



Comment recompresser des images JPEG crypto-compressées ?

Journée ICAR

Vincent Itier

19 *Juillet* 2016

Contexte

Objectifs :

- Transfert images
- Stockage images sur serveur

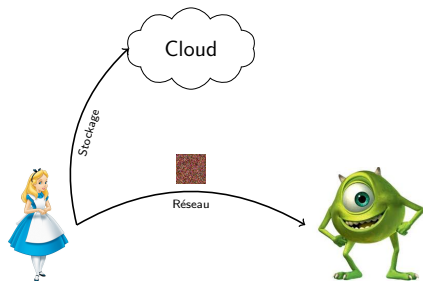
Problèmes :

- 1 Protection données personnelles
- 2 Taille (coût transfert/stockage)

Solutions :

- 1 Chiffrement
- 2 Compression

Crypto-compression !



Contexte

Objectifs :

- Transfert images
- Stockage images sur serveur

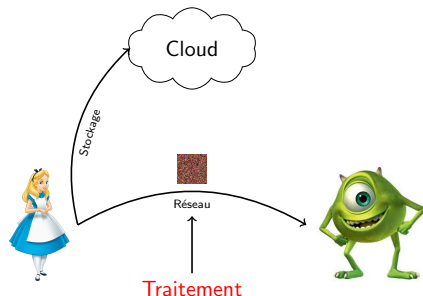
Problèmes :

- 1 Protection données personnelles
- 2 Taille (coût transfert/stockage)

Solutions :

- 1 Chiffrement
- 2 Compression

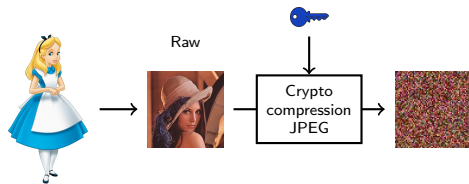
Crypto-compression !



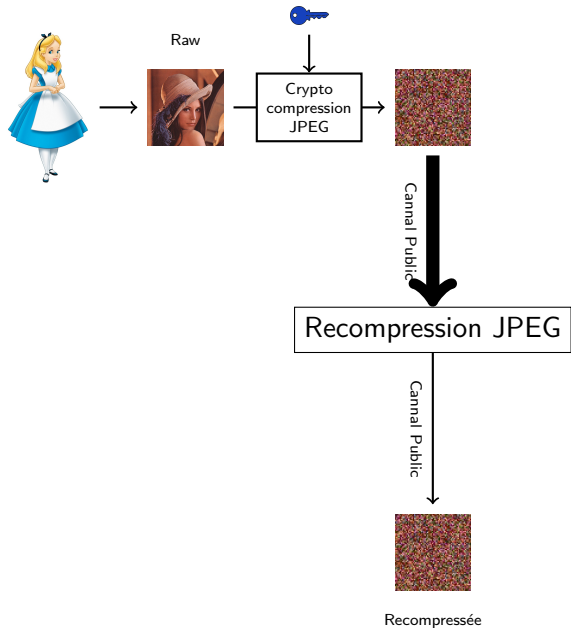
Problème :

