Cryptimage

user guide

## Contents

1. Introduction

Cryptimage is an open source software under the license GNU GPL v3 which purpose is to reproduce old analog TV encryption systems like "discret 11" (used between 1984 and 1995 by french TV network "canal plus") , "nagravision syster" (used between 1995 and 2010), "videocrypt" used by Sky TV and by several other broadcasters on astra satellites, and finally the MAC video standard associated with Eurocrypt encryption.

This software allows to encrypt a video file (image and sound) , and allows also a decryption of an encrypted file, by meeting the standard of discret11, nagravision syster, videocrypt and Eurocrypt.

Besides the ability to reproduce in a digital way these encryption systems, its second use is to allow the re-use of hardware descramblers by injecting to them an encrypted video file produced by cryptimage.

2. Definition of discret 11

The discret11 process is to encrypt the image by delaying each line by three values to choose from (0, 902 and 1804 milliseconds), delays are selected through an algorithm based on a pseudo-random sequence, the sound is rendered unintelligible by subjecting it to a spectrum inversion around the frequency 12800 Hz.
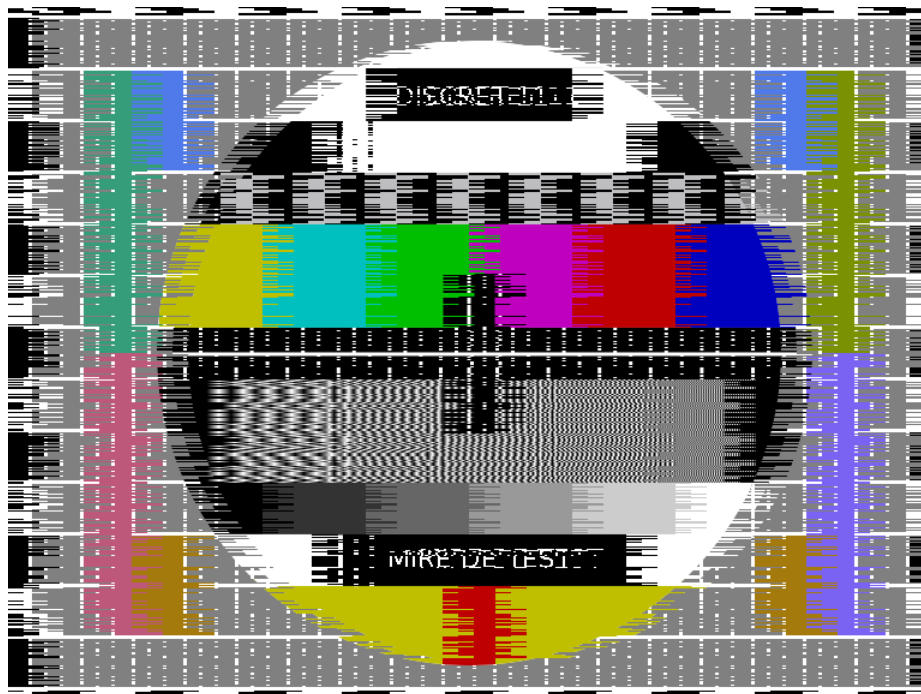
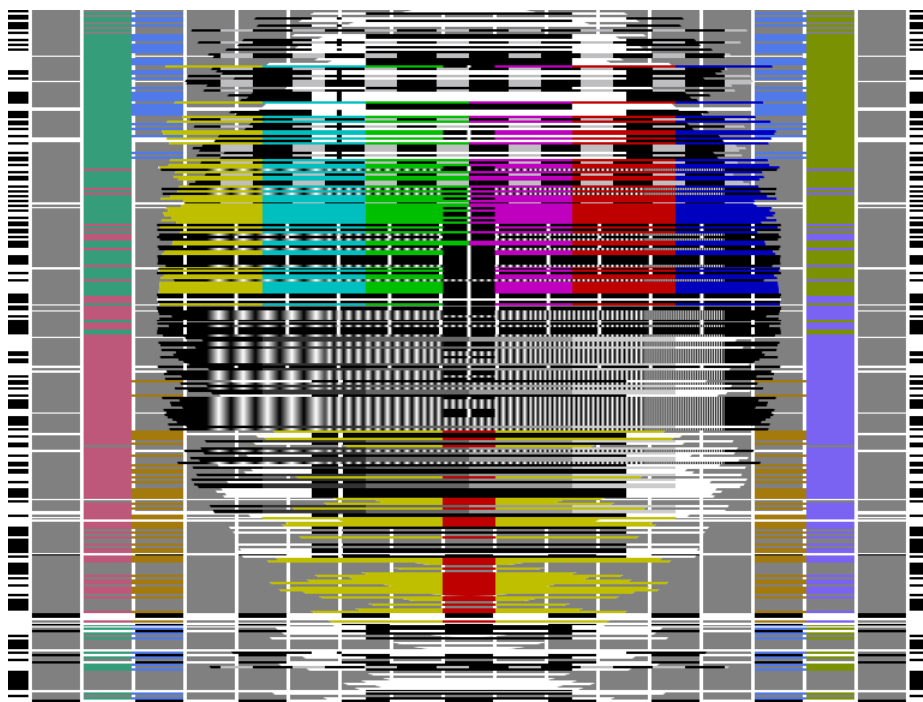*Discret11 encryption example, on a Philips PM5544 tv card*

3. Definition of nagravision syster

Nagravision syster (SYStème TERrestre) scrambles the image by permuting lines, a TV frame has 2 interlaced fields, each field has 288 lines and these lines are permuted (except line 288 which is not

permuted), then the first 32 lines of each encrypted field are shifted to the previous encrypted field, which give this pattern for an encrypted field :

- the first 255 lines are permuted

- the next 32 lines (256 to 287) are permuted but belong to the next field

- the last line (288) is not permuted and belongs to the current field

in order to decrypt a TV frame we must reorder the lines in a specific way , by taking 32 lines of a field (lines 256 to 287), then the next 255 lines of the next field, and we regroup these lines (287) in a new field, the new order of these lines will be given by the use of an algorithm, which consists to select an offset and an increment, and to use a "primary table" which contains 256 values (0 to 31), this table is read 255 times in a circulary way, the start adress is given by the offset (values : 0 to 255) which an addition is made (increment, odd values between 1 and 127).
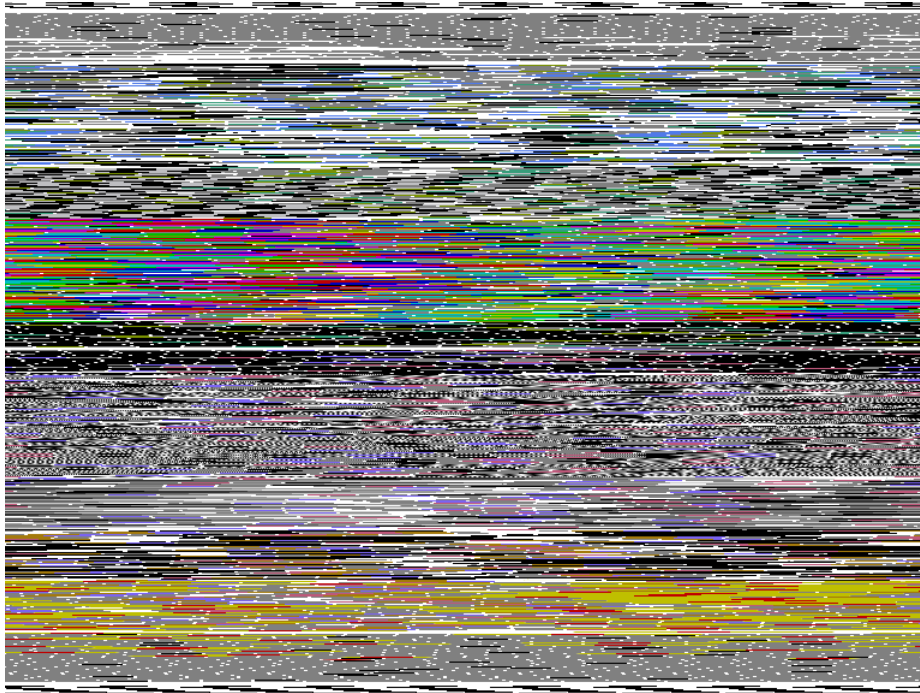

Nagravision syster encryption example on a Philips PM5544 test card

4. Definition of videocrypt

Videocrypt scrambles the image by using "cut and rotate" method. At each line a cut point (256 possibilities) is chosen, right part of the image goes to the left, left part goes to the right.

Sound is not encrypted, although at one time it was considered doing.

