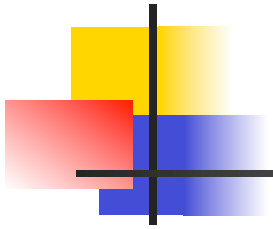
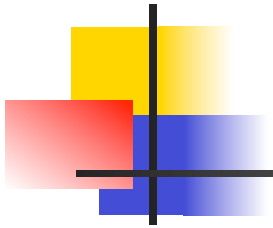


Plan du Cours

1. Introduction
2. Outils mathématiques de base
3. Stratégie de compression
4. Transformée
5. Quantification
6. Codage (cf cours CDCCE (TRS))
7. Compression d'images fixes : de JPEG à JPEG2000
8. Compression de vidéos : de MPEG I à MPEG IV
9. Transmission de documents confidentiels et sécurité



Historique

Recherches et Normes en Compression d'images

- 1964 FFT Transformée de Fourier Discrète
- 1974 DCT Transformée en cosinus discrète
- 1990-92 DWT Ondelettes Bi-orthogonales
- 1992 Norme JPEG
- 2000 Norme JPEG 2000

JPEG (Joint Picture Expert Group)

Objectifs :

⇨ Comprimer des images fixes (couleur ou niveaux de gris)

- Normalisation en 1992 par deux groupes d'experts : ISO[1] et CCITT[2]
- Version **avec pertes** (JPEG - 1992) ou **sans pertes** (JPEG LS - 1998)
- Version pour image avec un nombre limité de niveaux (JBIG)
- Qualité d'image réglable

Principales applications :

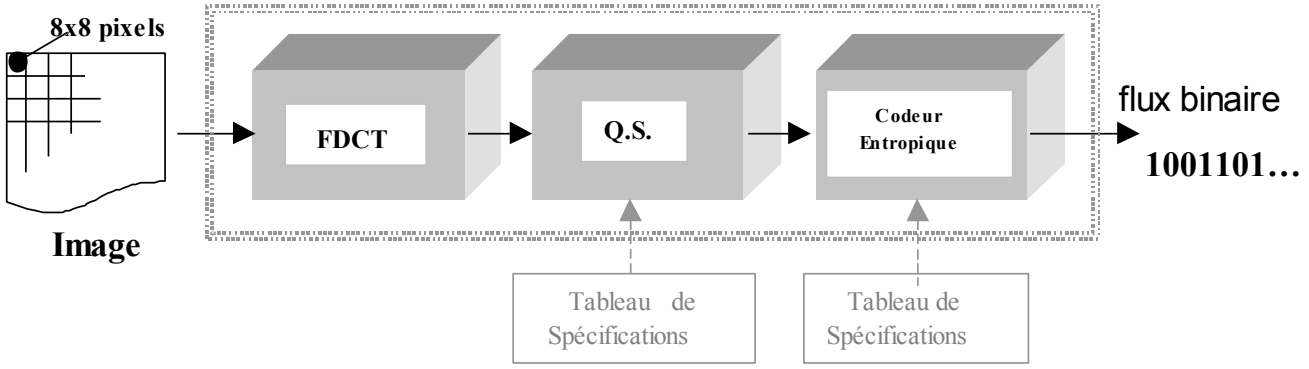
⇨ Fax, imprimantes, Internet, appareils photos numériques,…

1- International Standard Organisation

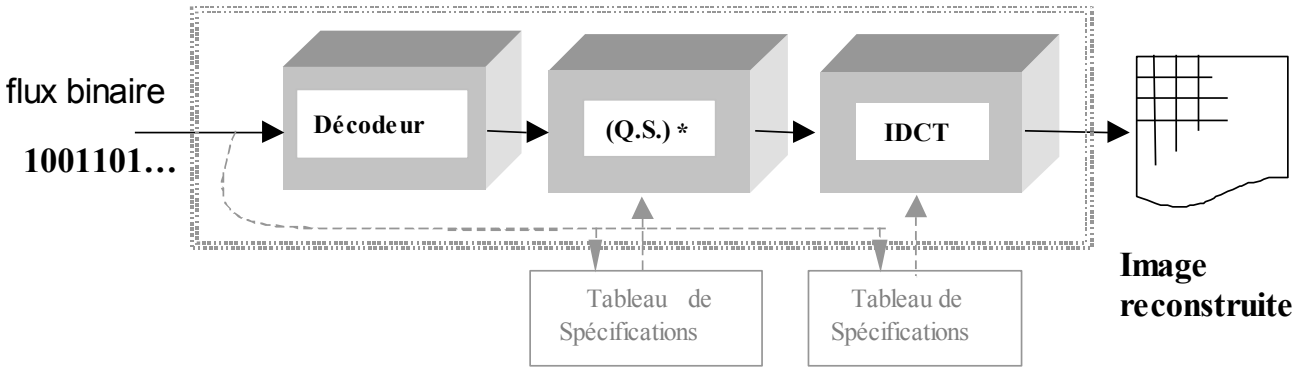
2- Comité Consultatif International Télégraphique et Téléphonique