- Traitement dans le domaine crypto-compressé

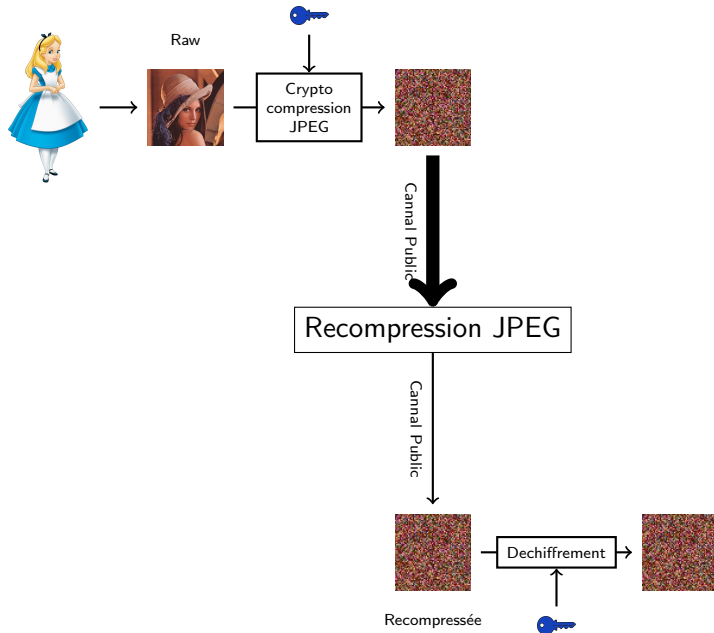
Contexte



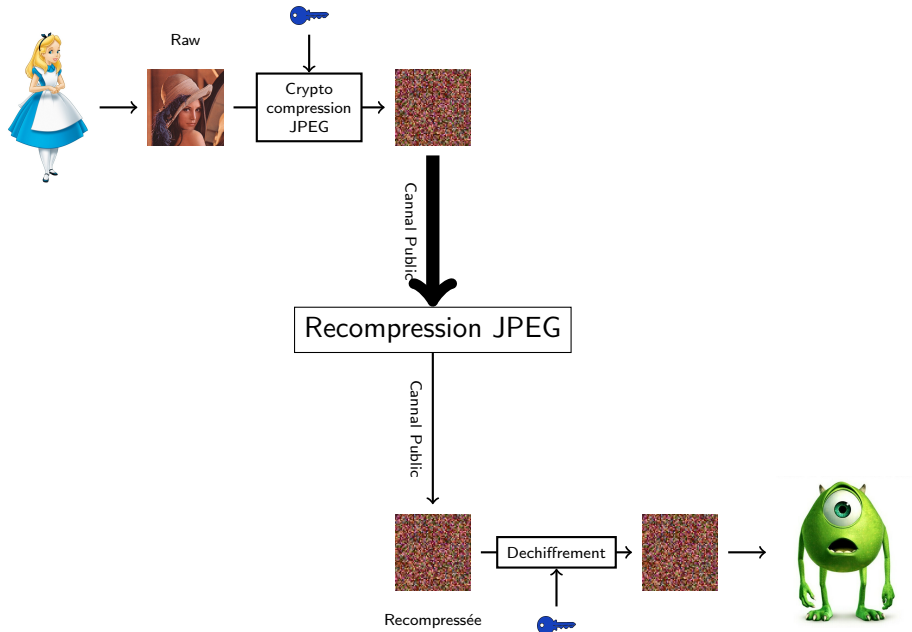
Contexte



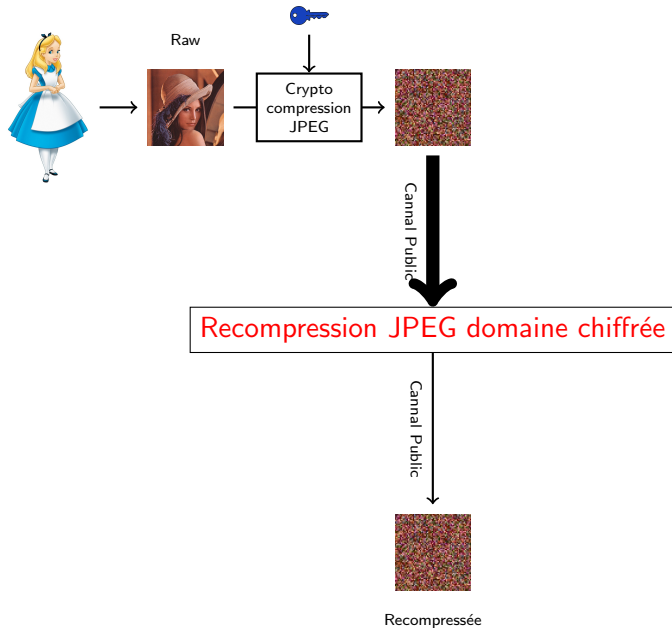
Contexte



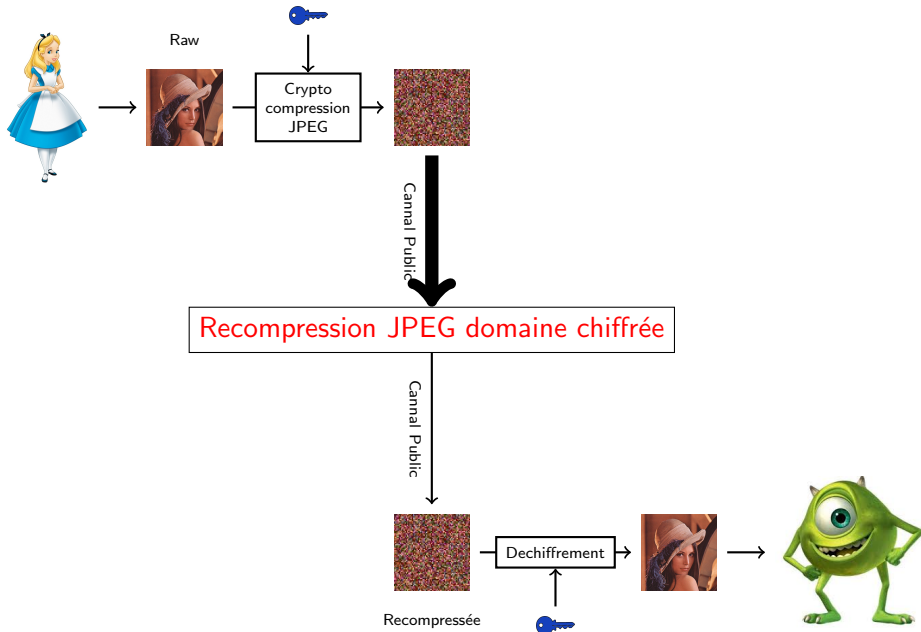
Contexte



Contexte



Contexte



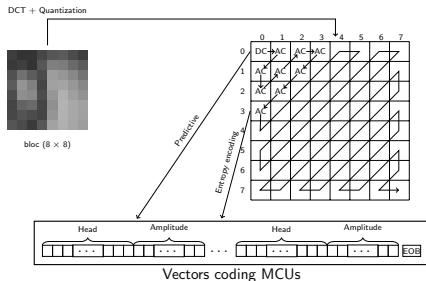
Sommaire

- 1 Contexte
- 2 **Crypto-compression JPEG**
 - Format JPEG
 - Chiffrement JPEG
- 3 Recompression JPEG
- 4 Recompression JPEG crypto-compressées
- 5 Résultats
- 6 Conclusion

Format JPEG

Étapes compression JPEG

- 1 Conversion YUV
- 2 Division en block : 8×8
- 3 Transformée en cosinus discrète (DCT)
- 4 Quantification (perte)
- 5 Codage par plages / Codage entropique



Étapes décompression JPEG

- 1 Décodage
- 2 Déquantification
- 3 Transformée inverse (IDCT)
- 4 Conversion RGB



International Telecommunication Union.

