans un sous répertoire « cryptimage », ceci afin de recharger automatiquement ces choix lors du prochain lancement de cryptimage.

8. Utiliser cryptimage avec un décodeur matériel

Cryptimage peut donc servir à générer des fichiers vidéos en vu de tester un véritable décodeur discret11, tel que celui fournit à l'époque par canal plus.

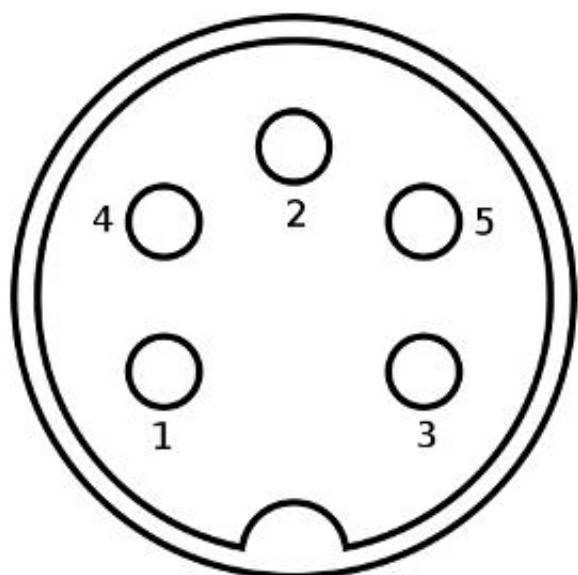


le décodeur officiel discret11

a. Fixer un numéro de série dans la rom

La première étape consiste à fixer un numéro de série personnalisé dans la puce rom du décodeur, afin de pouvoir ensuite générer plus tard un code clavier valide avec cryptimage.

Pour cela nous allons utiliser la prise de type « Din 5 broches » se situant à l'arrière du décodeur, l'opération consiste à relier la broche 1 à la masse de blindage :



affectation des broches :

1 : programmation du numéro de série

2 : masse audio

3 : sortie vidéo

4 : sortie son

5 : masse audio

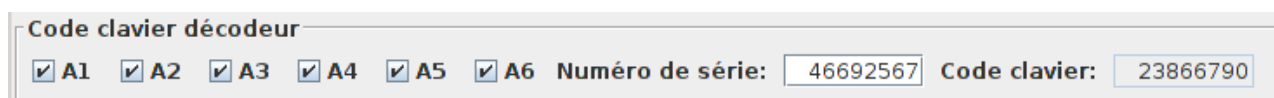
prise DIN vue de face à l'arrière du décodeur

Une fois la broche 1 reliée à la masse de blindage nous pouvons alors utiliser le pavé numérique en façade du décodeur pour entrer un numéro de série dans la rom du décodeur :

- tapez 4 fois de suite la touche « ENT »
- entrez les 4 premiers chiffres du numéro de série
- tapez une fois la touche « MEMO »
- tapez 2 fois de suite la touche « ENT »
- entrez les 4 derniers chiffres du numéro de série
- tapez une fois la touche « MEMO »

le numéro à 8 chiffres sera alors mémorisé dans la puce rom du décodeur (exemple : 4669 2567), retirez ensuite le pontage que vous avez fait entre la broche 1 et la masse de blindage de la prise DIN pour terminer l'opération.

Dans cryptimage entrez le numéro de série afin de connaître le code clavier :



ici nous voyons que le code clavier pour le numéro de série « 46692567 » est « 23866790 », le mot de 16 bits entré dans l'interface étant 18270, le niveau d'audience 1 avec toutes les cases A1 à A6 cochées.

Pour entrer le code clavier dans le décodeur :

- appuyez sur la touche ENT, le voyant jaune doit clignoter ensuite
- tapez les 8 chiffres du code clavier
- appuyez sur la touche MEMO pour valider, le voyant jaune doit s'éteindre, le voyant vert s'allumera ensuite pour décoder tout signal vidéo crypté.

b. Injecter un fichier vidéo à votre décodeur

Maintenant que nous avons correctement configuré notre décodeur officiel (numéro de série et code clavier) nous pouvons tester notre décodeur en lui envoyant des fichiers cryptés avec cryptimage.

La méthode consiste à déposer notre fichier vidéo crypté sur une clé USB, puis d'utiliser un adaptateur TNT équipé d'une prise USB (fonction magnétoscope numérique) et d'une sortie vidéo composite et d'une sortie audio (connexion RCA ou péritel), puis à relier cet adaptateur TNT à l'entrée vidéo composite du décodeur ainsi que son entrée audio (via un adaptateur entrée RCA vidéo composite → péritel) :



adaptateur TNT équipé d'un port USB en façade



*câble péritel permettant
d'avoir les entrées et sorties
au format RCA*

La lecture des fichiers se fera alors via l'adaptateur TNT qui lira la clé USB contenant nos fichiers cryptés, le décodeur recevra sous format vidéo composite ce fichier grâce aux sorties vidéo composite et audio de notre adaptateur TNT, il faudra ensuite relier la sortie vidéo/audio du décodeur à un téléviseur.