JPEG : Principe

CODEUR



DECODEUR



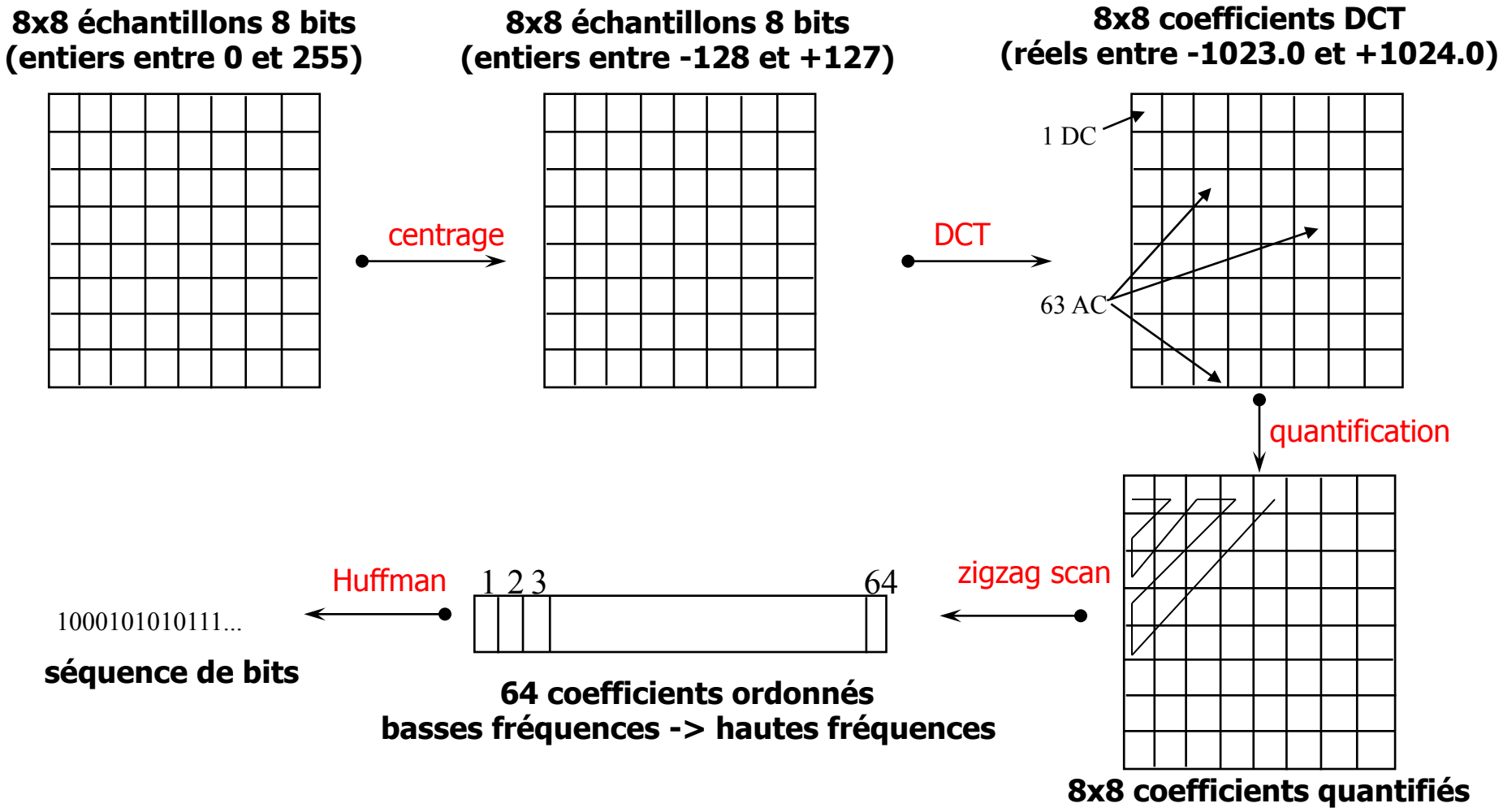
Performances (taux de compression / qualité) :

Images couleur : jusqu'à 50:1 -> peu de dégradation

Images niveaux de gris : au-delà de 20:1 -> dégradations visibles

JPEG : Principe

Traitement JPEG sur chaque bloc 8x8 d'une image :



Quelques Résultats

Image d'origine

Quelques Résultats

TC = 10:1

Quelques Résultats

TC = 20:1

Quelques Résultats

TC = 30:1

Quelques Résultats

TC = 40:1

Quelques Résultats

TC = 60:1

Quelques Résultats

TC = 80:1

Quelques Résultats

TC = 120:1

Avantage Et Inconvénients

- **AVANTAGE** : Gros succès de JPEG
  - 80% des images sur le web seraient encodées JPEG ;
  - Appareils photos numériques.

- **MAIS** :
  - Efficacité de codage limitée ;
  - Effets visuels de blocs à forte compression ;
  - Les applications d'imagerie demandent de nouvelles fonctionnalités non supportées par JPEG.

- Souhait du comité JPEG de définir une nouvelle norme pour répondre à ces 3 problèmes : **JPEG 2000**.

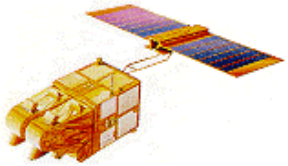
Le Futur : JPEG 2000

Critères exigés (« requirements ») :

- Excellent rapport distorsion / débit (30% « meilleur » que JPEG)
- Gestion de 2 à 16 millions de couleurs sur la même architecture ;
- Compression avec ou sans pertes ;
- Transmission progressive par résolution et par raffinement ;
- Faible complexité algorithmique (euh !!!) ;
- Accès aléatoire dans le fichier compressé pour extraction de régions ; d'intérêt (ROI - Regions Of Interest) ;
- Robustesse aux erreurs de transmission ;
- Protection des informations pour l'exploitation correcte de l'image.

Le Futur : JPEG 2000

Applications visées par JPEG 2000



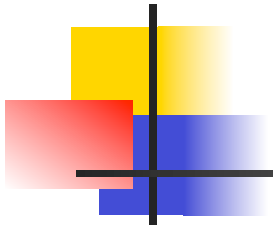
- Internet
- Appareils photo numériques
- Imprimantes
- Scanners
- Télécopie
- Images médicales
- Télécommunications mobiles
- Images Satellites

Processus De Normalisation

- Projet défini en 1996 ;
- Appel à contribution lancé en Mars 1997 ;
- 22 algorithmes candidats sont présentés ;
- Tests objectifs (mesure qualité) et subjectifs (visuels).

Structure de base retenue

1. Transformée en ondelettes (Filtres 9-7)
2. Codeur par plan de bits
3. Codeur Entropique



Processus De Normalisation

- En décembre 1999 : « Working Draft » ;
- « Committee Draft » adopté en mars 2000 ;
- Version finale (« International Standard ») fin 2000.