Information technology-digital compression and coding of continuous-tone still images-requirements and guidelines.

CCITT recommendation T.81, 1992

Format JPEG

Coefficients DCT :

$c_{(0,0)}$	$c_{(0,1)}$	$\dots$
$c_{(1,0)}$	$c_{(1,1)}$	
$\vdots$		

Table de quantification :

$q_{(0,0)}^{QF}$	$q_{(0,1)}^{QF}$	$\dots$
$q_{(1,0)}^{QF}$	$q_{(1,1)}^{QF}$	
$\vdots$		

Coefficients quantifiés :

$c'_{(0,0)}$	$c'_{(0,1)}$	$\dots$
$c'_{(1,0)}$	$c'_{(1,1)}$	
$\vdots$		

Quantification (perte):

$$c'_{(u,v)} = \left\lfloor \frac{c_{(u,v)}}{q_{(u,v)}^{QF}} \right\rfloor. \quad (1)$$

Déquantification :

$$\hat{c}_{(u,v)} = c'_{(u,v)} \times q_{(u,v)}^{QF}. \quad (2)$$

Format JPEG

Structure JPEG :

- HEADER :
 - ▶ Tables quantification
 - ▶ Tables de Huffman
- SOS : Données image encodées

Structure d'encodage des coefficients :