Videocrypt encryption example on a Philips PM5544 test card

5. Definition of MAC-Eurocrypt

MAC (Multiplexed Of Analog Components) is a video standard developed in the 80s, which consists of sequentially transmitting sound, then chroma and finally luma to each of the 576 lines of the image, unlike other standards colors (PAL/SECAM/NTSC) the chroma part is not mixed with the luma, which allows for much better quality.

For pay television, an encryption method is possible, with Eurocrypt, based on the "cut and rotate" principle similar to videocrypt, with two variants:

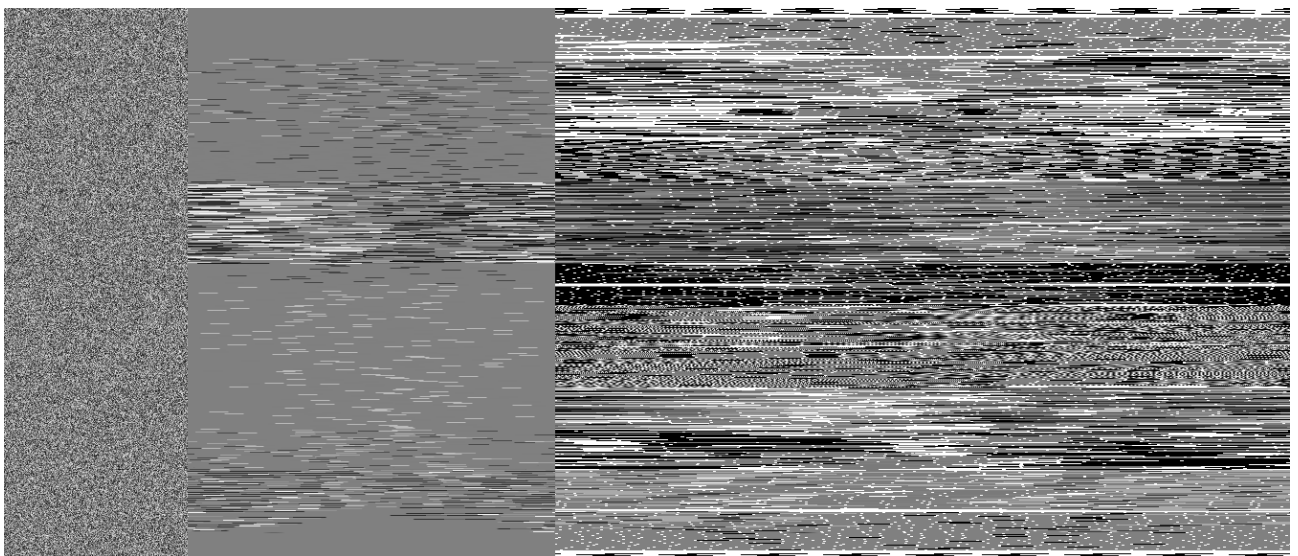- **single cut** where only the chroma part undergoes a cut point, with the luma part which is found in the middle of the 2 parts of the chroma having undergone a rotation,

- **double cut** where the chroma part and the luma part both undergo a "cut and rotate" operation.
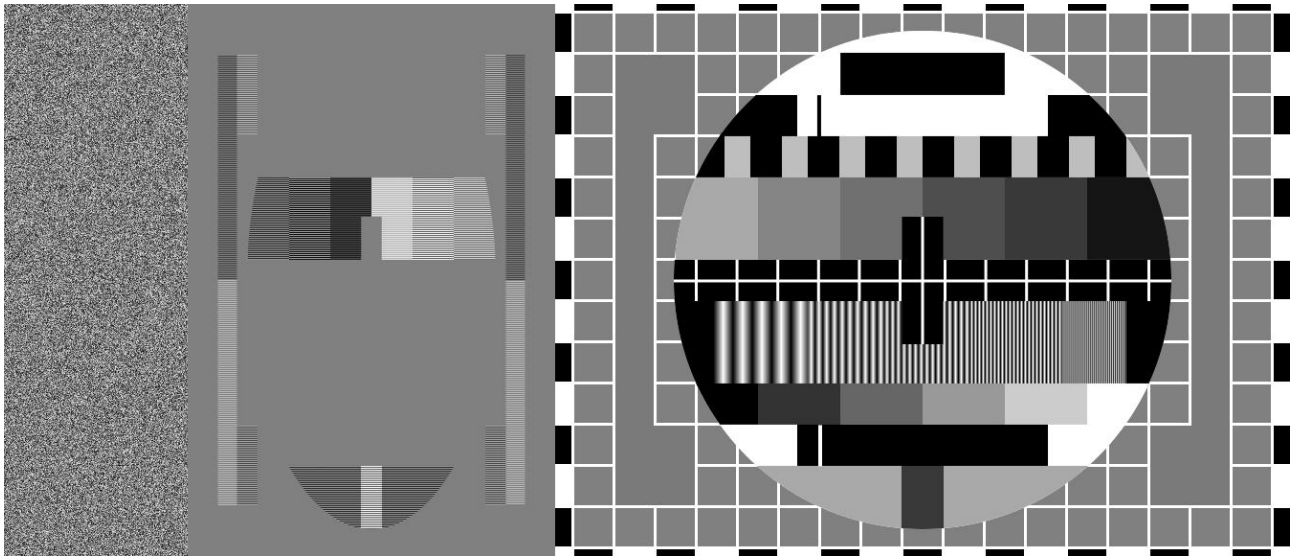
MAC encoding without Eurocrypt encryption
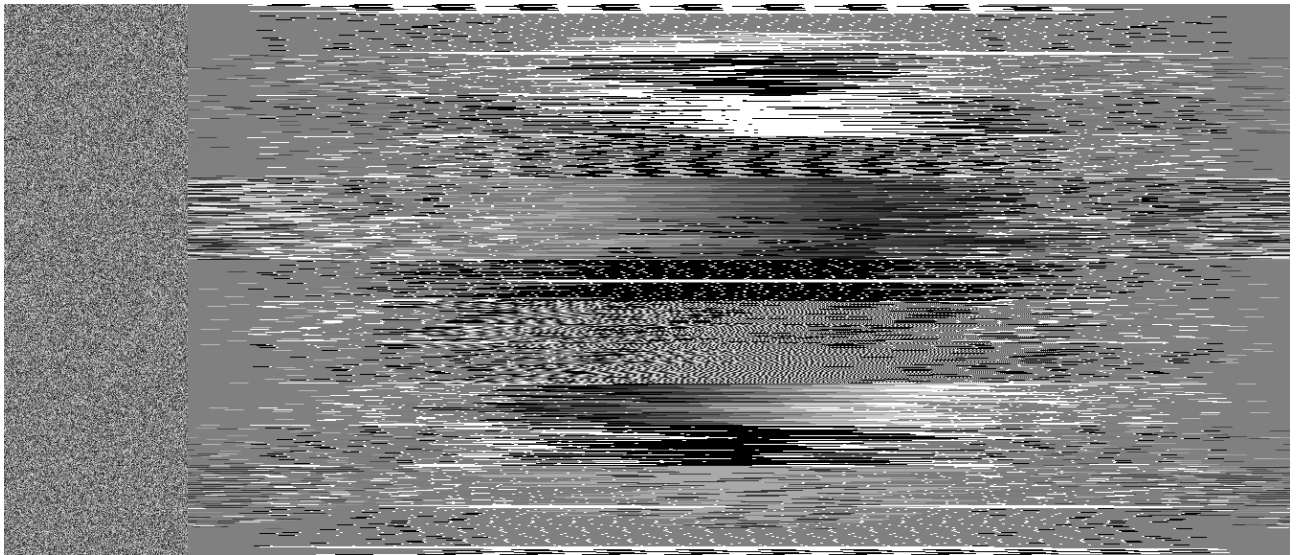
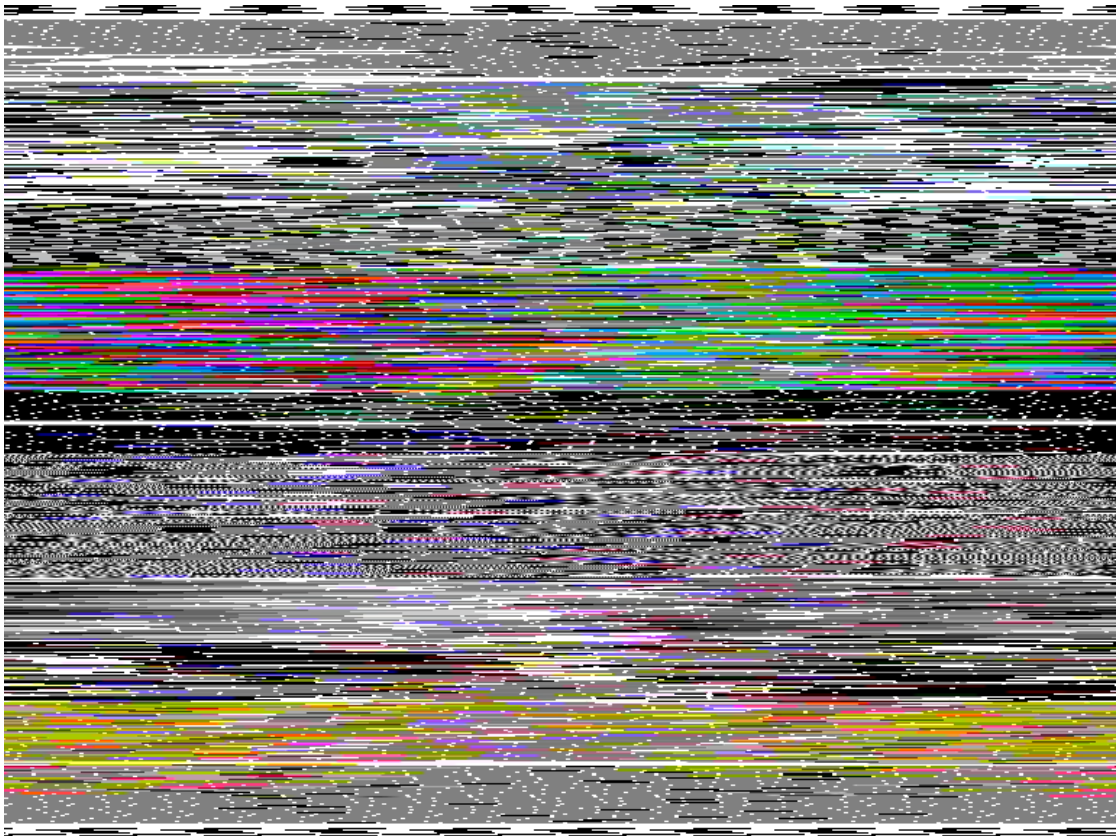*MAC encoding with Eurocrypt single cut encryption*