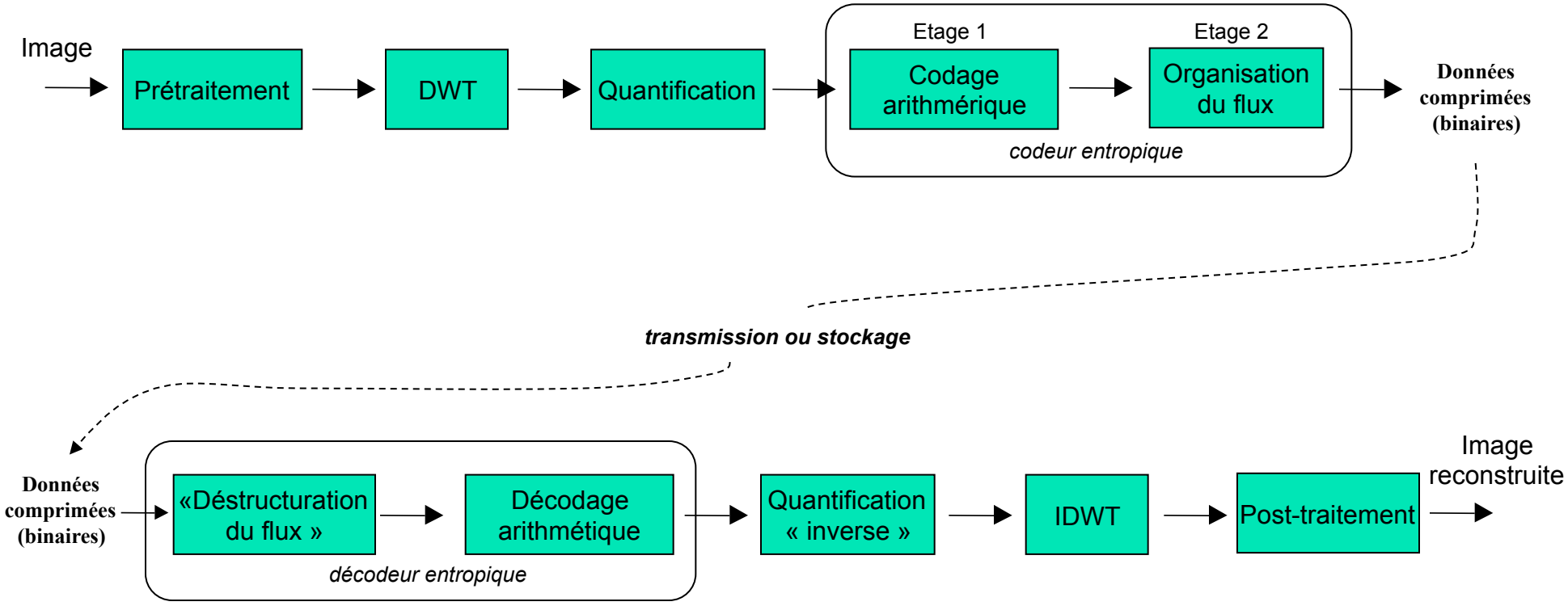
Qu'est-ce qui est normalisé ?

- Seuls la syntaxe et le décodeur sont normalisés ;
- Le codeur est seulement informatif.