- HEAD :
 - ▶ Codage par plage des 0
 - ▶ Taille en bits de l'amplitude
- AMPLITUDE : code valeur

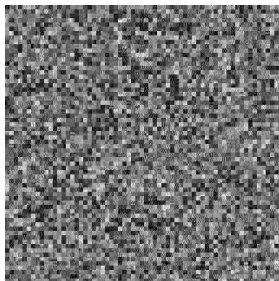
```
ff d8 ff e0-00 10 4a 46-49 46 00 01-01 00 00 01
00 01 00 00-ff db 00 43-00 01 01 01-01 01 01 01
01 01 01 01-01 01 01 01-02 01 01 01-01 01 01 02
02 01 02 03-03 03 03 03-03 03 03 04-04 05 04 04
04 05 04 03-03 05 06 05-05 06 06 06-06 06 03 04
07 07 07 06-07 05 06 06-06 ff db 00-43 01 01 01
01 02 01 02-03 02 02 03-06 04 04 04-06 06 06 06
06 06 06 06-06 06 06 06-06 06 06 06-06 06 06 06
06 06 06 06-06 06 06 06-06 06 06 06-06 06 06 06
00 11 08 02-00 02 00 03-01 22 00 02-11 01 03 11
01 ff c4 00-1f 00 00 01-05 01 01 01-01 01 01 00
00 00 00 00-00 00 00 01-02 03 04 05-06 07 08 09
0a 0b ff c4-00 b5 10 00-02 01 03 03-02 04 03 05
05 04 04 00-00 01 7d 01-02 03 00 04-11 05 12 21
31 41 06 13-51 61 07 22-71 14 32 81-91 a1 08 23
42 b1 c1 15-52 d1 f0 24-33 62 72 92-09 0a 16 17
18 19 1a 25-26 27 28 29-2a 34 35 36-37 38 39 3a
43 44 45 46-47 48 49 4a-53 54 55 56-57 58 59 5a
63 64 65 66-67 68 69 6a-73 74 75 76-77 78 79 7a
83 84 85 86-87 88 89 8a-92 93 94 95-96 97 98 99
9a a2 a3 a4-a5 a6 a7 a8-a9 aa b2 b3-b4 b5 b6 b7
b8 b9 ba c2-c3 c4 c5 c6-c7 c8 c9 ca-d2 d3 d4 d5
d6 d7 d8 d9-da e1 e2 e3-e4 e5 e6 e7-e8 e9 ea f1
f2 f3 f4 f5-f6 f7 f8 f9-fa ff c4 00-1f 01 00 03
01 01 01 01-01 01 01 01-01 00 00 00-00 00 00 01
02 03 04 05-06 07 08 09-0a 0b ff c4-00 b5 11 09
02 01 02 04-04 03 04 07-05 04 04 00-01 02 77 00
01 02 03 11-04 05 21 31-06 12 41 51-07 01 71 13
22 32 81 08-14 42 91 a1-b1 c1 09 23-33 52 60 15
62 72 d1 0a-16 24 34 e1-25 f1 17 18-19 1a 26 27
28 29 2a 35-36 37 38 39-3a 43 44 45-46 47 48 49
4a 53 54 55-56 57 58 59-5a 63 64 65-66 67 68 69
6a 73 74 75-76 77 78 79-7a 83 84 85-86 87 88 89
89 8a 92 93-94 95 96 97-98 99 9a a2-a3 a4 a5 a6
a7 a8 a9 aa-b2 b3 b4 b5-b6 b7 b8 b9-ba c2 c3 c4
c5 c6 c7 c8-c9 ca d2 d3-d4 d5 d6 d7-d8 d9 da e2
e3 e4 e5 e6-e7 e8 e9 ea-f2 f3 f4 f5-f6 f7 f8 f9
fa ff da 00-0c 03 01 00-02 11 03 11-00 3f 00 eb
e4 93 c9 1f-bb 7c 7d c8-7e 5f f6 0e-57 f9 0b da
b9 ad 5a 58-2e fe dd ba-46 df b7 64-3e 5f c8 14
7d 06 95 4d-3d f1 58 b7-c7 c3 6c d8-07 5d ae e3
6e 5f d3 03-d2 b9 c8 ab-9a e1 0e e2-58 c2 9a e7
ec e7 9e bf-e2 bf 95 7f-03 46 85 f5-67 fa c5 4e
a4 9c ac 78-e7 8f 20 91-ed ef 51 1e-61 92 c8 b9
ad c7 96 31-39 bf 43 76-f4 43 36-bf 34 3e 99
ac 22 79 ea-09 c2 da f9-92 43 ba 34-0b 26 d0 22
50 38 e3 a3-1f e1 ef 5f-a5 3e 34 f3-64 b1 b9 58
ee 12 02 d2-a4 c4 4d 29-7c b2 47 3c-6a 71 81 d3
```

