Hack'in Trégor – Cryptographie et stéganographie sur images

Club Cyber ENSSAT

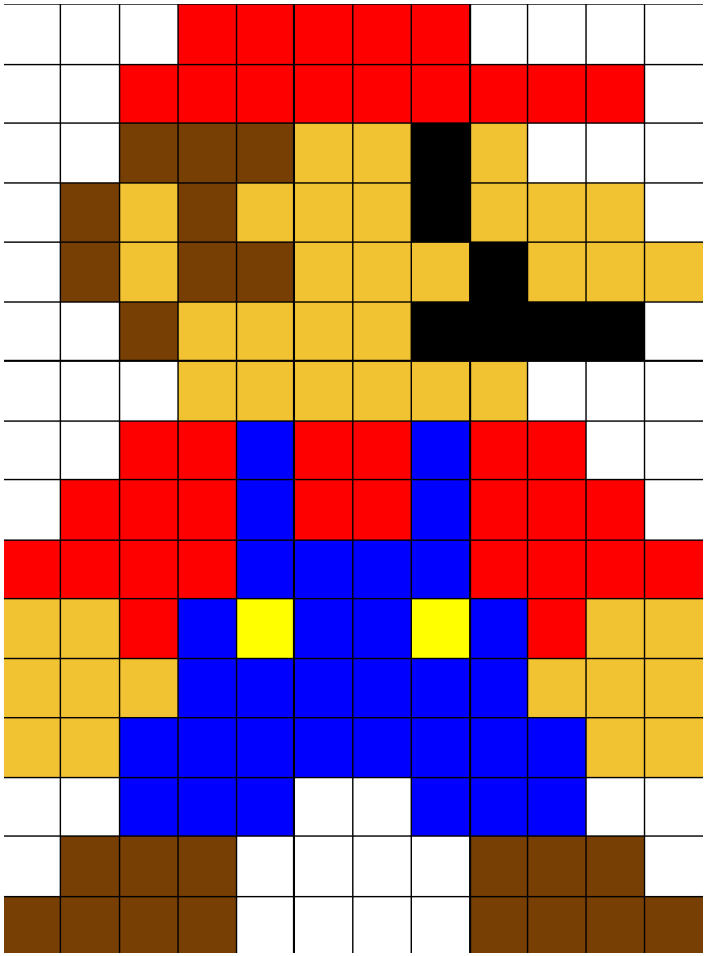
24 octobre 2024

Table of contents

Plan

Comment voir une image ?

C'est une matrice de pixels.



(Rouge, Vert, Bleu)

(255,0,0)	(0,0,255)	(0,0,255)
(0,0,255)	(255,255,0)	(0,0,255)
(0,0,255)	(0,0,255)	(0,0,255)

Plan

Principe du `xor`

Table de vérité du `xor`

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

C'est le *ou exclusif* : un dessert *ou* l'autre, mais pas les deux !

Propriétés du xor

Table de vérité du `xor`

Si

$$c = m \oplus k$$

alors on peut retrouver m à partir de k et c :

$$m = c \oplus k$$

Explication :

Dans la table de vérité du `xor`, on remarque que, pour $a \in \{0, 1\}$, $\boxed{a \oplus a = 0}$ et $\boxed{0 \oplus a = a}$, d'où :

$$\begin{aligned} c \oplus k &= (m \oplus k) \oplus k \\ &= m \oplus (k \oplus k) \\ &= m \oplus 0 \\ &= m \end{aligned}$$

Xor entre entiers

Exemple : $10 \oplus 44$

On convertit en binaire :

$$\begin{aligned} 10 &= 1010_2 \\ 44 &= 101100_2 \end{aligned}$$

Puis on effectue le `xor` bit à bit :

$$\begin{array}{cccccccc} & 0 & 0 & 1 & 0 & 1 & 0 \\ \oplus & 1 & 0 & 1 & 1 & 0 & 0 \\ \hline = & 1 & 0 & 0 & 1 & 1 & 0 \end{array}$$

On obtient $100110_2 = 38_{10}$.

Xor entre images

Principe

On `xor` les pixels entre eux :

$$\underbrace{(r_1, g_1, b_1)}_{\text{pixel image 1}} \oplus \underbrace{(r_2, g_2, b_2)}_{\text{pixel image 2}} = \underbrace{(r_1 \oplus r_2,\ g_1 \oplus g_2,\ b_1 \oplus b_2)}_{\text{pixel résultat}}$$

Exemple :

$$(255, 70, 0) \oplus (0, 255, 255) = (255, 185, 255)$$

On applique ensuite ceci pour chaque pixel.

Plan

Modification de pixel

Légère modification de la couleur d'un pixel

Si l'on modifie les derniers chiffres d'un pixel :

(60, 100, 220) (68, 108, 228)

Cela ne va pas être visible sur une image à l'œil nu.

Cacher du texte dans un pixel

Comment cacher du texte dans un pixel ?

- Message : `Lorem ipsum`
- Conversion en ASCII :

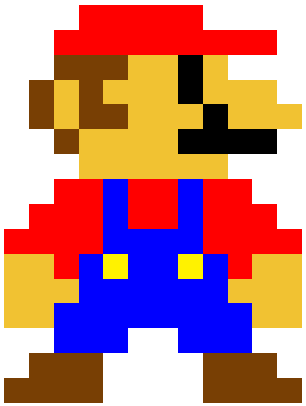
  `[76, 111, 114, 101, 109, 32, 105, 112, 115, 117, 109]`

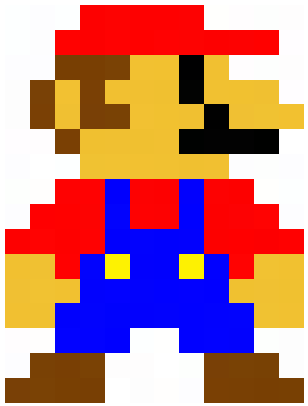
- Modification du dernier chiffre des pixels :

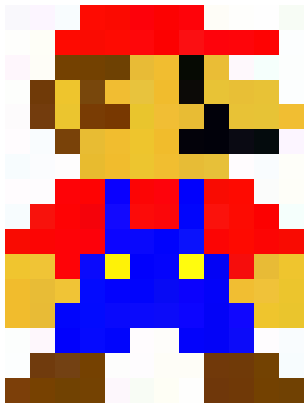
  (67, 106, 221) (61, 101, 221) (61, 104, 221) ...

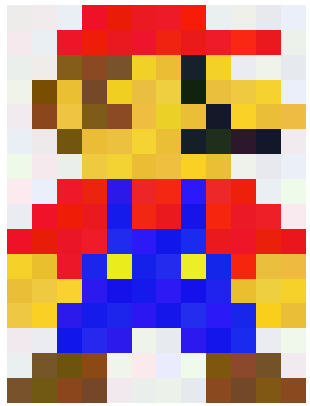
Exemple

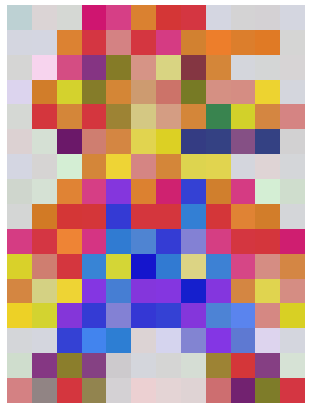
Message : Lorem ipsum dolot sit amet ...


Original


base 2


base 10


base 25


base 100

Merci pour votre attention

Lien vers le code et la présentation sur `github` :

`https://github.com/lasercata/Hack_in_Tregor_CyberClub_demo`