MAC encoding with Eurocrypt double cut encryption
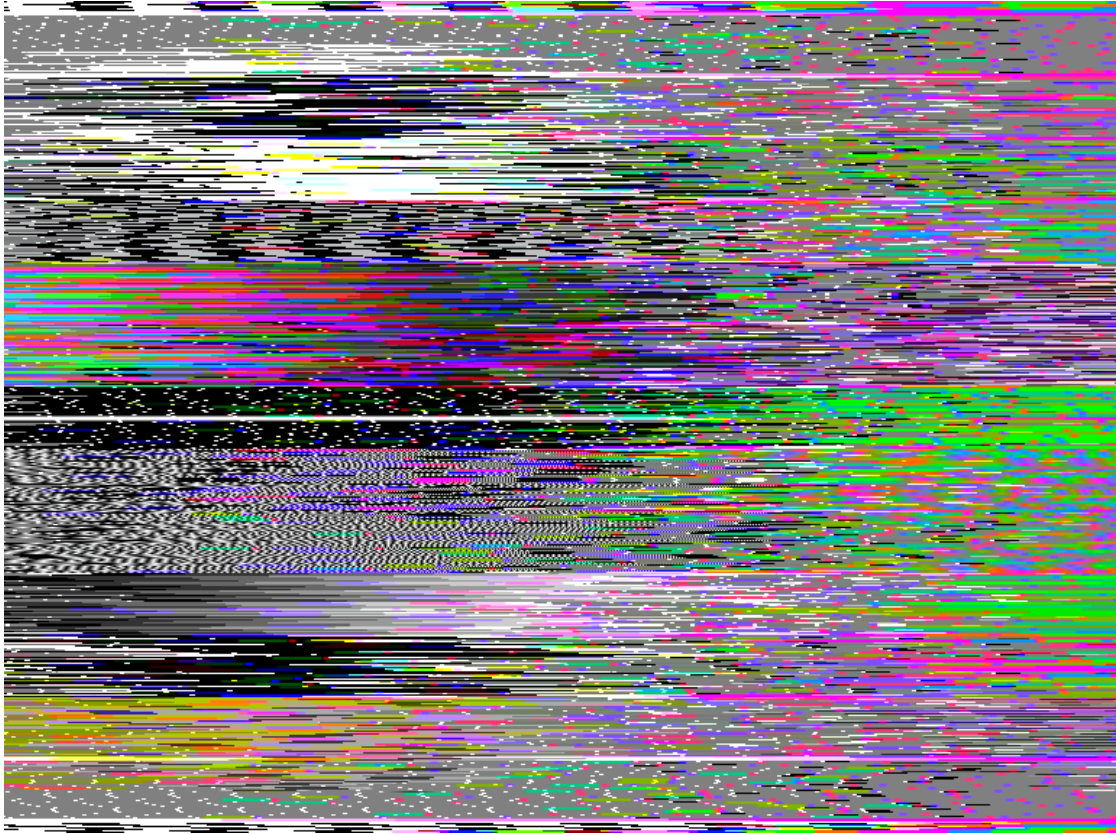
Decoding of a "Eurocrypt simple cut" encrypted MAC format by a satellite/cable receiver that does not have the necessary rights for Eurocrypt decoding
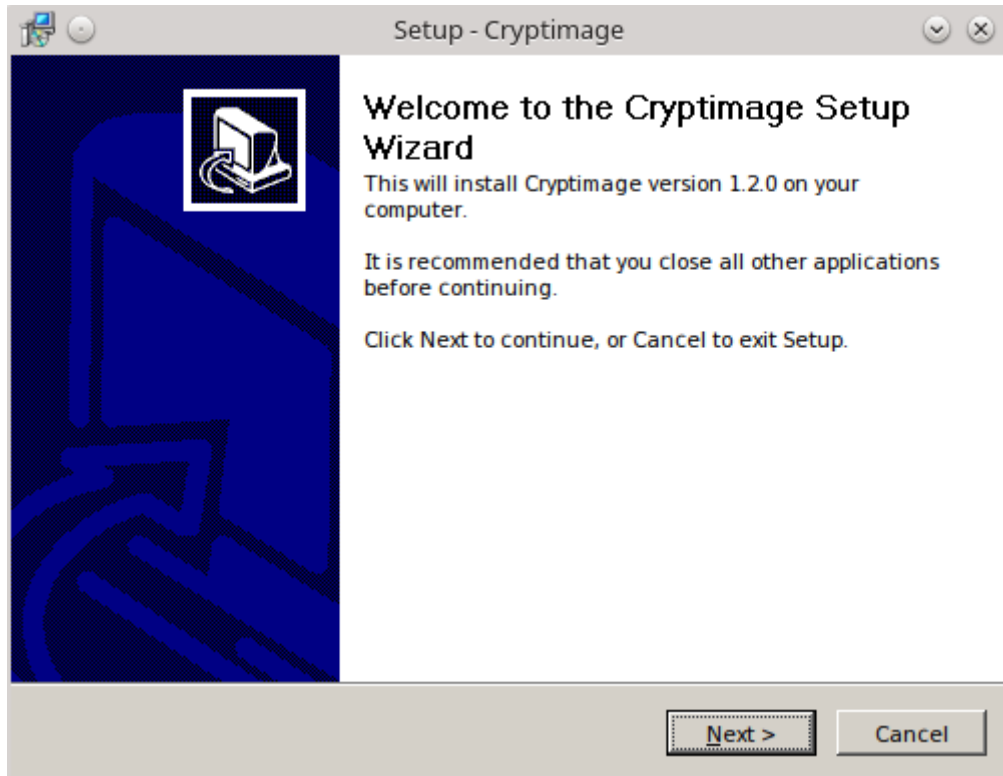

Decoding of a "Eurocrypt double cut" encrypted MAC format by a satellite/cable receiver that does not have the necessary rights for Eurocrypt decoding

6. Software installation

a. Windows

For windows OS the easiest way is to use the setup.exe file, available in cryptimage website, under the download section :

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

Setup.exe will install cryptimage with an embedded java virtual machine, create a shortlink in desktop for cryptimage, install the documentation files and a link to uninstall the software.

b. Linux, MacOSX

If you use linux or MacOSX then you will have to download the jar version.