⋮
⋮

État de l'art



Xor



Shuffle

Méthodes

- Xor
 - + Préservation de la taille
 - Chiffrement partiel
- Shuffle
 - Pas de préservation de la taille
 - + Chiffrement incompréhensible



J. M. Rodrigues, W. Puech, and A. G. Bors.

Selective encryption of human skin in jpeg images.
International Conference on Image Processing, pages 1981–1984, 2006



W. Li and Y. Yuan.

A leak and its remedy in jpeg image encryption.
International Journal Computational Mathematics, 84(9):1367–1378, 2007.

Sommaire

- 1 Contexte
- 2 Crypto-compression JPEG
 - Format JPEG
 - Chiffrement JPEG
- 3 Recompression JPEG
- 4 Recompression JPEG crypto-compressées
- 5 Résultats
- 6 Conclusion

Problème : Recompression JPEG



Raw

Problème : Recompression JPEG



Raw → JPEG 75%
compression 75%

Problème : Recompression JPEG



Raw



JPEG 75%



JPEG 50%

recompression 50%

Problème : Recompression JPEG



Raw



JPEG 75%



JPEG 50%

compression 50%



JPEG 50%

Problème de requantification JPEG :

- Trouver la matrice de quantification minimisant les erreurs en fonction du facteur de qualité



S. Chan.

The Use of the JPEG Image Compression Standard and the Problem of Recompression.
Ph.D. dissertation, University of Kent, Canterbury, U.K., 1992.



H. H. Bauschke, C. H. Hamilton, M. S. Macklem, J. S. McMichael, and N. R. Swart.

Recompression of jpeg images by requantization.
IEEE Transactions on Image Processing, 12(7):843–849, 2003.

Domaine chiffré :

- Après recompression déchiffrement impossible

Sommaire

- 1 Contexte
- 2 Crypto-compression JPEG
 - Format JPEG
 - Chiffrement JPEG
- 3 Recompression JPEG
- 4 Recompression JPEG crypto-compressées
- 5 Résultats
- 6 Conclusion

Méthode proposée

Recompression :

- Suppression du bit de poids faible de l'AMPLITUDE (division par 2)

$$c_{(u,v)}^* = \left\lfloor \frac{c'_{(u,v)}}{2} \right\rfloor. \quad (3)$$

- Multiplication par 2 des coefficients de la table de quantification

$$q_{(u,v)}^* = q_{(u,v)}^{\text{QF}} \times 2. \quad (4)$$

Adaptation Crypto-compression :

- Chiffrement par une méthode de l'état de l'art
- Tables de quantification coefficients pairs

Recompression

Problème Xor :

- Savoir quels bits de la séquence aléatoire ne sont plus utilisés
 - ▶ Pas de chiffrement des coefficients de taille 1

Problème :

- Requantification fausse si coefficients impairs

Table de quantification

	0	1	2	3	4	5	6	7
0	16	11	10	16	24	40	51	61
1	12	12	14	19	26	58	60	55
2	14	13	16	24	40	57	69	56
3	14	17	22	29	51	87	80	62
4	18	22	37	56	68	109	103	77
5	24	35	55	64	81	104	113	92
6	49	64	78	87	103	121	120	101
7	72	92	95	98	112	100	103	99

T_{50}

	0	1	2	3	4	5	6	7
0	16	16	16	16	32	48	48	64
1	16	16	16	16	32	64	64	48
2	16	16	16	32	48	64	64	64
3	16	16	16	32	48	80	80	64
4	16	16	32	64	64	112	96	80
5	32	32	48	64	80	112	112	96
6	48	64	80	80	96	128	128	96
7	80	96	96	96	112	96	96	96

