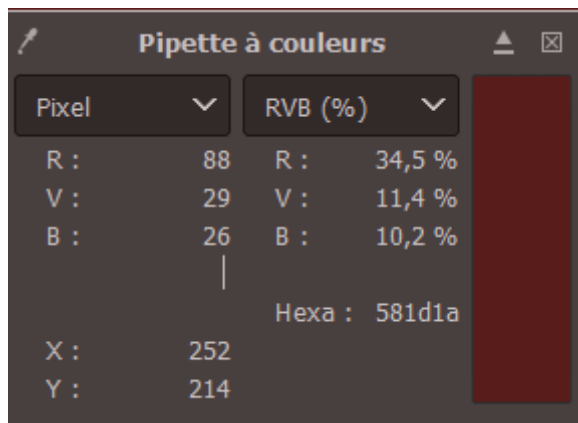


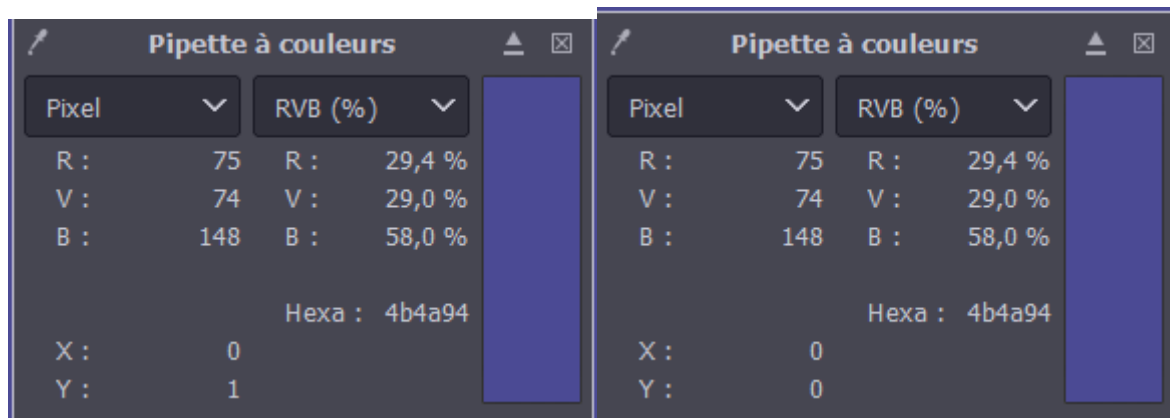
[Couleurs de pixels](#)

La couleur aux ordonné (252,214) en code hexadécimal est 581d1a,

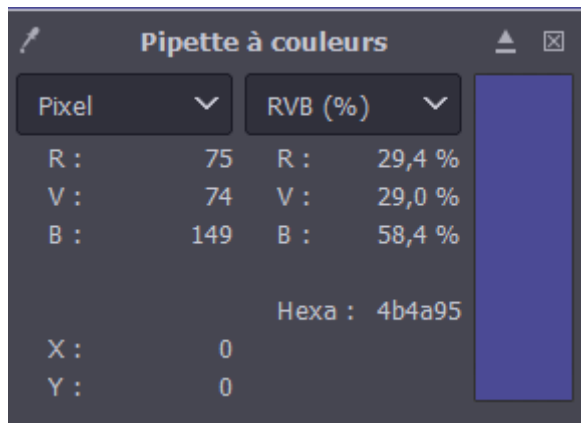
Celui pour le code HTML est #581d1a

[Description du procédé stéganographique](#)

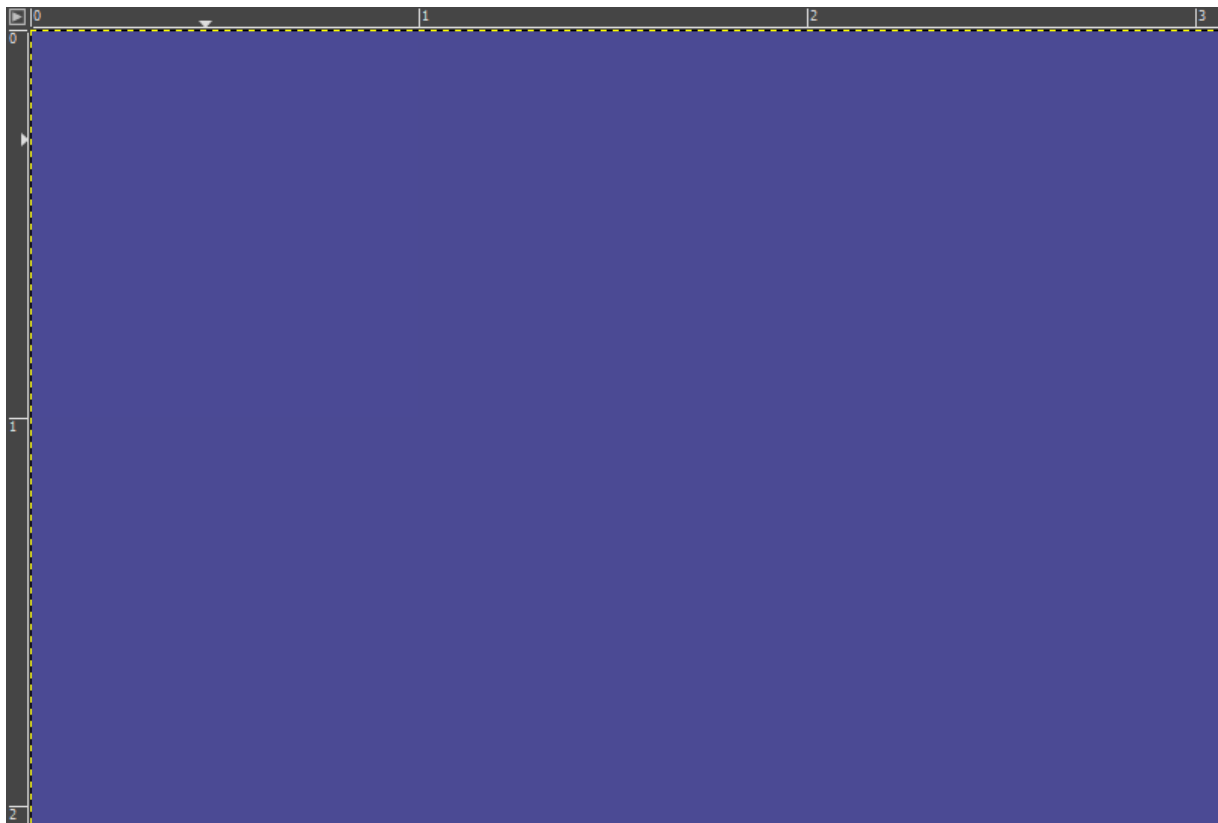
- 1) La couleur des deux pixels est identique pour les coordonnées (0,0) et (0,1)