A java virtual machine must be installed on your PC :

https://www.java.com/

When all these things are installed the launch of cryptimage can be made by double clicking on the jar file, which will launch the java virtual machine (if it's not the case you will have to associate "jar file extension" to java.exe process in your OS),

another way for running cryptimage is to type this in a console :

java -jar cryptimage.jar

7. Using cryptimage

At startup you will see the main interface :
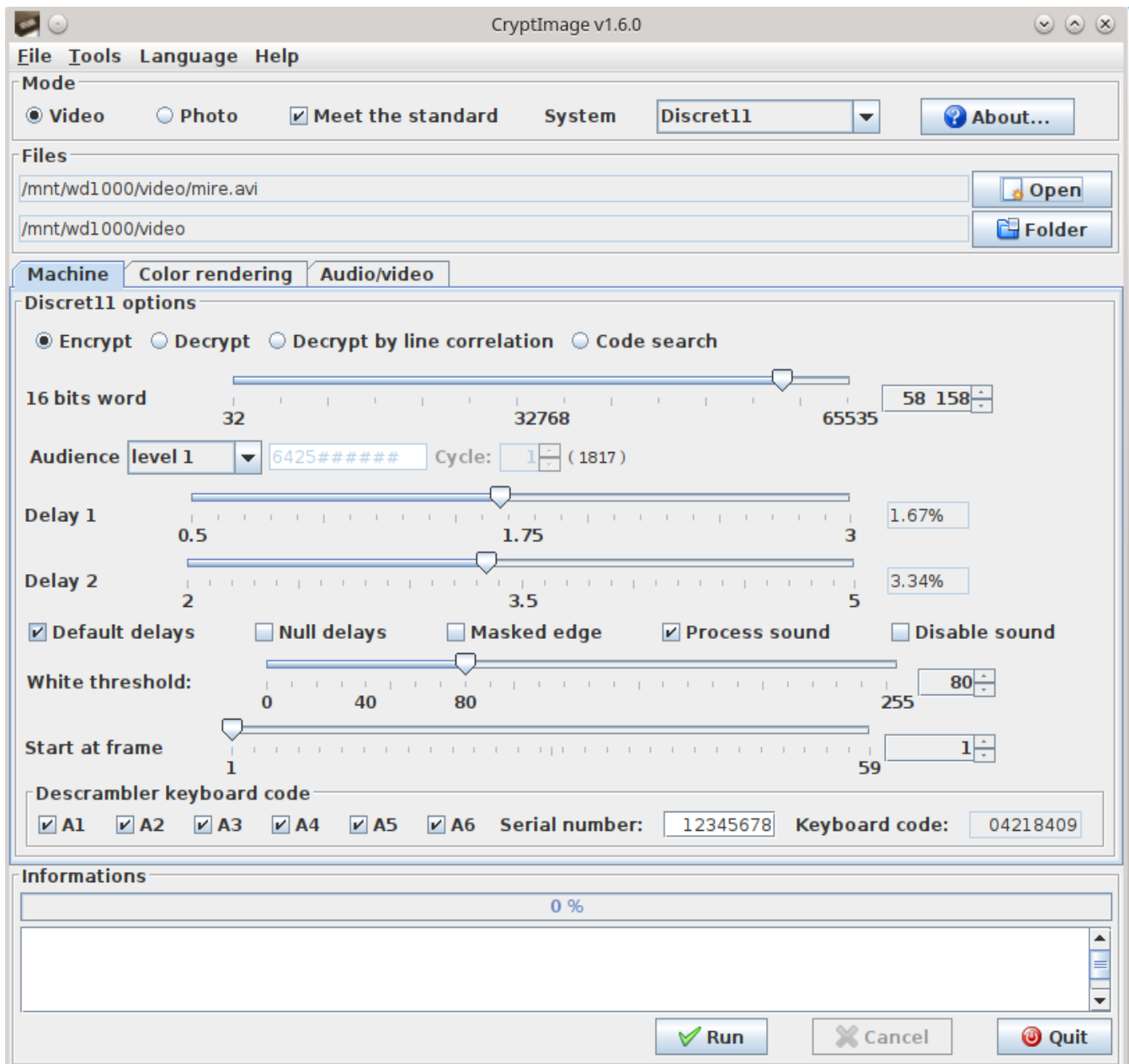
Cryptimage interface, the look and feel will be different depending your operating system

The interface has 6 sections : "mode", "files", "Discret11/nagravision syster/videocrypt/MAC-Eurocrypt/transcode options" (Machine tab), "Descrambler keyboard code", "audio/video options" and "informations".

There is a menu bar with a "language" menu, 6 languages are available : german, english, spanish, french, italian and polish.

a. Mode
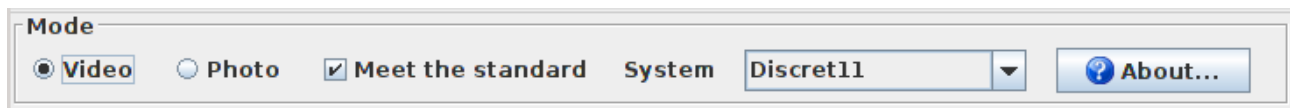
Here you can select 2 modes : "video" if you want to encrypt/decrypt a video file, "photo" if you want to encrypt/decrypt an image file.

A checkbox "meet the standard" allows you a total respect of discret11 standard, if checked then the image will be automatically resized to 4/3 ratio and 720x576 or 768x576 pixels size, TV lines 310 and 622 will be managed and colorized to white or black, if this checkbox is not checked then a simplified mode will be used for discret11 encryption (image will keep its original size, and no colorization for TV lines 310 and 622).

For nagravision syster, videocrypt and MAC-Eurocrypt this checkbox will be checked by default and there is no way to uncheck it, because nagravision syster, videocrypt and MAC-Eurocrypt can only work on a 4/3 ratio and 720~768x576 pixels.

Finally a combobox "system" allows to choose between discret11, nagravision syster , videocrypt, MAC-Eurocrypt and Transcode.

b. Files
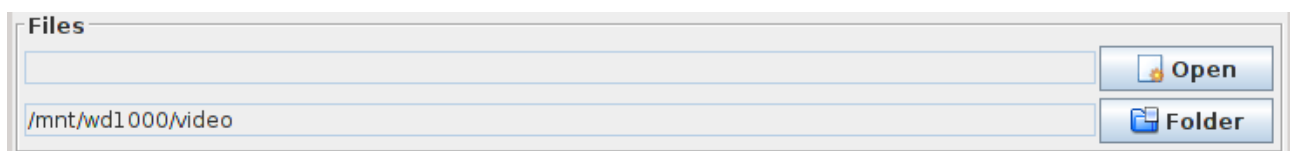
This section allows you to open the video/image to be encrypted/decrypted (button "open"), and to setup the working folder, a folder where the encrypted/decrypted files will be written (button "folder").

c. Discret11 options

This panel allows several encrypt/decrypt settings for discret11 system (this panel will be displayed if "discret11" is selected on the combobox "system").

- Encrypt, Decrypt, Decrypt by line correlation

These buttons allows to choose between the encrypt and decrypt mode, and a special mode "decrypt by line correlation" allows to decrypt the file automatically, without parameters like 16 bits value (this special mode is only available when checkbox "meet the standard" is checked).

- 16 bits word

It's a value between 32 and 65535, which will be used by cryptimage for setting others parameters like 11 bits word, level audience and keyboard code. Every discret11 descramblers are configured with a 16 bits word (this value is deducted from the keyboard typed eight-digit code on the front, we'll see that later in the documentation).

- Audience

a. Levels : 1 to 7

You can choose 7 audience levels from the combobox and a special level called "multicode", the first 7 levels of audience allow to automatically generate a 11 bits word (values 1-2047), with this 11 bits value a pseudo-random generator will be initialized, which allows then the selection of one
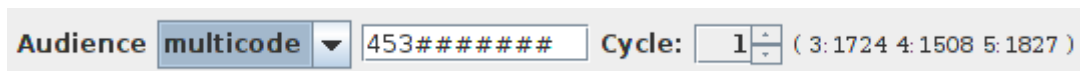
of 3 type of delay value for the encrypt/decrypt process .

Cryptimage also indicates in parenthesis the 11 bit word used depending on the selected audience level.

Audience level "7" corresponds to that used at the time by canal plus the last weekend of the month , it's an "universal code", which enable official descramblers to operate even in the absence of a valid keyboard code.

If checkbox "meet the standard" is checked then cryptimage will be able to decrypt the video without having to set the audience level in the interface, because the blink rate of TV lines 310 and 622 will allow to retrieve the correct audience level.
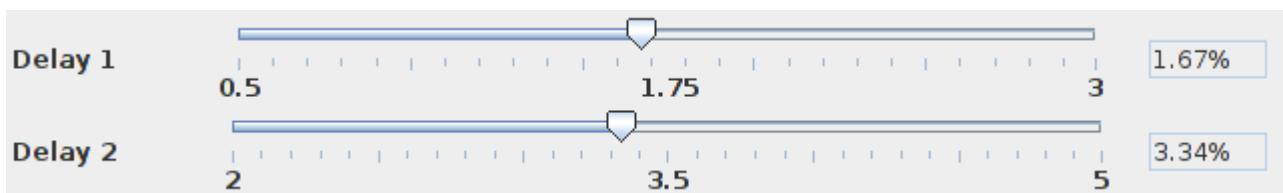
b. Multicode

You can also select "multicode", a special audience level, the multicode gives you the ability to specify up to 10 audience levels, these audience levels will be used in a cyclically way, ("cycle" paramater is the time in seconds for the duration of each audience level), in parenthesis cryptimage will display the corresponding 11 bits word for each audience level entered.