P_{50}

$p_{(0,0)}^{QF'}$	1	2	4	8	16	32	64
$QF' \simeq$	98%	95%	89%	76%	51%	27%	15%

Diagram illustrating the quantization factor (QF') and its corresponding percentage values for different quantization levels (0 to 7). Red arrows and labels indicate the relationship between the quantization factor and the percentage values:

- From 1 to 2: $/2$
- From 2 to 4: $/2$
- From 4 to 8: $/2$
- From 8 to 16: $/2$
- From 16 to 32: $\times 2$
- From 32 to 64: $\times 2$

Recompression JPEG d'images crypto-compressées

Coefficient DCT :

-435	160	...
125	17	
⋮		

Table de quantification :

1	3	...
3	3	
⋮		

Coefficient quantifié : $\left\lfloor \frac{160}{3} \right\rfloor = 53$

Recompression

R/S	(Huffman code)	Amplitude	(binary)	# bits
0/6	1111000	53	110101 1	13
0/5	11010	26	11010	10

Coefficient DCT : $26 \times (2 \times 3) = 156$

Sommaire

- 1 Contexte
- 2 Crypto-compression JPEG
 - Format JPEG
 - Chiffrement JPEG
- 3 Recompression JPEG
- 4 Recompression JPEG crypto-compressées
- 5 Résultats
- 6 Conclusion

Recompression JPEG d'images crypto-compressées



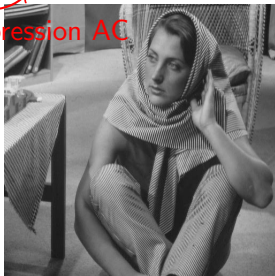
Raw image 257Ko

Recompression JPEG d'images crypto-compressées



Raw image 257Ko → JPEG 76% 45.9Ko

crypto-compression AC



Recompression JPEG d'images crypto-compressées



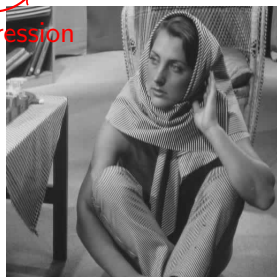
Raw image 257Ko



JPEG 76% 45.9Ko



JPEG 51% 26.5Ko



recompression

Qualité de la Recompression JPEG

JPEG classique :

JPEG 76%



41.1 Ko

JPEG 51%



23.7 Ko

Méthode proposée :



