

TP Stéganographie

TIAGO GOMES

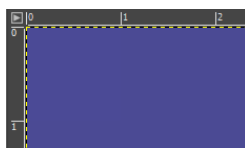
*****Dans cet exercice le professeur souhaite nous introduire à la méthodologie et à l'utilisation de la Stéganographie, au travers de recherches, de manipulations et de l'élaboration d'une trace écrite. Pour suivre ce compte rendu, le support fourni par le professeur est nécessaire. On entreprend ce travail grâce à un exercice simple qui consiste à trouver la valeur en hexadécimal de la couleur d'un pixel donnée.*****

Couleur d'un pixel :

Au travers de l'exercice et grâce aux informations fournies j'ai pu trouver pour le pixel 252,214 la couleur 581d1a en html/hexa grâce à l'outil pipette du logiciel GIMP.

Description du procédé de stéganographie :

Comme on peut le voir dans ces captures d'écran (prise avec Share X) le pixel aux coordonnées (0,0) est bel et bien différent de son voisin le pixel (0,1) on peut l'observer grâce au code hexa différent sur les deux échantillons obtenus avec l'outil pipette.



Mais quand on l'observe à l'œil nu sur cette deuxième capture d'écran, les couleurs semblent exactement pareilles malgré leur différence colorimétrique. Cette différence nous sera utile plus tard au cours de ce devoir.

Retrouver un message :

Nombre de caractères :

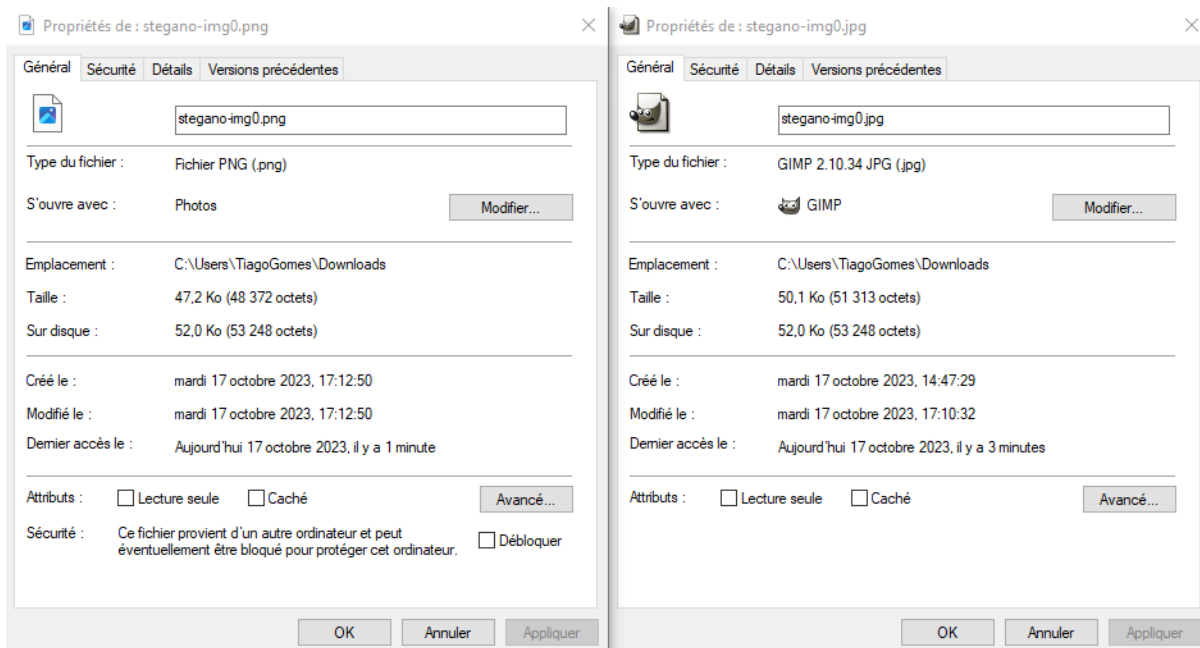
- 148 (en binaire donne 10010100) = 0
- 149 (en binaire donne 10010101) = 1
- 94-94-94-94 95-94-94-94
= 0000 0100 = 4 Caractères
- 4*8 = 32 octet à piocher dans la ligne (1,0)-(1-31)

1^{er} : 0101 0100 = en décimal (84) = T
2^{ème} : 0100 0010 = en décimal (66) = B
2^{ème} : 0010 0000 = en décimal (32) = Un espacement
4^{ème} : 0010 0001 = en décimal (65) = !

Comme vu précédemment la différence entre les deux couleurs ne se voit pas à l'œil nu, ce qui nous permet de cacher des informations dans ce fameux code couleur, ci-dessous j'explique comment grâce au devoir j'ai pu trouver une information dissimulée dans une image. Ci-dessus, de manière très synthétique, nous avons ma méthode de recherche. Pour commencer, j'ai suivi les consignes du devoir en récoltant les valeurs de la couleur bleue comme demandé, celle-ci variait entre (148 et 149). En la convertissant en binaire et en prenant l'octet le plus faible (le dernier octet), nous pouvions associer 148 à 0 et 149 à 1. Traduction faite du binaire en texte, de la suite d'octets, le résultat obtenu est 4 (le nombre de caractères), en suivant la consigne, on comprend que l'on devait multiplier 4 par 8 pour obtenir le bon nombre de pixels (32) qui une fois interprétés en octets nous donnaient le mot caché. Un tableau sur une page Wikipédia fourni par le tp me permettait de faire la conversion mais j'ai préféré utiliser un site de traduction ([Pour lien cliquer ICI](#)) de binaire en lettres, afin d'aller plus vite. D'après la norme ASCII on trouve en convertissant en valeur décimale puis en lettres le message suivant : TB !

Choix du format de sauvegarde du fichier :

Octet trouvé : 0000 0000 (ce qui n'est pas le même qu'avant)



Le fichier voit sa taille augmenter. On peut déterminer que des données ont changé dans celui-ci.

Tout format d'image contenant des informations sur la colorimétrie d'un pixel peut être utilisé dans le cas de la sténographie. Le paramètre qui change réellement est la difficulté à décrypter le message. Par exemple, en bitmap (.bmp) l'image est en noir et blanc on peut donc déterminer que le noir est 0 et le blanc est 1 en code binaire. D'autres formats peuvent

toujours être utilisés mais la façon d'y intégrer nos données devra être revue pour être adaptée à celui-ci.

Vers l'infini et au-delà et conclusion :

*****La stéganographie est présente un peu partout autour de nous, comme dans les méthodes gestuelles de communication militaire qui permettent aux soldats de transmettre des informations et des ordres aux autres soldats sans être compris par les personnes non concernées. Comme la stéganographie est partout autour de nous, on la trouve aussi dans notre domaine, l'informatique, tout élément que notre ordinateur peut lire, peut techniquement contenir des valeurs cachées. Un exemple récent tiré d'un site de prestataire informatique (<https://www.ipe.fr/>), le ransomware SyncCrypt est parfait car il illustre une utilisation récente de la stéganographie. Ce ransomware se trouve dans de faux mails que l'on vous envoie (SPAM), souvent avec un fichier à télécharger, dès lors que vous avez cliqué sur le fichier ou exécuté celui-ci un programme/script caché commencera à crypter toutes vos données en vous demandant une rançon pour pouvoir espérer les récupérer. C'est dans ce genre de cas que la stéganographie est utilisée à mauvais escient, on doit donc mettre en place des protocoles de sécurité pour protéger les utilisateurs de ces éventuelles attaques.*****