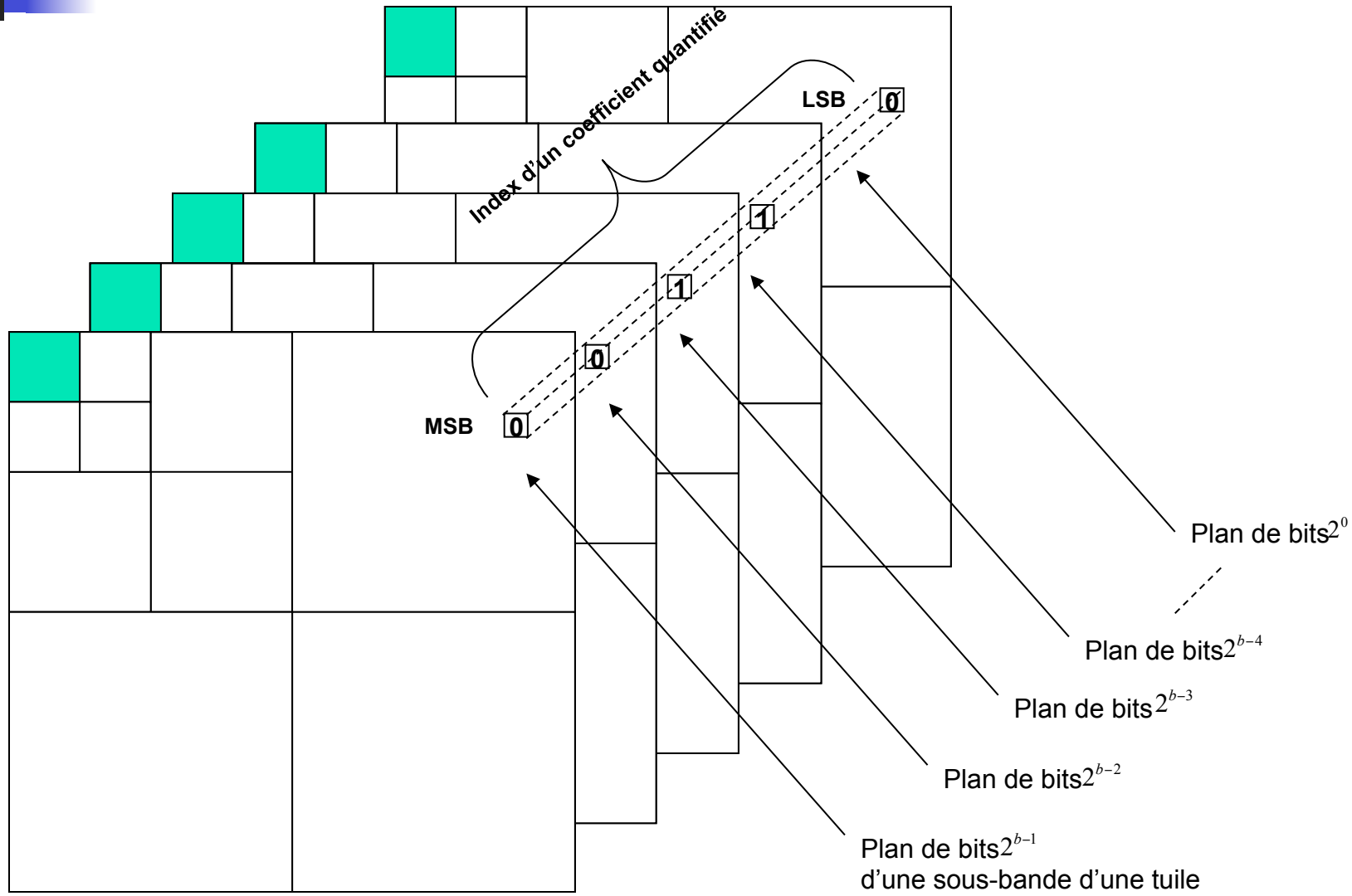
Caractéristiques De JPEG 2000

- Gestion :
  - des images multi-composantes (ex.: couleur) ;
  - des dynamiques de 1 à 32 bits ;
- Découpage de l'image en « tuiles » et transformation de chaque « tuile » ;
- Choix de transformées en ondelettes (lifting ou convolution). Filtres pré-implémentés ou utilisateurs ;
- Multirésolution : Nombre de niveaux de décomposition variable et choix de l'arbre de décomposition ;
- Codage par blocs uniformes de 64x64 coefficients transformés.

JPEG 2000 : schéma



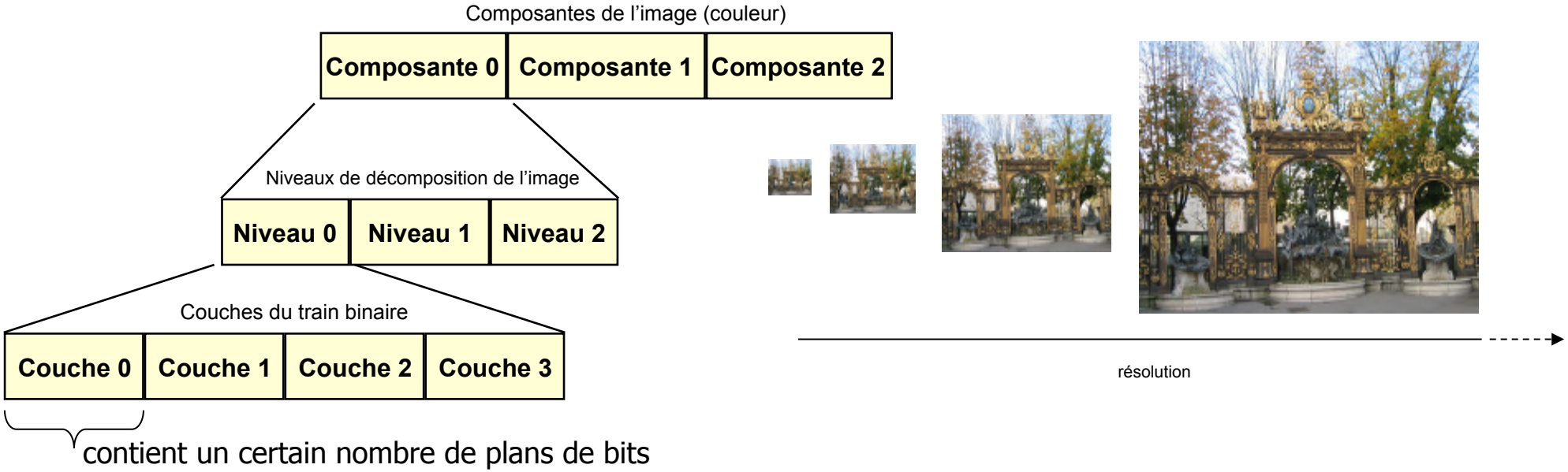
JPEG 2000 : plans de bits



Organisation du train binaire

Etage 2

« Résolution Progressive »