The "multicode" was used by canal plus in 1987 in order to disable illegal descramblers, but this method failed (hackers quickly found a solution for their illegal descramblers), and "multicode" was quickly removed, after that only one level audience was used .

- Delays 1 and 2

These 2 sliders allow to set 2 of the 3 types of delays in pixel shift percentage, (the other delay, "delay 0" means no delay). Generally you will not have to change these two delays, default settings (1.67% and 3.34%) are correct for a good simulation of discret11, however some unofficial hardware descramblers may need different values, if their circuits were poorly calibrated.

A check box "default delays" allows at any time to bring back the sliders delays to the default settings.

This checkbox allows to set the 3 delays values to zero, making it possible to have an image always in clear, except lines 310 and 622 which will be in "discret11" mode, this allows a hardware decoder

to act as an encoder when we will give it this type of video, it will encrypt the image instead of decoding it when it will see lines 310 and 622 flashing in "discret11" mode.

- Masked edge

This option will hide the black segments of the left vertical edge of the image with color pixels taken further in the current line of encryption, to prevent some pirate descramblers operate (including "radio Plans" descrambler that uses the black detection edge as a method for decryption).

This anti-piracy measure was used by Canal Plus in 1985.

Note that if this box is checked while the "decrypt" mode is selected then it will effectively ensure that the black vertical border located on the right will be hidden.

- Process sound, Disable sound

Checkbox "Process sound" means that the sound will be encrypted/decrypted by cryptimage if this checkbox is checked. If unchecked then the sound will keep his original signal.

Checkbox "Disable sound": if checked then sound will be muted, the resulting encrypted/decrypted file will not have a sound track.

- White threshold

This slider will set the RGB color value of white, for the detection of TV lines "310" and "622" by the system, lower values can help the descramble process, and if "null delays" checkbox is enabled then it will allow to save the video file with TV lines 310 and 622 drawed to full white.
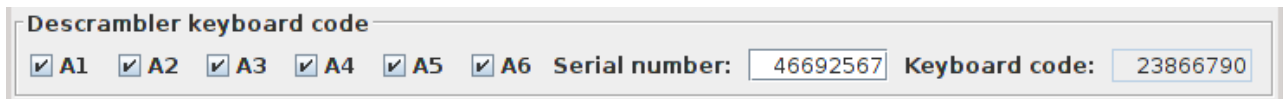
- Start at frame

A video is composed of frames, with cryptimage you have the opportunity to tell the encoder / decoder from which field it should start its work, simply drag the cursor on the frame number from

which the encryption / decryption must to start.

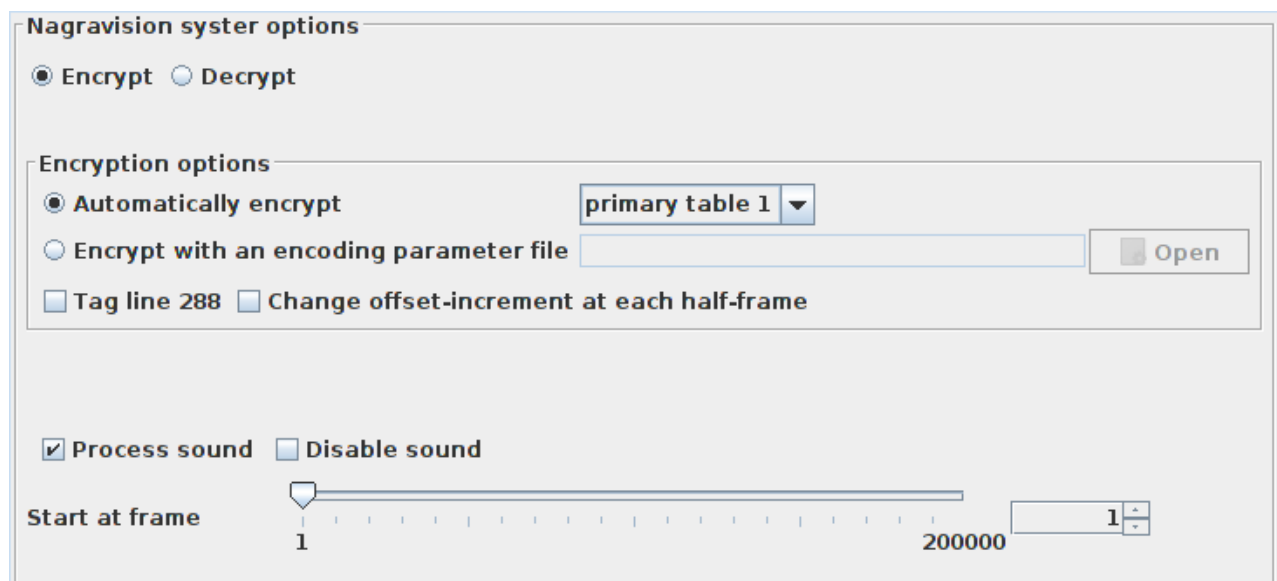## - Descrambler keyboard code

This section of the interface is useful for those who have an official discret11 descrambler, it allows you to find the keyboard code.

This keyboard code is calculated based on your descrambler serial number (number that you can enter in the "Serial Number" field), then according to audience level permissions (check boxes A1 to A6) and finally 16-bit word, the keyboard code will be displayed on "keyboard code" field in the interface.

# d. Nagravision syster options

a. Encryption options

This panel is displayed when "nagravion syster" is selected ("system" combobox), and when the button "encrypt" is selected.

These encryption options allow you to create "nagravision syster" encrypted video/photo files.

There are 2 ways for encrypting in nagravision syster :

- **"Automatically encrypt"**: using a primary table (you can select "primary table 1" or "primary table 2"), the program will randomly generate an offset and increment for each half-frame of the video file (or the photo file).

- **"Encrypt with an encoding parameter file"**: it's a text file (with the extension "enc") that describes for each progressive frame 2 values (offset and increment), this file also indicates what type of primary table to use, such a file can be generated via the menu "tools, generate an encoding parameter file":
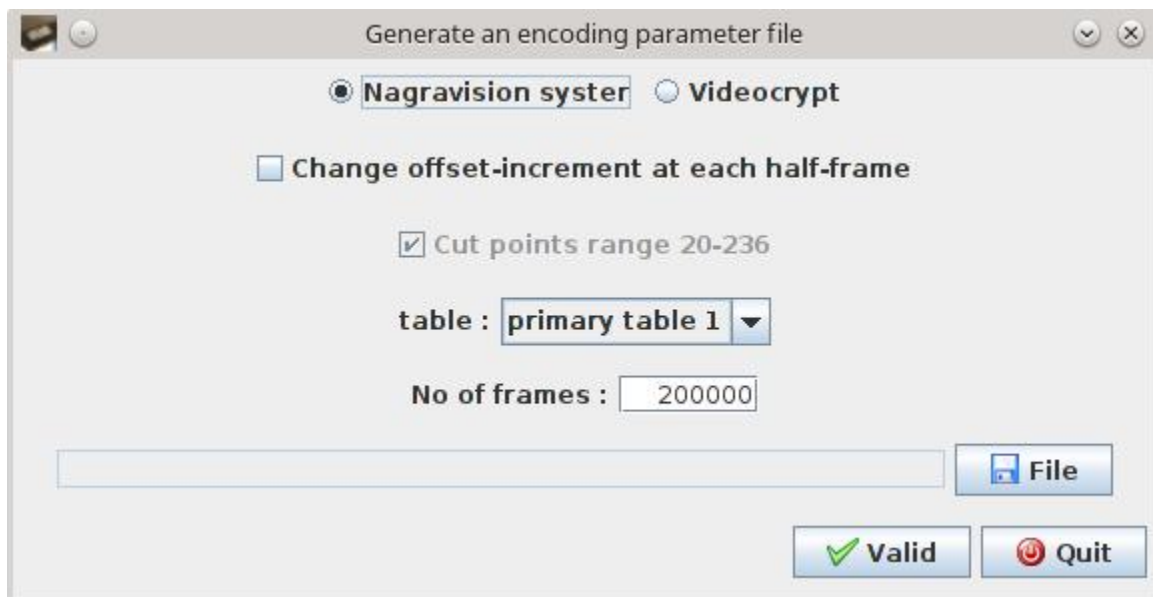
to be valid this file must have at least a number of rows equal or greater than the number of frames of the video.

There are 2 types of selectable primary table:

- Primary Table 1: used by several satellite/cable channels in europe, as well as canal plus until september 1997.

- Primary Table 2: used only by canal plus from september 1997 until the extinction of analogue terrestrial broadcasting TV in France in late 2010.