Une méthode alternative consiste à utiliser un modulateur RF relié à la sortie vidéo composite (ainsi que la sortie audio) de votre adaptateur TNT, puis de relier le modulateur RF à l'entrée antenne de votre téléviseur, puis enfin de relier le décodeur à l'entrée péritel du téléviseur, cette méthode a l'avantage de reconstituer le montage d'époque tel qu'il avait été prévu pour le décodeur officiel (image prélevée par le décodeur depuis le téléviseur via la prise péritel) .



modulateur RF acceptant en entrée du RCA et une péritel

Il est conseillé d'ajouter un transcodeur PAL vers SECAM avant d'injecter le signal vidéo au décodeur ou au téléviseur, car les lignes à retards analogiques du décodeur officiel discret11 s'accommodent mal d'un signal PAL (couleurs non fidèles).

Un résumé du montage permettant d'injecter de la vidéo cryptée à notre décodeur :

- Cryptimage → clé USB → adaptateur TNT → décodeur officiel → téléviseur

ou

- Cryptimage → clé USB → adaptateur TNT → modulateur RF → téléviseur → décodeur officiel

9. Conseils

Afin d'obtenir une bonne qualité d'image lors du décryptage d'un fichier vidéo (que ce soit avec cryptimage ou avec un décodeur officiel) il est conseillé d'utiliser un taux de compression vidéo le moins destructeur possible lors de l'étape du cryptage du fichier vidéo,

car le principe du décryptage consiste à déplacer des pixels, ce qui peut accentuer les défauts de compression du fichier initial (artefacts de compression, défauts de couleur), utiliser un bitrate vidéo égal ou supérieur à 10000 permet de limiter les pertes. Un décodage d'un fichier compressé avec le codec h264 ou divx ou mpeg2 fera apparaître inévitablement des parasites, des artefacts de compression désordonnés un peu partout dans l'image, surtout si le bitrate était trop bas lors de l'étape de cryptage du fichier.

La solution pour éviter tous ces problèmes au décodage est d'utiliser **lors de l'étape du cryptage** le codec de compression vidéo sans pertes **huffyuv** dans la liste déroulante de l'interface (ou bien

FFV1 qui peut aussi faire l'affaire), ce type de codec permet d'obtenir la meilleure qualité possible, l'image décodée sera **exactement identique au bit près** à l'image originale, le seul inconvénient des codecs huffyuv et FFV1 est la grande taille du fichier généré (néanmoins il est possible de le « zipper » en vu de réduire la taille du fichier pour le stocker de manière permanente sur un support de type DVD-R).

Une autre alternative consiste à sélectionner le codec « h264 v2 » qui a la particularité de coder les couleurs sur un espace 4:4:4 YUV au lieu du traditionnel 4:2:0 (meilleure précision des couleurs), les pertes seront moins élevées, l'inconvénient c'est que peu d'adaptateurs TNT sauront lire les fichiers codés sur un espace de couleurs 4:4:4, si vous voulez utiliser un adaptateur TNT il faudra probablement utiliser le codec « h264 », « mpeg2 » ou « divx » dans la liste déroulante des codecs pour la compatibilité de lecture.

Sachez qu'il est préférable de ne pas utiliser en entrée des fichiers vidéos bruts « ts », ou « m2t » issus d'un enregistrement de la TNT, ces fichiers n'ont pas d'index vidéo et poseront quelques problèmes à cryptimage, il faut au préalable traiter ces fichiers avec des logiciels comme handbrake (gratuit) afin d'avoir un véritable fichier vidéo indexé dans un conteneur « avi », « mp4 » ou « mkv ».

Concernant le choix du codec audio vous aurez la meilleure qualité possible en choisissant « wav » dans la liste déroulante des codecs audio, un bon compromis consiste aussi à utiliser « mp3 192 kbs » ou « mp3 320 kbs », pour la fréquence d'échantillonnage le 48000 Hz donne évidemment la meilleure qualité, dans tous les cas ne descendez jamais en dessous de 160 kbs si vous utilisez le MP3 lors d'un cryptage de fichier, car la qualité du décodage audio sera particulièrement mauvaise si par exemple un taux de 96 kbs a été utilisé pour le codec MP3 lors de l'étape du cryptage du fichier.

Enfin si vous voulez faire décoder par cryptimage des cassettes VHS contenant un signal discret¹¹ ou nagravision systere alors la numérisation de ces cassettes devra être soignée, en utilisant une carte tuner ou d'acquisition vidéo permettant d'obtenir une géométrie parfaite de l'image (pas d'overscan, pas de décalage vertical des lignes d'un cran vers le haut ou vers le bas), numérisez en récupérant la trame impaire et paire et sans faire de désentrelacement, l'image doit être au format 720x576 ou 768x576, utilisez un codec vidéo peu ou pas destructeur avec un bon débit pour garantir une image propre et exploitable par cryptimage si vous utilisez la méthode de décodage par corrélation de lignes.

10. Bugs

Si cryptimage ne fonctionne plus correctement alors supprimez le fichier de configuration « cryptimage.conf » situé dans le répertoire de l'utilisateur (« documents and settings » sous windows, dossier « home » sous linux) dans un sous répertoire « cryptimage », cela permettra de repartir avec les réglages par défaut.