Compte rendu stéganographie :

1° introduction :

Tout d'abord, nous pouvons commencé par dire que la Stéganographie est l'étude de procédés de dissimulations d'une informations dans une autre, comme le dis l'article Wikipédia a son nom *:"Si la cryptographie est l'«art du secret», la stéganographie est l'art de la dissimulation : l'objet de la stéganographie est de faire passer inaperçu un message dans un autre message et non de rendre un message inintelligible à autre que qui-de-droit.*

Dans ce travail pratique, nous allons essayer de trouver un message dissimulé dans une image.

Avant le début du TP nous aurons besoins de trois outils pour le réalisé :

-Le logiciel GIMP

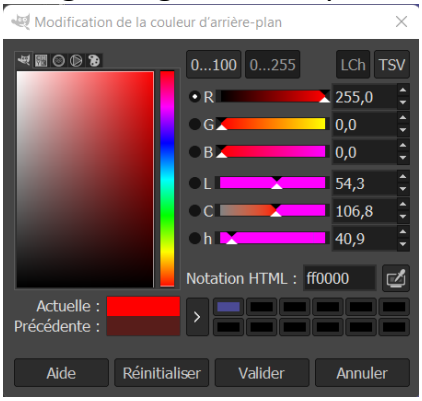
-le code des couleurs (voir ici)

-le code ASCII (voir ici)

2° Pour pouvoir commencer, il faut comprendre quesqu'un pixel ?

Tout simplement un Pixel qui vient de l'Anglais (Pictures Elements) est le plus petit élément d'une image informatisé, c'est-à-dire qu'une image électronique est une suite de pixel codé grâce à trois couleurs dominantes appelés le RGB (Red Green Blue). Donc grâce à ses trois couleurs en informatique nous pouvons créer toutes les couleurs possible et imaginable juste en jugeant l'intensité qui vas de 0 à 255, par exemple pour avoir une

image rouge tous les pixels seront rouges à une intensité de 255.



3° commençons le TP !!

Pour commencer le TP, il faut récupérer l'image (Img0), ensuite l'ouvrir avec GIMP installer au préalable.

Une fois sur GIMP, veuillez prendre la loupe[1] pour grossir l'image à 25600%, grâce à ça nous visualiserons à l'écran que les pixels font 256x256.

Une fois l'image ouverte dans GIMP, et l'image zoomé il faut se rendre au pixel (252,214) pour voir la couleur il suffit de prendre l'outil pipette et cliquez sur le pixel voulu en maintenant la touche Majuscules.

Ensuite trouvé la couleur ainsi que le code hexadécimal.

A noté que si l'on change la couleur d'un pixel en ajoutant ou en retirant un petit nombre à l'un ou l'autre des trois composants, la couleur ne change pas à l'œil nu !

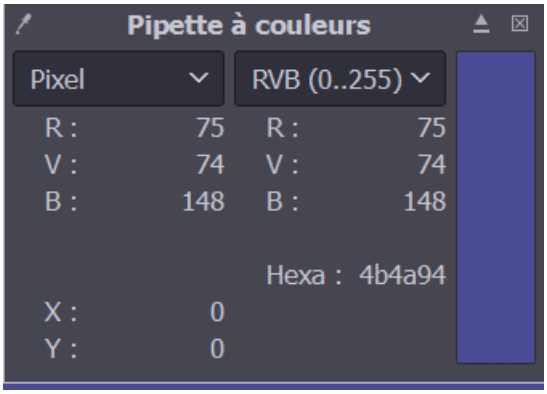
[1] A savoir qu'un appuie sur la touche « CTRL » pendant le clique permet un zoom arrière

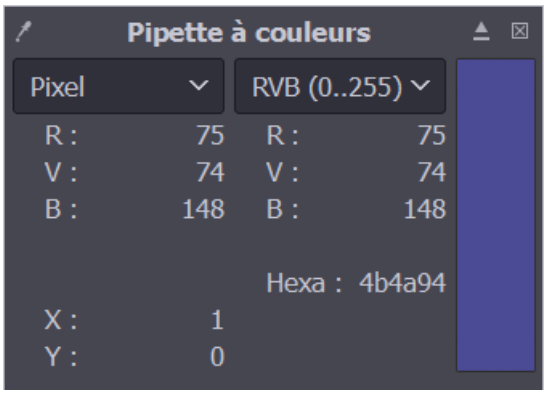
4° Descriptif du procédé stéganographique :

Il faut vérifier les deux pixels de coordonnées (0,0) (0,1) (les deux premiers pixels de l'image sur la ligne horizontale) soit de la même couleur.