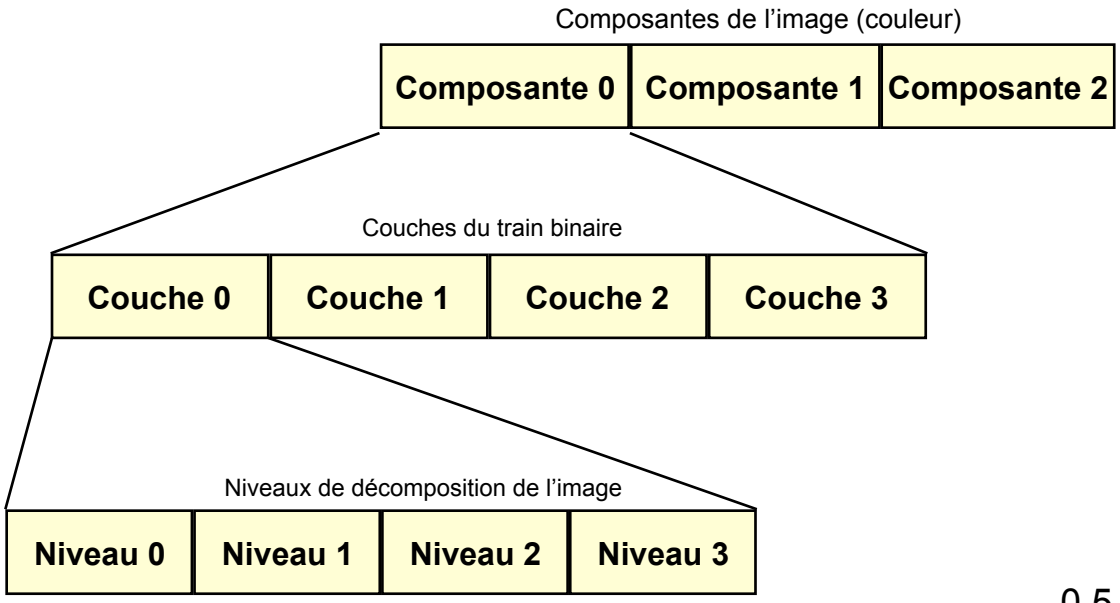


contient un certain nombre de plans de bits

Organisation du train binaire

Etage 2

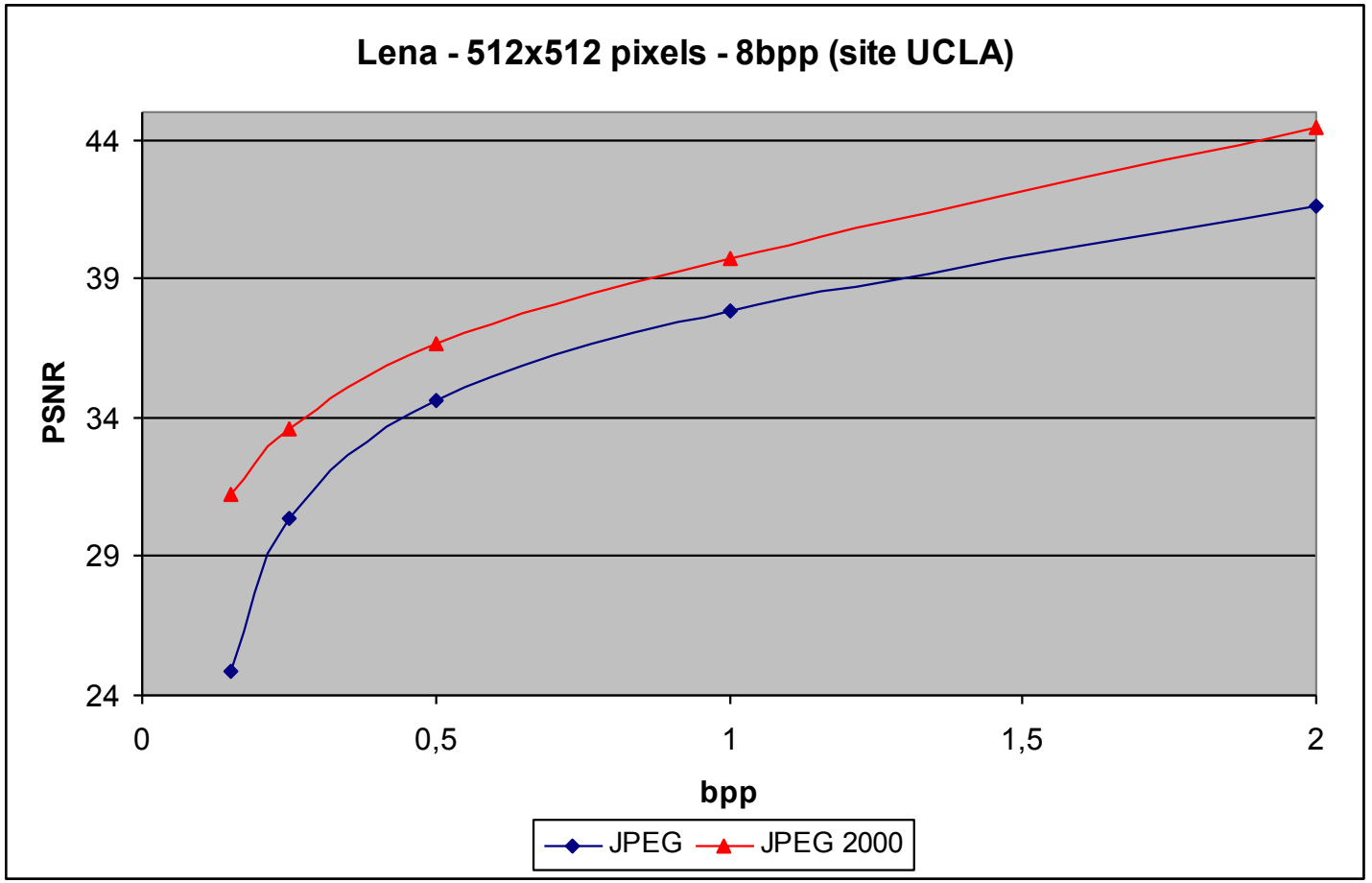
« Qualité progressive »



0,1 bit/pixel

0,5 bits/pixel

JPEG vs JPEG 2000

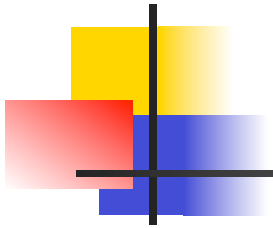


JPEG vs JPEG 2000

JPEG (DCT)

Ondelettes (JPEG-2000)

Taux de Compression 80:1



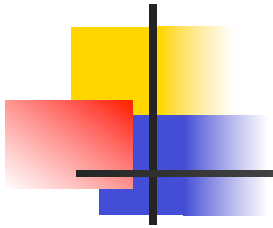
Les Sites Internet

Le site officiel JPEG :

http://www.jpeg.org/

Un modèle de vérification en JAVA est disponible à l'adresse :

http://www.jj2000.epfl.ch/



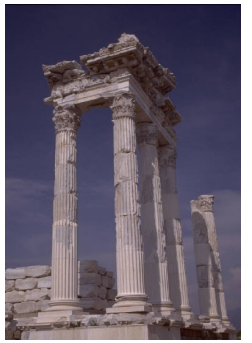
Plan du Cours

1. Introduction
2. Outils mathématiques de base
3. Stratégie de compression
4. Transformée
5. Quantification
6. Codage (cf cours CDCCE (TRS))
7. Compression d'images fixes : de JPEG à JPEG2000
8. Compression de vidéos : de MPEG I à MPEG IV
9. Transmission de documents confidentiels et sécurité