In addition to these two encryption options you can "tattoo" line 288 by checking the box **"tag line 288",** values like "type of primary table", "offset", "increment" will be coded in line 288 with white and black pixels, the type table used will be coded on 2 bits, the offset and the increment will be coded each on 8 bits, each bit utilizes 8 pixels in the image, the tattoo is placed at the bottom left of the image, on both last lines of the image (line numbers 575 and 576 of a progressive frame 768x576 lines).

Finally a checkbox **"change offset-increment at each half-frame"** allows to change offset-increment at each half-frame, if unchecked offset-increment will be changed every 2 half-frames.

b. Decryption options

This panel is displayed when "nagravion syster" is selected ("system" combobox), and when the button "Decrypt" is selected.

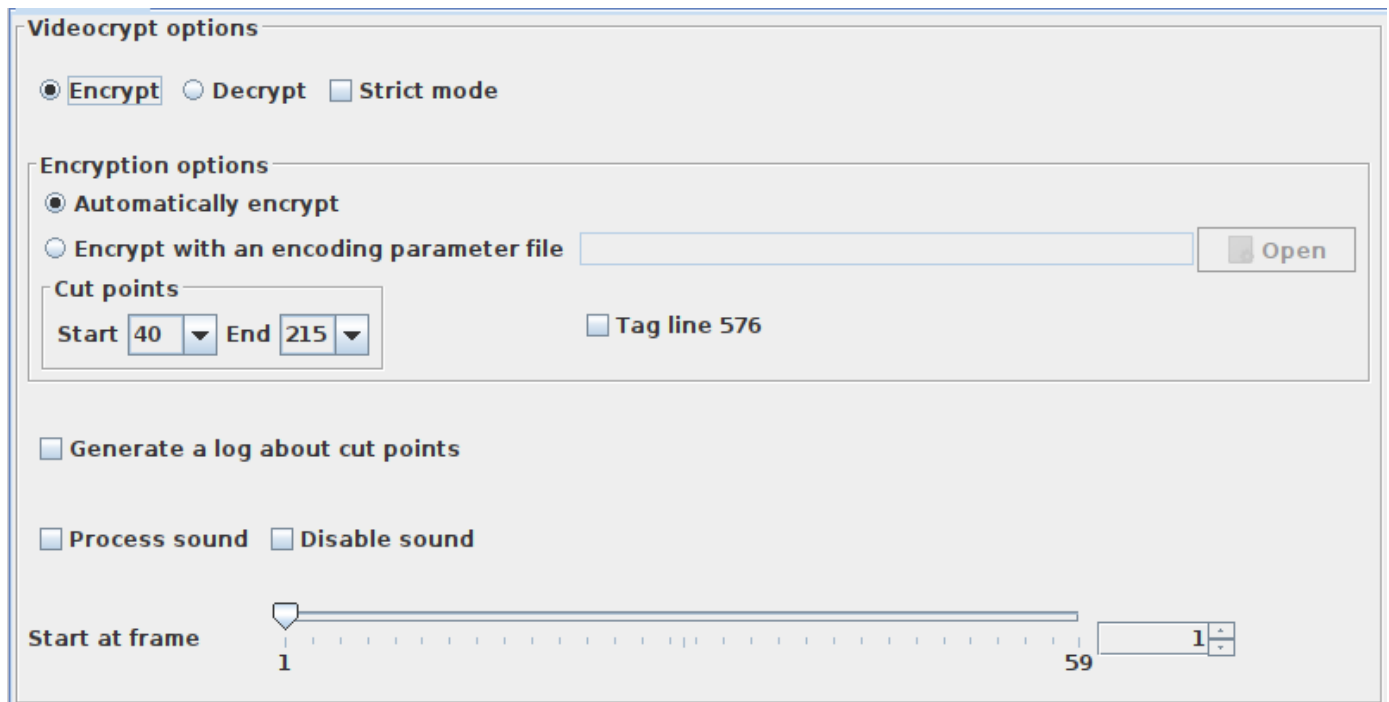There are 3 ways for decrypting in nagravision syster :

- **"Decrypt with a decoding parameter file"**: it's a text file (with the extension "dec") that describes what primary table   and what offset/increment values to use for each half-image when we want a decryption, this file **is automatically generated** by cryptimage when a video/image is encrypted in nagravision syster mode.

- **"Decrypt with the tag of line 288"**: Decryption will be done automatically if a tag is present on line 288, if you have checked "tag line 288" option during the encrypting step then you can use this decrypting option.

- **"Decrypt by line correlation"**: Decryption will be done by testing the 32768 possibilities of decryption and the correct offset/increment values will be found, if you choose this option then you have to select one of the two primary tables in the combobox, this method of decryption by line of correlation is quite slow but gives quite good results.

Note that as for the discret11 panel you have the same sound options ("Process sound", "Disable sound") and you have also the option "start at frame".

For debugging purposes a "reverse decoding" checkbox allows you to decode a video that has been "encoded" by a syster decoder (using SDR hacktv software, by sending VBI informations to force a syster decoder to activate and decode a video in clear, allowing to obtain a video encrypted in syster "reverse mode").

e. Videocrypt options

a. Encryption options

This panel is displayed when "videocrypt" is selected ("system" combobox), and when the button "encrypt" is selected.

There are 2 ways for encrypting in videocrypt :

- **"Automatically encrypt"**: the software will chose randomly the cut points.

- **"Encrypt with an encoding parameter file"**: a "vid" file which contains seed values for the random number generator, this file can be generated via the menu "tools, generate an encoding parameter file".

A listbox "Cut points" allows to set the range of cut points, in order to have the same visual rendering as the TV channels which have used videocrypt , by default the range will be "40-215".

A checkbox "Tag line 576" allows to put in line 576 a tattoo which represents the range of cut points and the seed value for the random number generator, in order to have an automatic decrypting by reading this tattoo.

The "strict mode" check box allows you to reproduce the particular right and left margins of the videocrypt.

You can also generate a report (CSV format) about these cut points by checking the checkbox "generate a log about cut points". This CSV file will be splitted every 113 frames (65088 lines) in order to allow old spreadsheet programs to load them.

b. Decryption options

This panel is displayed when "videocrypt" is selected ("system" combobox), and when the button "decrypt" is selected.

There are 3 ways for encrypting in videocrypt :

- **"Decrypt with a decoding parameter file"** : it's a text file (with the extension "vid") that describes how to feed the random number generator in order to select the cut points for each line.

- **"Decrypt with the tag of line 1"**: the decryption will be done automatically by reading the tattoo on line 1, if the option "Tag line 1" has been selected during the encryption step.

- **"Decrypt by line correlation"**: the decryption will be done automatically by following a special algorithm, this method is very slow (3 seconds by frame) .

Note that as for the discret11 panel you have the same sound options ("Process sound", "Disable sound") and you have also the option "start at frame".

f. MAC-Eurocrypt options

The MAC-Eurocrypt option allows images to be encoded in MAC (Multiplexed of Analog Components) format, where sound, chroma and luma are transmitted sequentially,
Optionally a "Eurocrypt" encryption mode can be activated.

- **"Encode to MAC"** with **"Disable Eurocrypt"** option: the first 192 pixels of the image will contain the sound in digital format, the next 384 the chroma part of the image, with chroma V (R – Y) part on a line, and on the next part chroma U (B – Y), and finally the luma (Y) occupies the remaining 768 pixels of the image.
The output image will therefore have a format of 1344 x 576 pixels.

- **"Encode to MAC"** with **"Enable Eurocrypt with simple cut"** option: encoding to the MAC format is carried out, then the chroma part is rotated "cut and rotate", all the pixels of the chroma to the left of the cut point are moved after the last pixel of the luma zone.

- **"Encode to MAC"** with **"Enable Eurocrypt with double cut"** option: encoding to the MAC format is carried out, then the chroma part undergoes a "cut and rotate" operation, and the luma part also undergoes a "cut and rotate" operation.

- **"Encode to MAC, then decode to 576p without Eurocrypt management"** with **"Disable Eurocrypt"** option: encoding to the MAC format is carried out, then decoding to the 576p format is carried out immediately, without worrying to process possible Eurocrypt encryption, the purpose of this option is to simulate the rendering of an encrypted MAC signal on a satellite/cable terminal where no subscription has been taken out.

- **"Decode from MAC to 576p"**: this option allows you to find the original 768 x 576 pixel image from an image encoded in MAC 1344 x 576 pixels, combined with the Eurocrypt options it also allows you to decode Eurocrypt.