Nous voyons à l'œil nu que ce sont les mêmes couleurs mais allons vérifier dans les propriétés du pixel.

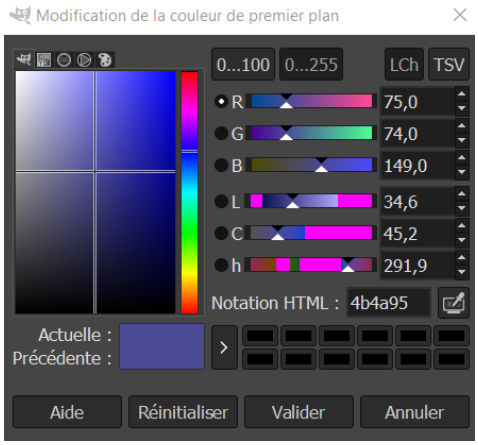
Une fois dans les propriétés, nous voyons que le code hexa(4b4a94) (aussi appelé code HTML) est le même donc la couleur est exactement la même. Ensuite nous voyons grâce au codage RGB (expliqué plus haut) que les couleurs sont aussi les mêmes.





Pour vérifier ce que nous avons dit plutôt, nous allons modifier d'une petite valeur la couleur bleue du pixel en ajoutant 1 : c'est-à-dire que le bleu va passer de 148 à 149.

WARNING : viellez à rester sur une grille de type « RGB (0...255) »



Une fois modifier, nous voyons que malgré la différence de bleu aucune différence n'est visible à l'œil nu. Pourtant les codes hexa sont bien différent !!

Pour le pixel (0,0) le code hexa est : 4b4a95

Alors que le pixel (0,1) le code hexa est : 4b4a94

Deux codes hexa différents pourtant aucune différence a l'œil nu.

Grâce à cette non-perception de la modification d'une ou des unités des trois composants de la couleur d'un pixel, on peut alors cacher par exemple un Bit dans un pixel, pour être plus précis, si le bit vaut 0 on modifie la composante de couleur de sorte que son écriture binaire soit 0 et dans l'autre sens si le Bit doit être 1, on modifie de sorte que l'écriture binaire finisse par 1, en laissant inchangé les autres pixels.

5° retrouver un message :

Nous avons vue au-dessus comment cacher un message maintenant voyons comment retrouvé un message.

Pour continuer il faut télécharger cette image(Stegano-img0) ensuite l'ouvrir sur GIMP comme l'image précédente. Dans cette image, tous les Bits dissimulé corresponde au Bit de poids faible de la composante bleu de la couleur des pixels

Le nombre L de caractères du message est dissimulés dans la ligne d'ordonné 0. Le nombres de caractères est caché dans les 8 premiers pixels de cette ligne, tous ces pixels donne un bit de l'écriture binaire de cette longueur.

Il faut donc utiliser GIMP pour retrouver le message caché dans cette image

Ce que nous savons : le message qu'il faut retrouver est un petit texte qui est codé en binaire en utilisant le codage ASCII .Ce codage code chaque caractère du message dissimulé sur huit bits. Donc le nombre de pixels qui dissimule un

bit du message est donc égale à 8*L (le nombre L est a trouvé grâce à la ligne 0). Les pixels qui dissimulent le message sont eux sur la ligne 1 en partant de la gauche.