2) Voici le pixel après avoir rajouté 1 en Bleu



3) On ne voit pas la différence à l'œil entre les pixels (0,0) et (0,1)



[Retrouver le message](#)

Pour trouver la longueur du message on regarde la ligne 0, et l'on regarde le bit de la couleur BLEU,

1) voici les valeurs de composantes bleues,

0.0	1.0	2.0	3.0	4.0	5.0	6.0	7.0
148	148	148	148	148	149	148	148

2) On peut en déduire que le bit faible est 148 et donc le fort et 149.

Ce qui se traduit par 0000 0100, ce qui donne le chiffre 4

La longueur du message est de 4 octets, soit 32 bits

Coordonnée	Valeur bleu	Bits
1.0	148	0
1.1	149	1
2.1	148	0
3.1	149	1
4.1	148	0
5.1	149	1
6.1	148	0
7.1	148	0
8.1	148	0
9.1	149	1
10.1	148	0
11.1	148	0
12.1	148	0
13.1	148	0
14.1	149	1
15.1	148	0
16.1	148	0
17.1	148	0
18.1	149	1
19.1	148	0
20.1	148	0
21.1	148	0
22.1	148	0
23.1	148	0
24.1	148	0
25.1	148	0
26.1	149	1
27.1	148	0
28.1	148	0
29.1	148	0
30.1	148	0

31.1	149	1
------	-----	---

Le code est découvert est 01010100 01000010 00100000 00100001

4) grâce a la table de ASCII voici la traduction du code binaire :

0 101 0100 > T

0 100 0010 > B

0 010 0000 > espace

0 010 0001 > !

Le message est TB !

Dissimuler un message

[Choix du format de sauvegarde du fichier](#)

1) Voici la photo au format JPG

Nom	Date	Type	Taille
 stegano-img0	20/10/2024 15:57	Fichier JPG	54 Ko
 stegano-img0	20/10/2024 15:54	GIMP 2.10.38 PNG	48 Ko

2) Une fois l'image chargé, on peut remarquer que tous les pixels sont passés à 149, au niveau des deux premières lignes, le message qui était dissimuler n'existe plus

3) On remarque que l'image d'origine qui est au format PNG fait 48ko, l'image qui est au format JPG fait 54ko, on remarque que lorsque l'on enregistre sur le JPG le fichier prend 6ko, cela provient de la compression qui ce fait avec perte.

4) après avoir testé avec JPG, BMP, PNG, GIF, TIF, PDF, EPS, ICO et HEIF. On peut dire que cela fonctionne avec presque tous les formats, sauf avec JPG et HEIF et pour ICO cela fonction, mais le message caché et décalé comparé à celui d'original.

Vers l'infini et au-delà

Il existe plusieurs types de stéganographie, les 5 principaux types que l'on peut utiliser pour en faire son du texte, de l'image, de la vidéo, de l'audio et du réseau.

Les dernières attaques connues sont une attaque qui a ciblé le personnel militaire ukrainien via des courriels d'hameçonnage en ce faisant passer pour d'autre militaire afin de transmettre un cheval de Troie, une autre attaque a été dissimulé au sein de fichiers Word qui lors de son ouverture déclenche le téléchargement d'un VBS qui lui-même déclenche d'autre téléchargement derrière comme une photo ainsi que de logiciels malveillants.

La stéganographie consiste à dissimuler une information dans une image, un texte ou bien sur d'autre support, comme on n'a pu constater dans ce TP en modifiant 1 bit sur la couleur bleu on peut y mettre un message sans que l'on puisse le remarquer car la différence, de plus presque tous les formats photo permettent de dissimulé un message sans qu'il soit effacer.