Transmission de documents confidentiels et sécurité

Problème très ancien

transmettre des informations secrètes (militaires), déjouer la censure …



déjà au V^{ème} siècle avant Jésus Christ …

Aujourd'hui

- **Organisation Mondiale de la Propriété Intellectuelle** (près de 200 états membres)
- **cadre particulier de la protection juridique des documents numériques (premier traité signé le 20/12/96)**

protocole de protection des images numériques qui transitent sur Internet

(enregistrement + tatouage)

Transmission sécurisée : les méthodes

Cryptographie

- **transformer un message pour qu'il devienne illisible**
- clé + moyen de cryptage ⟹ décodage

substitution de lettres d'alphabets décalés (Jules César)…algorithme RSA (Internet)

Stéganographie

- **dissimuler un message dans un autre**
- connaissance du procédé de dissimulation ⟹ décodage

pochoirs superposés (ère médiévale)…encre invisible (2nde guerre mondiale) …

Tatouage

- **insérer une signature invisible et indélébile dans une image**
- clé secrète + règle ⟹ décodage

schémas substitutifs, additifs … (années 90)

Cryptographie ancienne

L'exemple du code de César :

substitution monoalphabétique la plus ancienne connue de l'Histoire

Texte clair A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Texte codé D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Texte à coder : ESIAL ouvre ses portes pour les cours d'ouverture.

Texte codé : HVLD0 RXYUH VHV SRUWHV SRXU OHV FRXUV G'RXYHUWXUH.

26 décalages possibles seulement :
code très peu sûr mais très longtemps utilisé (simplicité)

D'après http://www.bibmath.net/crypto/moderne/clepub.php3

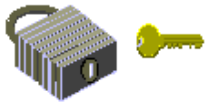
Cryptographie moderne à clé publique

Lorsqu'on ne peut avoir recours à la valise diplomatique …

Algorithme RSA

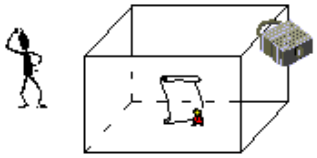
Cryptographie à clé publique :

Etape 1 : Fabrication des clés. Bob fabrique une clé publique qui permet de sceller le message codé dans la boite (ici : le cadenas), et une clé privée qui permet d'ouvrir le cadenas.

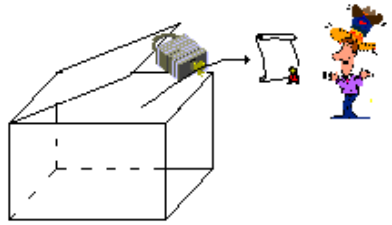


Etape 2 : Distribution des clés. Bob fait parvenir à Alice le cadenas, mais garde la clé pour lui.

Etape 3 : Envoi du message. Alice met son message dans une boite qu'elle ferme à l'aide du cadenas.



Etape 4 : Réception du message. Bob ouvre la boite a l'aide de sa clé, et récupère le message. Personne n'a pu l'intercepter puisque lui seul pouvait ouvrir la boite.



D'après http://www.bibmath.net/crypto/moderne/clepub.php3

Algorithme RSA (Rivest, Shamir, Adleman – 1977)

1- Création des clés :

Bob crée 4 nombres p, q, e et d :

p et q sont deux grands nombres premiers distincts.
Leur génération se fait au hasard, en utilisant un algorithme de *test de primallité* probabiliste.
e est un entier premier avec le produit (p-1)(q-1).
d est tel que ed=1 modulo (p-1)(q-1). Autrement dit, ed-1 est un multiple de (p-1)(q-1).
On peut fabriquer d à partir de e, p et q, en utilisant *l'algorithme d'Euclide*.

2- Distribution des clés :

Le couple (n,e) constitue la clé publique de Bob. Il la rend disponible par exemple en la mettant dans un annuaire.
Le couple (n,d) constitue sa clé privée. Il la garde secrète.

3- Envoi du message codé :

Alice veut envoyer un message codé à Bob.
Elle le représente sous la forme d'un ou plusieurs entiers M compris entre 0 et n-1.
Alice possède la clé publique (n,e) de Bob. Elle calcule C=Me mod n. C'est ce dernier nombre qu'elle envoie à Bob.

4- Réception du message codé :

Bob reçoit C, et il calcule grâce à sa clé privée D=Cd (mod n).
D'après un théorème du mathématicien Euler, D=Mde=M (mod n). Il a donc reconstitué le message initial.

Stéganographie

Cacher plutôt que chiffrer …

histoire-stéganographie

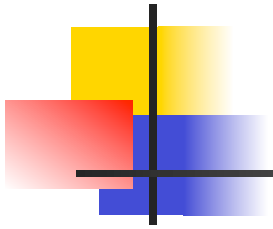
D'après http://www.bibmath.net/crypto/moderne/clepub.php3

Stéganographie

Cacher plutôt que chiffrer …

démo-stéganographie

D'après http://www.bibmath.net/crypto/moderne/clepub.php3



Le tatouage en quelques mots

Tatouage visible : masquage d'un document à l'aide d'une ou plusieurs marques visibles qui ne sont effaçables correctement que si l'on possède une clé secrète.

Tatouage fragile : permet de prouver qu'un document n'a pas été falsifié (i.e. n'a pas subi de transformation pouvant modifier son interprétation)

Tatouage semi-fragile : permet de détecter localement des manipulations malveillantes tout en étant robuste à certains traitements (comme par exemple la compression)

Tatouage aveugle : la marque est extraite à l'aide du document tatoué (éventuellement attaqué) seulement

Tatouage semi-aveugle : la marque est extraite à l'aide du document tatoué et de la connaissance de la signature (marque)

Information secrète : le fait que l'algorithme d'insertion et d'extraction n'est pas public n'est pas suffisant. Il faut une information secrète, généralement la clé.