- **"Random seed"**: represents the number used to initialize a pseudo-random value generator, which is used to create the cut points for Eurocrypt.

g. Transcode options

The transcode option allows you to convert images without encrypting/decrypting them, useful for testing PAL/Secam modes.

h. Colors rendering
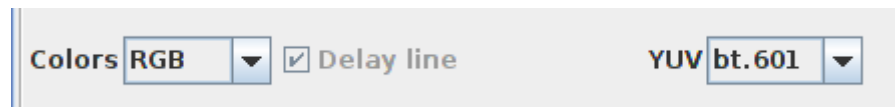
The tab "Colors rendering" allows to choose how the colors will be rendered for the files created by cryptimage.

- **RGB** : colors will not be modified, they will be the same as the input file.

- **Pal** : colors will be changed, by following the Pal standard (phase rotations), U and V chroma will be averaged by group of 2 lines if the checkbox "Delay line" is checked. This version of Pal is not used with discret11.

- **Pal composite**: much more realistic version of pal rendering, with a dedicated control panel:
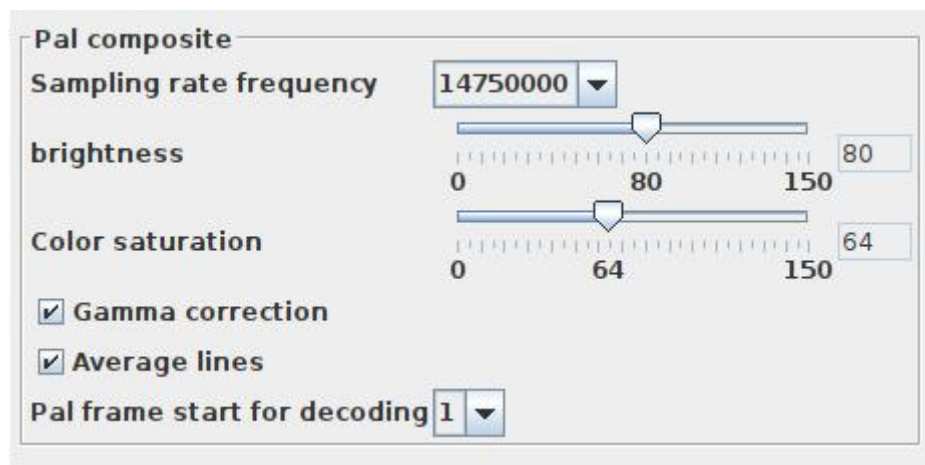
this mode is divided into 3 variants:

- encode and decode: produces a PAL color image.

- encode only: produces a black and white image with PAL chrominance information in the form of dot and hatch patterns.

- decode only: produces a PAL color image from a black and white image with chrominance coded in the form of dot and hatch patterns (black and white image generated by the "encode only" mode).

- **Secam** : colors will be changed, U and V chroma of each line will be computed depending on the previous line, in case of interruption of alternation "V-U" (red, blue) then lines will go into black and white or will be set to red, blue or purple depending on the context.

A combobox "YUV" allows to set the matrix color for the conversion RGB to YUV, "bt.601" for

SD videos (single definition), "bt.709" for HD videos (high definition), "special" if these 2 options don't give good results.

This tab "colors rendering" is useful if you want the same visual rendering of a Pal/Secam TV set, when nagravision and videocrypt systems are used, a rendering that is very different from RGB mode.

i. Audio/video options

These are options for the generated video file, you can select the resolution of the file (only if you have checked "Meet the standard"), crop the input image to 4:3 pan and scan, letterbox or 4/3 stretch (only in encrypt mode), the compression video codec, the file container (extension), audio codec and its bitrate, sample rate (44100 or 48000 Hz) video compression rate (bitrate), the number of frames for this file (the duration of the file will be displayed in parenthesis).

Also you have the option to timestamp the video file name, date, time, the discret11 options, keyboard code will be automatically added to the name of the video file created.

A check box "preview mode" allows you to disable the creation of the video file on disk, it will open a new window which will act as a "preview mode", there is no sound in this preview mode, an "on/off" button in this preview mode window allows to enable/disable the encryption/decryption process.
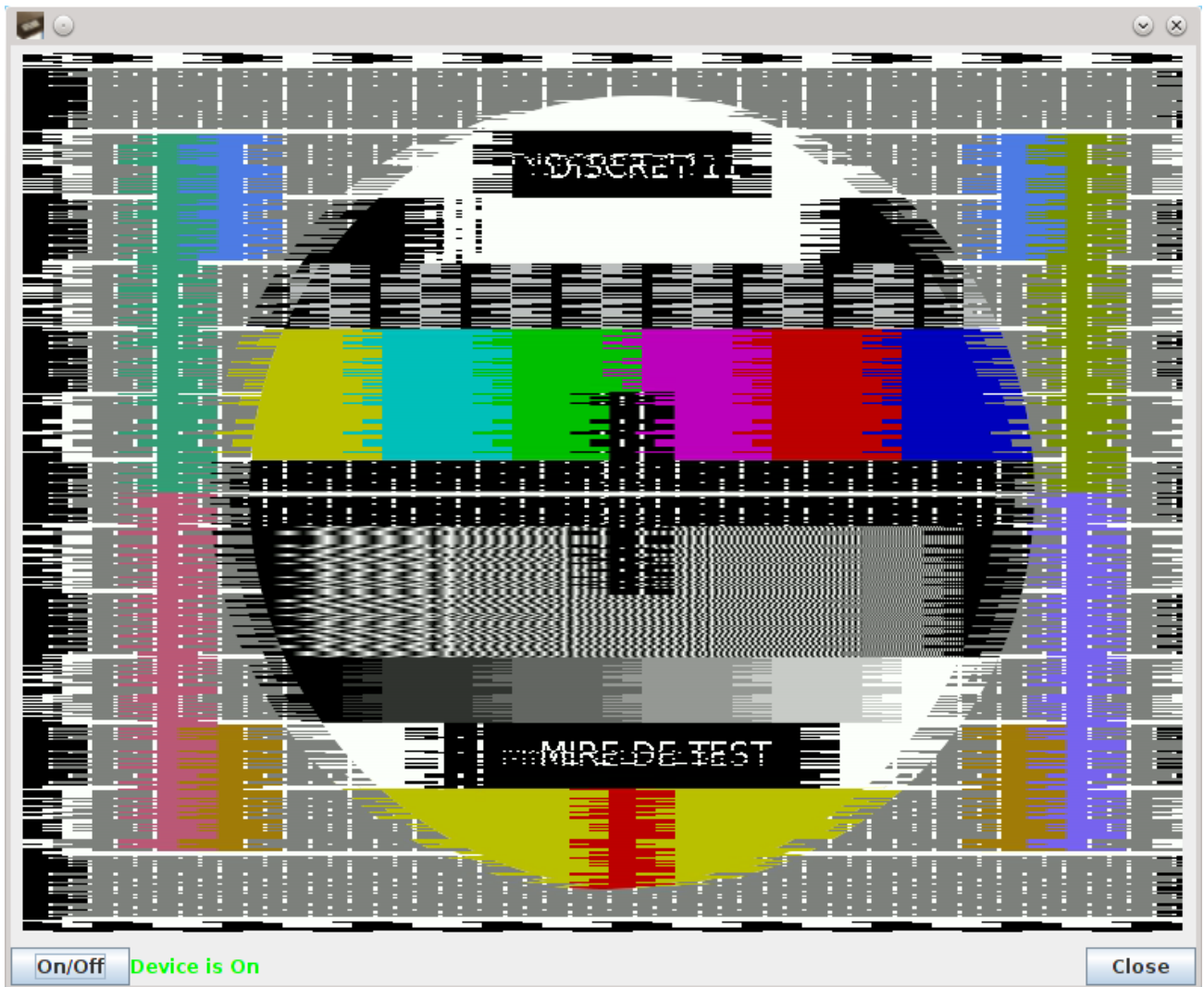
Window of the preview mode

j. Informations
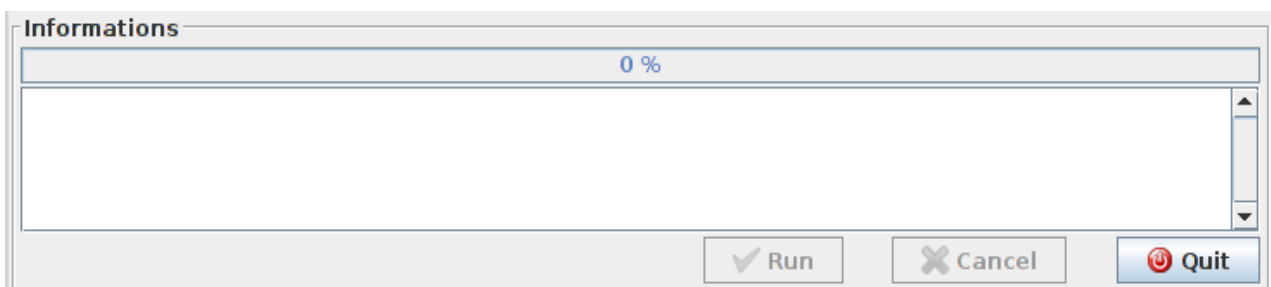
This part of the interface allows you to track the progress of processing the video file, via a progress bar with a percentage, a text box to display the information messages and any error messages.