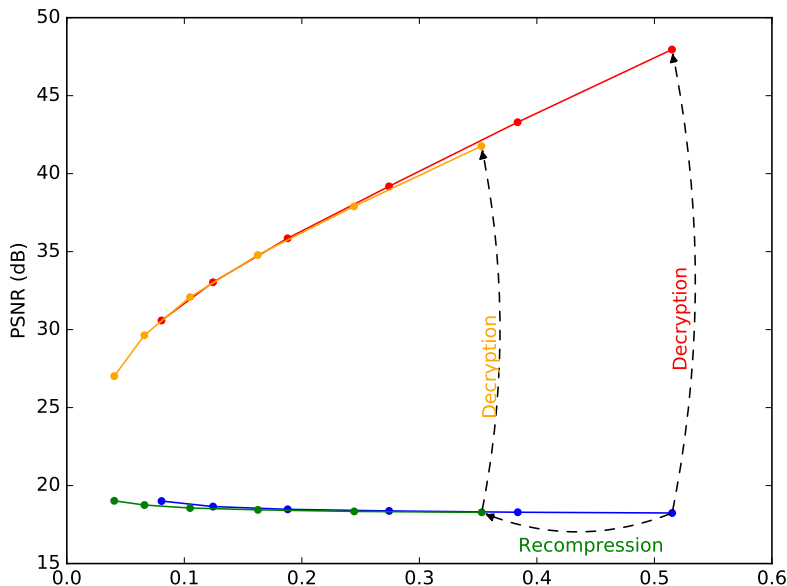
43.9 Ko



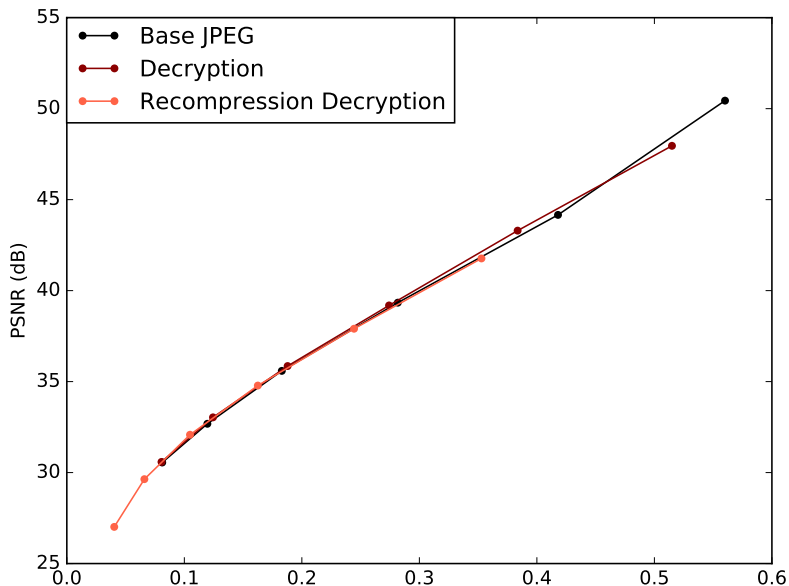
20.2 Ko

recompression

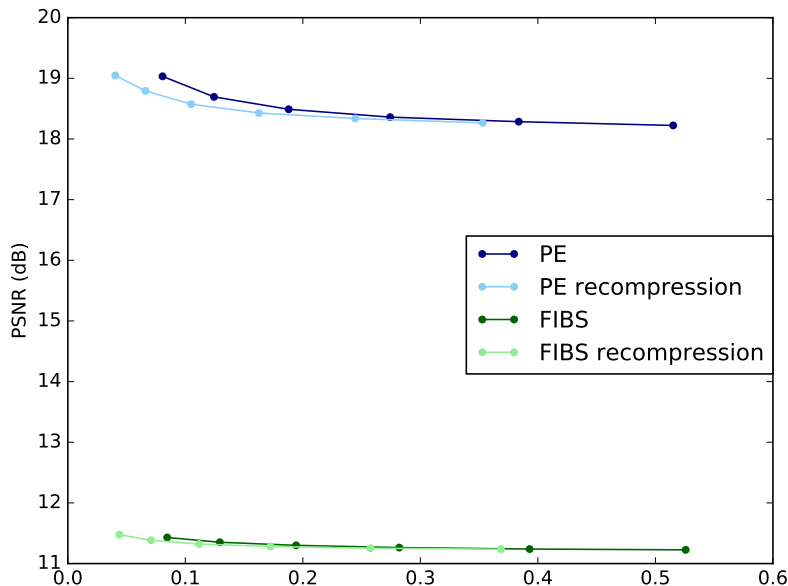
Recompression JPEG d'images crypto-compressées



Recompression JPEG d'images crypto-compressées

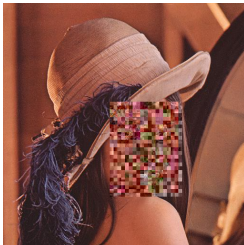


Recompression JPEG d'images crypto-compressées



Crypto-compression sélective et recompression

JPEG 76%

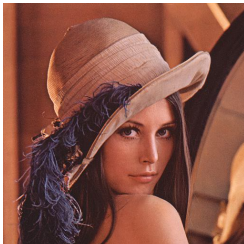


44.1 Ko

JPEG 51%



20.4 Ko



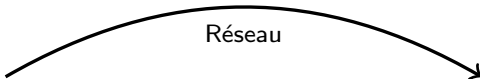
43.9 Ko



20.2 Ko



Réseau



Conclusion :

- Recompression comparable à la simple compression JPEG
- Chiffrement : Sélectif, Partiel, Complet

Perspective :

- Plusieurs recompressions