Image déposée (tatouage visible)

Image enregistrée chez Digimarc

Tatouage : principaux défis

Principaux défis théoriques du tatouage :

- ✓ **Capacité d'insertion :** *de quelques dizaines de bits à plusieurs kilobits selon l'application*
- ✓ **Invisibilité :** *cacher le message sans gêner le confort visuel ni l'interprétation sémantique*
- ✓ **Robustesse :** *face à des traitements bienveillants ou malveillants (attaques) du signal tatoué**
- ✓ **Sécurité :** *liée aux attaques exploitant une faille de l'algorithme lui-même***

* Objectif de l'attaque: faire disparaître le tatouage

** Objectif de l'attaque: accéder à un secret pour ensuite faire disparaître le tatouage de manière « chirurgicale » ou accéder à des informations confidentielles ou encore usurper une identité et s'en servir pour tatouer un document

Les attaques

2 types d'attaque : malveillantes ou traitements courants

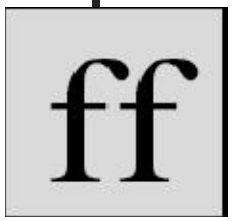
- bruitage de l'image
- transformation géométrique (décalage, rotation, zoom,…)
- filtrage linéaire (passe-bas, passe-haut, passe-bande) ou non linéaire (médian)
- réhaussement de contraste
- compression avec perte
- conversion de format (ex: JPEG vers GIF)
- composition d'images, mosaïque
- …

Logiciels libres pour tester une méthode de tatouage :

- Stirmark (http://www.petitcolas.net/fabien/watermarking/stirmark/)
- Unzign (adresse non disponible)

La quasi-totalité des systèmes de tatouage peut se faire piéger (Stirmark et Unzign)

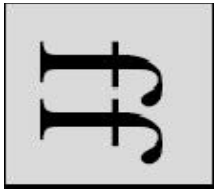
Les attaques : exemples



original

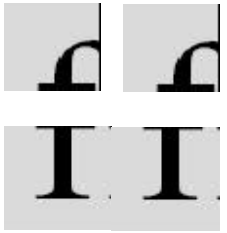
découpage

zoom



rotation

...

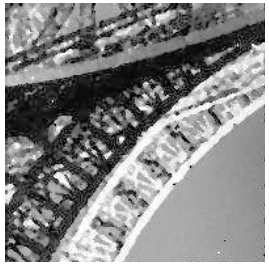


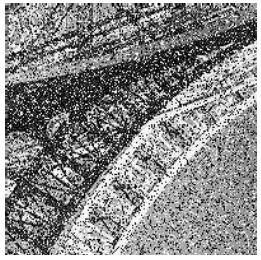
mosaïque

Bruit gaussien

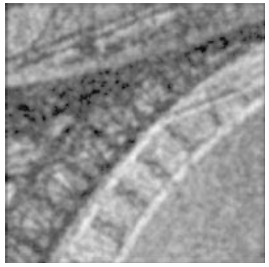
Filtrage non linéaire

original





Bruit sel et poivre



Filtrage linéaire

original

JPEG (80:1)

JPEG2000 (80:1)

Principes du tatouage

Tatouer = *insérer une marque contenant ou non de l'information*

marque = *quelques bits à quelques centaines de bits* 10011110101…

2 actions

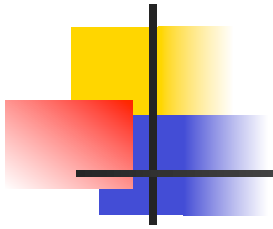
- ***insertion***
- ***lecture***

3 propriétés

- ***spécificité***
- ***invisibilité***
- ***robustesse aux attaques***

Classification des méthodes

- *Domaine initial / domaine transformé*
- *Additive / substitutive*
- *Fondée sur le contenu / de communication*



Tatouage d'images

DOMAINE SPATIAL

L'algorithme du Patchwork (Bender *et al* en 1995)

2 patches A et B de même taille (n pixels) choisis aléatoirement dans l'image (clé)

Règle de tatouage :

paire de pixels $(a_i, b_i) \Rightarrow (a'_i, b'_i)$

$$a'_i = a_i + 1$$
$$b'_i = b_i - 1$$

Extraction :

On calcule : $$S' = \sum_{i=1}^{n} (a'_i - b'_i) = \sum_{i=1}^{n} (a_i + 1 - b_i + 1) = 2n$$

Or on sait que statistiquement sur l'image on a pour n suffisamment grand : $$S = \sum_{i=1}^{n} (a_i - b_i) \approx 0$$