The "run" button will start the processing of the video file, the "cancel" button to cancel the operation, the button "quit" to close cryptimage.

Progress information messages when a video file is encrypted

At the end of the generation of the video/image file a text report will be generated in the working directory, it will contain different discret11 parameters used to generate this file.

Finally most of the interface options are saved in a configuration file (cryptimage.conf) stored in the user directory ("documents and settings" under windows, folder "home" on linux) in a subdirectory " cryptimage ", in order to automatically reload these choices at the next launch cryptimage.
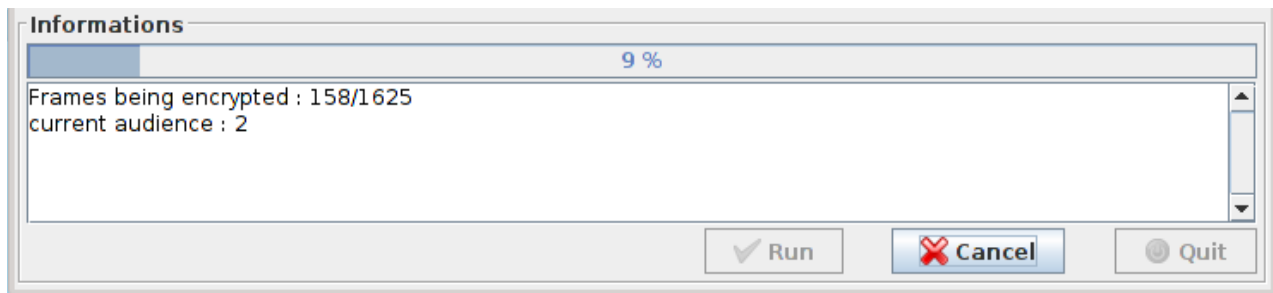
8. Using cryptimage with a discret11 descrambler

Cryptimage can therefore be used to generate video files, in order to test an official discret11 descrambler, such as the one provided at the time by canal plus.
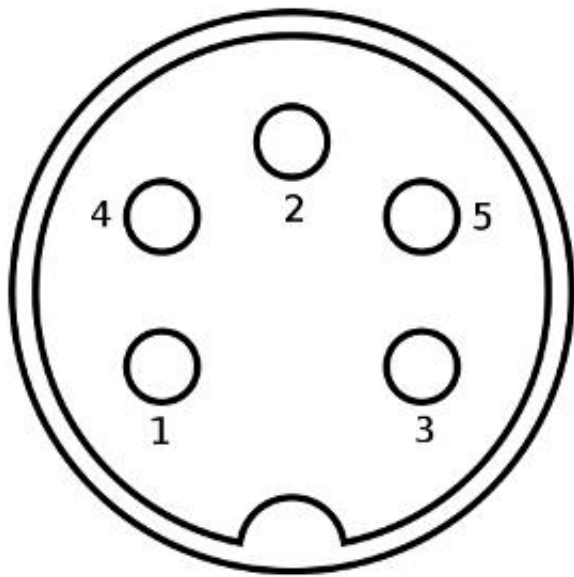

Official discret11 descrambler

a. Setting a serial number in rom memory

The first step is to set a custom serial number in the rom chip, so that you can later generate a valid keyboard code with cryptimage.

For this we will use the socket type "Din 5 pin" located in the back of the descrambler, the operation is to connect pin 1 to shield mass :

pin assignment:

1 : serial number programming

2 : audio ground

3 : video output

4 : audio output

5 : audio ground

DIN socket, front view at the back of the descrambler

Once pin 1 connected to the ground shield we can then use the keypad on the front descrambler to enter a serial number in the rom memory :

- Tap 4 times on the key "ENT"

- Enter the first 4 digits of the serial number

- Tap once the key "MEMO"

- Tap 2 times on the key "ENT"

- Enter the last 4 digits of the serial number

- Tap once the key "MEMO"

The 8-digit number will be stored in the rom chip (example: 4669 2567), then you can remove the bridge you made between pin 1 and shield ground to complete the operation.

In cryptimage enter the serial number in order to find the keyboard code :

Here we see that the keyboard code for serial number "46692567" is "23866790", the 16-bit word entered in the interface is 18270, the audience level is 1, with all permission boxes checked (A1 to A6).

To enter the keyboard code in the descrambler :

- Press the ENTER key, the yellow light will flash

- Tap the 8 digit keyboard code

- Press the MEMO button to confirm, the yellow light should go off, the green light will then switch to decrypt all encrypted video signal.

b. Inject a video file to your descrambler

Now that we have properly configured our official descrambler (serial number and keyboard code) we can test our descrambler by sending encrypted files with cryptimage.

We have to put an encrypted video file in a USB drive, and then use a DVB-T device which has a USB port (PVR function) and a composite video output and audio output (RCA or SCART connection), then we connect this DVB-T device to the composite video input of the descrambler and the audio input (via an RCA composite video input → SCART adapter) :

DVB-T device with a USB port (PVR function)

Scart cable, with inputs and outputs in RCA format

Reading the files will be done via the DVB-T device, which will read the USB key containing our encrypted files, the discret11 descrambler will receive this file via the composite video and audio outputs of our DVB-T device, and finally we will connect the descrambler to our TV via the scart cable (composite video output and analog audio output).

An alternative method is to use an RF modulator connected to the composite video output (as well as the audio output) of your DVB-T device, then connect the RF modulator to the antenna input of your TV, and finally connect the descrambler via the SCART cable to the TV, this method has the advantage of reconstituting the original installation as it had been planned for the official descrambler (video signal taken by the descrambler from the TV via SCART).

RF modulator, with RCA and scart inputs

It is advisable to add a transcoder "PAL to SECAM" before injecting the video signal to the descrambler or the TV, because analog delay lines of discret11 descrambler were not optimized for a Pal video signal (bad colors if Pal video is used on discret11 descramblers instead of Secam).

A summary of the assembly for injecting our encrypted video file to a discret11 descrambler :

- Cryptimage → USB key → DVB-T device → discret11 descrambler → TV

or

- Cryptimage → USB key→ DVB-T device → RF modulator → TV → discret11 descrambler

9. Advice

In order to get a good picture quality while decrypting a video file (with cryptimage or with an official descrambler) it is advisable to use a compression ratio less destructive as possible during the encrypting step,

because of the pixel shifting during the encrypting step some compression artifacts, color defects can occur if the compression rate was too strong, using a video bitrate equal or greater than 10000 will allow to limit quality losses.

The solution to avoid these quality problems is also to use a lossless video codec, like huffyuv or FFV1, this type of codec provides the best possible quality, the decrypted image will be exactly the same as the original image, the only drawback of huffyuv codecs and FFV1 is the large size of the generated file (although it is possible to "zip" the file in order to reduce the file size and to store it permanently on a DVD-R media for example).

Another alternative is to select the codec "h264 v2" which has the particularity to code colors on a color space " 4:4:4 YUV " instead of the traditional " 4:2:0 YUV" (best color accuracy), the losses will be lower, the disadvantage is that DVB-T devices can not play files encoded in a color space " 4:4:4 YUV ", if you want to use a DVB-T device then you have to use codec "h264", "mpeg2" or "divx" from the list of codecs for playback compatibility.

 "Ts" and "m2t" video files made from a recording of DVB-T device will trigger problems in cryptimage , these files don't have a video index, you must first modify these files with software like handbrake (free, open source software) in order to have a real indexed video file in a "avi", "mp4" or "mkv" container.

Regarding the choice of audio codec : you will have the best possible quality by choosing "wav" from the list of audio codecs, as a good compromise you can also choose "mp3 192 kbps" or "mp3 320 kbps", for the sampling frequency 48000 Hz obviously gives the best quality, in all cases you should never go below 160 kbps if you use mp3 codec for encrypting files, because the quality of the audio decrypting will be especially bad if for example a rate of 96 kbps was used for the mp3 codec during the encrypting step.

Finally if you want to decrypt VHS tapes containing discret11 or Nagravision syster signals then you must digitize with care those VHS tapes, with a tuner card or video capture device in order to obtain a perfect image geometry (no overscan, no vertical offset lines), you must digitize by keeping the odd and even fields (don't make deinterlace), the image must be 720x576 or 768x576 pixel size, and you must use a lossless video codec or a less destructive codec with a good bitrate, in this manner the decryption method by line correlation will be done with good results.

10. Bugs

If cryptimage is not working properly then delete the configuration file "cryptimage.conf" located in the user directory ("documents and settings" under windows, folder "home" on linux) in a subdirectory "cryptimage", cryptimage then will start with the default settings.