**Security Analysis – Plain-image sensitivity analysis**

On chiffre les trois images Lena en RGB et les trois images Barbara en niveaux de gris avec la même clé.

***RGB-color***



Fichiers :

* : lenaA.tif : (0,0) = {226,137,125}, (255,255) = {185,74,81} ;
* : lenaB.tif : (0,0) = {225,137,125}, (255,255) = {185,74,81} ;
* : lenaC.tif (0,0) = {226,137,125}, (255,255) = {185,74,80} ;

Taille : 256\*256

Format : 32 bits

L = 196 608 (travail sur valeurs de pixel : 3\*256\*256)

 = {21687, 25655, 9043, 10073, 30890, 18491, 15333, 29442, 11211, 27070, 12014, 31349, 15884, 23157, 667, 14650, 21148, 12134, 15404, 4767, 9831, 15703, 31388}

 est obtenue lors du chiffrement de *lenaA.tif*, le reste de l’échantillon est chiffré avec cette clé.

  = {26069, 32096, 29353, 26560, 12185, 12515, 30706, 432, 18597, 1131, 10132, 24923, 5679, 11623, 29205, 17088, 31630, 31712, 14629, 19290, 26783, 16209, 28966}

est obtenue lors du chiffrement de *lenaC.tif*, le reste de l’échantillon est chiffré avec cette clé.

Tables représentant les coefficients de corrélation et les indices NPCR et UACI pour des images presque identiques (1 bits de différent) chiffrées avec la même clé.

**Table 1**

Image ½

Corr. NPCR UACI Corr. NPCR UACI

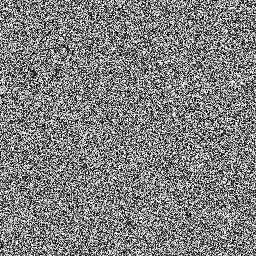
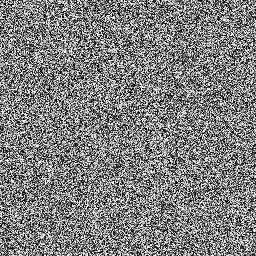
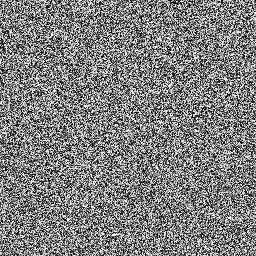
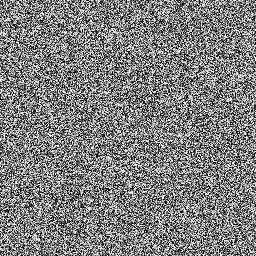
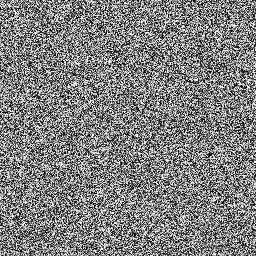
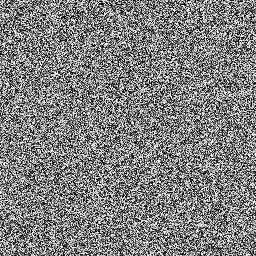
  / 0.0020 99.64 33.51 -0.0021 99.60 33.55

  /   0.0008 99.59 33.42 -0.0024 99.57 33.41

  0.0006 99.61 33.43 -0.0010 99.59 33.43

***Grayscale***

Pour garder le comportement d’une véritable image en niveau de gris, il faut baisser de 1bit les valeurs RGB récupérées.



Fichiers :

* : barbaraA.bmp : (0,0) = {221}, (255,255) = {30} ;
* : barbaraB.bmp : (0,0) = {220}, (255,255) = {30} ;
* : barbaraC.bmp (0,0) = {221}, (255,255) = {29} ;

Taille : 256\*256

Format : 8 bits.

L = 65 536 (travail sur valeurs de pixel : 256\*256)

 = {5181, 25898, 26508, 29850, 30146, 2689, 4108, 20166, 5240, 11767, 4394, 18989, 25147, 20480, 10071, 14351, 6047, 498, 11617, 7053, 12434, 24}

  = {5546, 17303, 28447, 5197, 5731, 16499, 25023, 19991, 19530, 11311, 20597, 23922, 14333, 5893, 5225, 22906, 27774, 32507, 20049, 20376, 13018, 29953}

Tables représentant les coefficients de corrélation et les indices NPCR et UACI pour des images presque identiques (1 bits de différent) chiffrées avec la même clé.

**Table 2**

Image ½

Corr. NPCR UACI Corr. NPCR UACI

  / -0.0017 99.64 33.43 0.0067 99.57 33.28

  /   0.0040 99.59 33.46 0.0017 99.58 33.36

  0.0036 99.63 33.44 0.0087 99.57 33.30

***Echantillons de 100 images***

Echantillon de 100 images en RGB-color, lena.bmp de 24 bits.

 = {21687, 25655, 9043, 10073, 30890, 18491, 15333, 29442, 11211, 27070, 12014, 31349, 15884, 23157, 667, 14650, 21148, 12134, 15404, 4767, 9831, 15703, 31388}

Coef corr = 0.000289, NPCR = 98.613225, UACI = 33.126162 ;

SD coef corr = 0.003653, SD NPCR = 0.991378, SD UACI = 0.343615;

(SD = *σ* = Standard Deviation)

Echantillon de 100 images en grayscale, barbara.bmp de 8 bits.

 = {5181, 25898, 26508, 29850, 30146, 2689, 4108, 20166, 5240, 11767, 4394, 18989, 25147, 20480, 10071, 14351, 6047, 498, 11617, 7053, 12434, 24}

Coef corr = 0.000256, NPCR = 98.612637, UACI = 33.125216 ;

SD Coef corr = 0.004081, SD NPCR = 0.991381, SD UACI = 0.346809 ;

**Table 3**

Indicator Lena RGB-Color Barbara Grayscale

*mL σL mL σL*

Corr. coef. 0.0003 0.0037 0.0003 0.0041

NPCR 98.61 0.99 98.61 0.99

UACI 33.13 0.34 33.13 0.35