Commençons par retrouver le nombre L dans la ligne 0 :

Pour le retrouvé prenons les 8 premiers pixels (en haut à gauche sur la ligne horizontal) car c'est codé en bit donc pour retrouver un nombre en binaire il faut à tout prix 8 caractères

Notons donc les valeurs de la composantes bleus trouvé :

Pixel (0,0) valeur bleue : 148

Pixel (0,1) valeur bleue : 148

Pixel (0,2) valeur bleue : 148

Pixel (0,3) valeur bleue : 148

Pixel (0,4) valeur bleue : 148

Pixel (0,5) valeur bleue : 149

Pixel (0,6) valeur bleue : 148

Pixel (0,7) valeur bleue : 148

Si nous traduisons ceci en binaire en prenant le plus petit nombre égal a 0 et le plus grand égal à 1 car en binaire il n'y a uniquement 2 caractères (le 0 et le 1)

Cela donnera : 0 0 0 0 0 1 0 0 maintenant nous pouvons traduire grâce au code ASCII :

4	04	04	0000100	EOT	*End of Transmission* (fin de transmission)

Une fois que nous savons que cela donne 4, une grande partie pour retrouver le message caché est faites car le nombre L égale à 4 donc 8*4 = 32

Faisons le lien avec la suite un message est caché en binaire avec 32 bits si on divise 32 par 8 on obtient 4 donc on sait donc que 4 caractères sont dissimulés grâce aux 32 premiers pixels de la ligne 1

Passons maintenant à la ligne 1 :

Partons du principe que le mécanisme est le même donc prenons 0 pour 148 et 1 pour 149 :

0 1 0 1 0 1 0 0

0 1 0 0 0 0 1 0

0 0 1 0 0 0 0 0

0 0 1 0 0 0 0 1

Une fois les 4 caractères trouvé en binaire cherchons la traduction !!

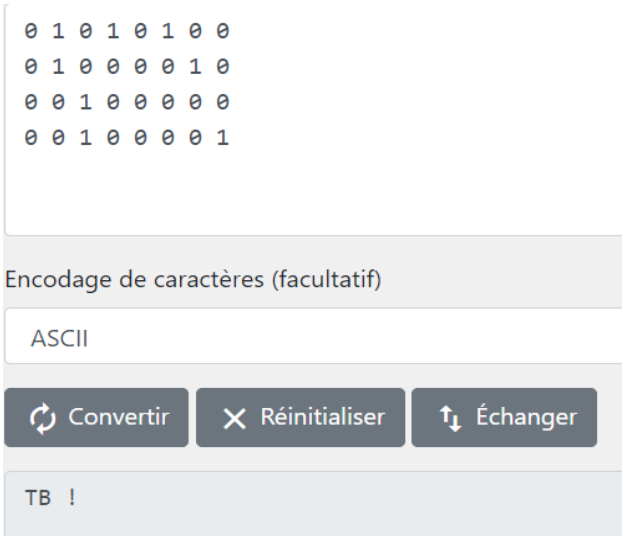
1010100	T
1000010	B
0010000	DLE

A savoir que DLE signifie espace en Français pour signifier un espace entre le B et le !

0100001	!

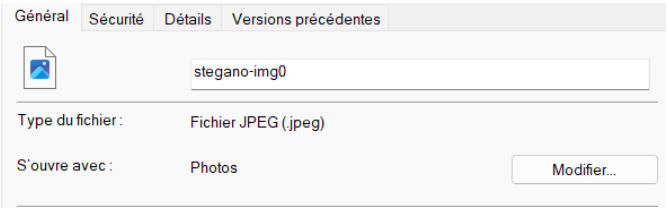
Le message caché est donc : TB !

ASTUCE : Pour faire la traduction un peu plus rapidement nous pouvons s'aider d'un traducteur sur internet !!



6° Les formats des fichiers :

Tout d'abord, sachez que pour une image il existe plusieurs formats de sauvegarde : bitmap (bmp), jpeg (jpg), portable network graphics (png), ...



Une fois le fichier enregistré en JPEG la composante bleue est égal à 149 partout.

L'image au format PNG a une taille de 49.0 Ko ou 50 218 octets

Au contraire l'image au format JPEG (JPG) est censé être un format compressé du png donc nous perdons les informations comme le message caché mais le fichier est un peu plus lourd que le PNG. 53.8 Ko contre 49.0 Ko.

Maintenant que nous connaissons un peu plus le procédé stéganographique nous imaginons bien qu'il peut être utilisé à des fins malveillants.

Quelques exemples de ce que l'on peut faire grâce à la stéganographie

Articles du Journal Le Monde Informatique