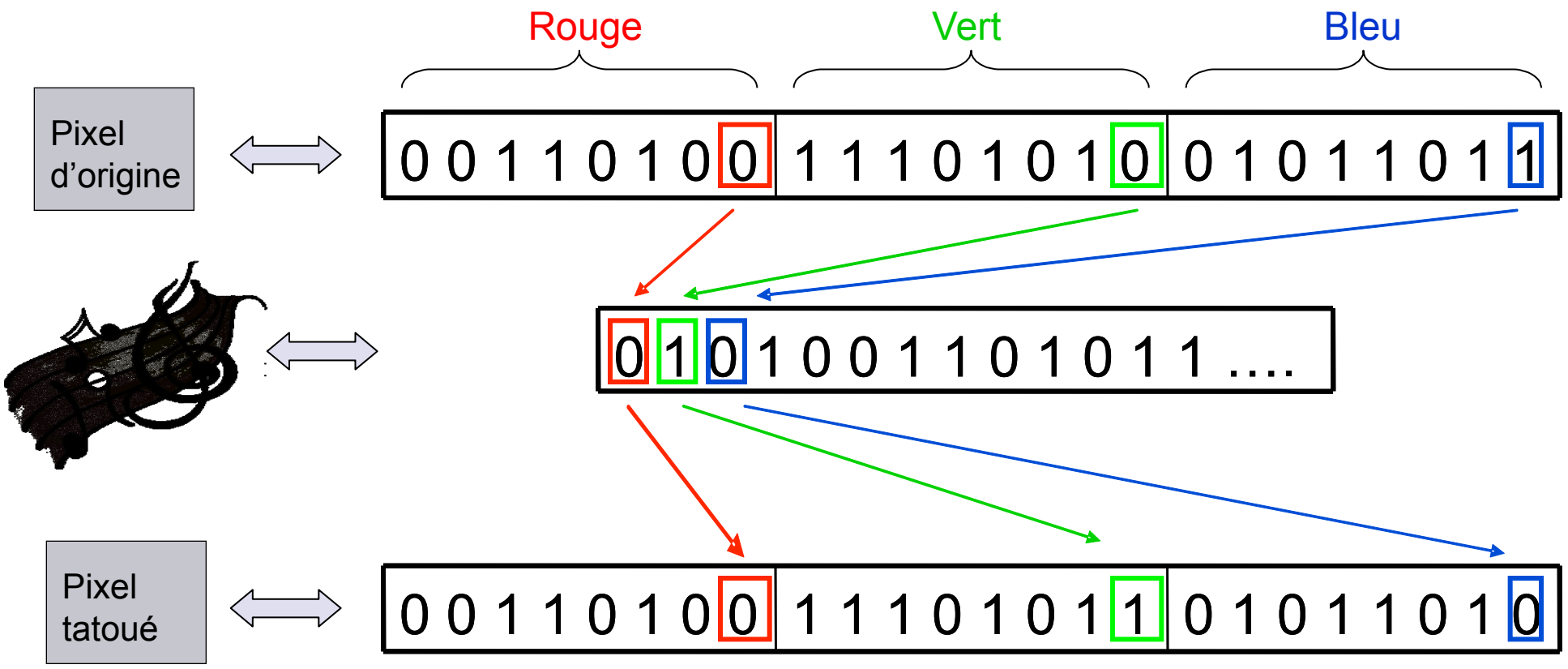
Donc seul un utilisateur possédant la clé peut retrouver $2n$

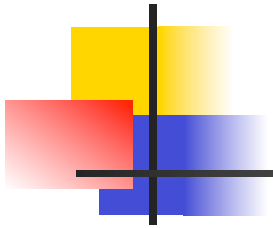
Limites de l'algorithme : Faible robustesse (attaques géométriques, filtrage,…)

Permet juste de répondre à la question : cette personne a-t'elle la clé ?

Méthode de tatouage : exemple

- Bit de poids faible (LSB pour Least Significant Bit) :





Tatouage d'images

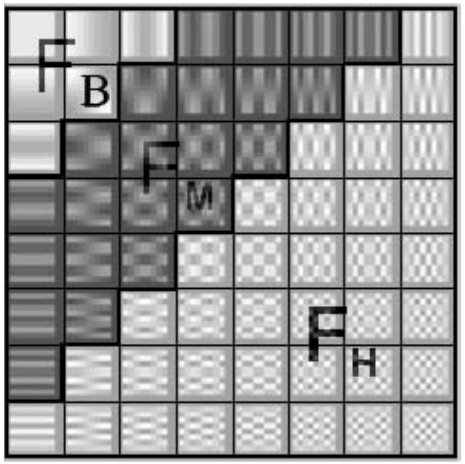
DOMAINE TRANSFORME

Meilleure prise en compte des propriétés psychovisuelles

Robustesse accrue

Algorithme de Koch et Zhao (1994)

Blocs DCT 8x8



Tatouage dans les moyennes fréquences

Fréquences basses (zones homogènes) : robuste mais visible

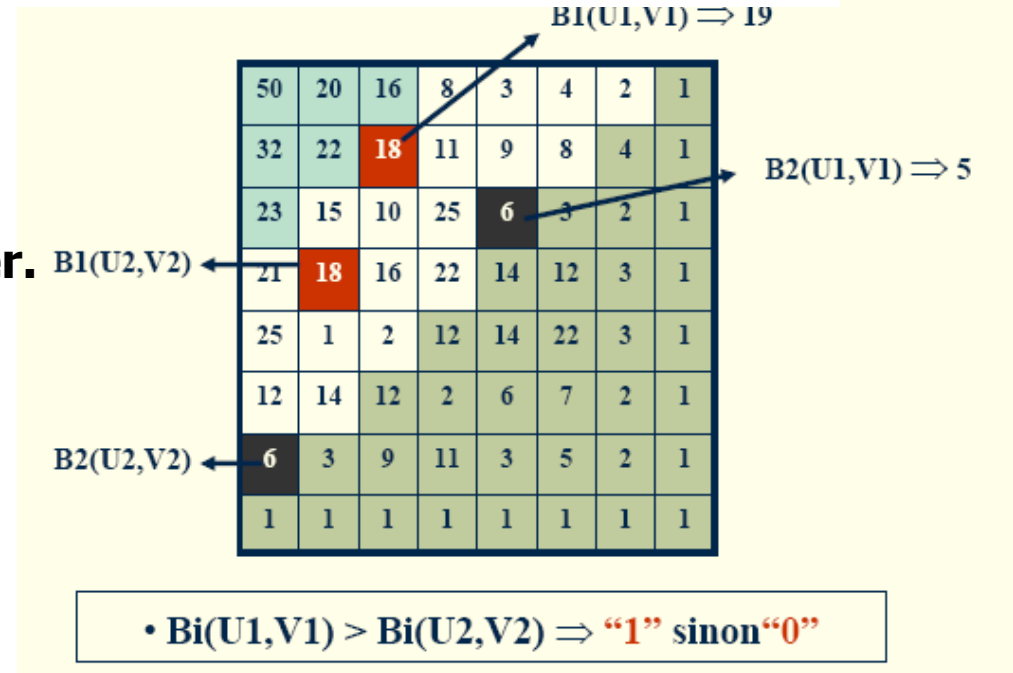
Fréquences hautes (forts contours) : invisible mais fragile

Algorithme de Koch et Zhao (1994)

Principes

Blocs DCT 8x8 choisis aléatoirement

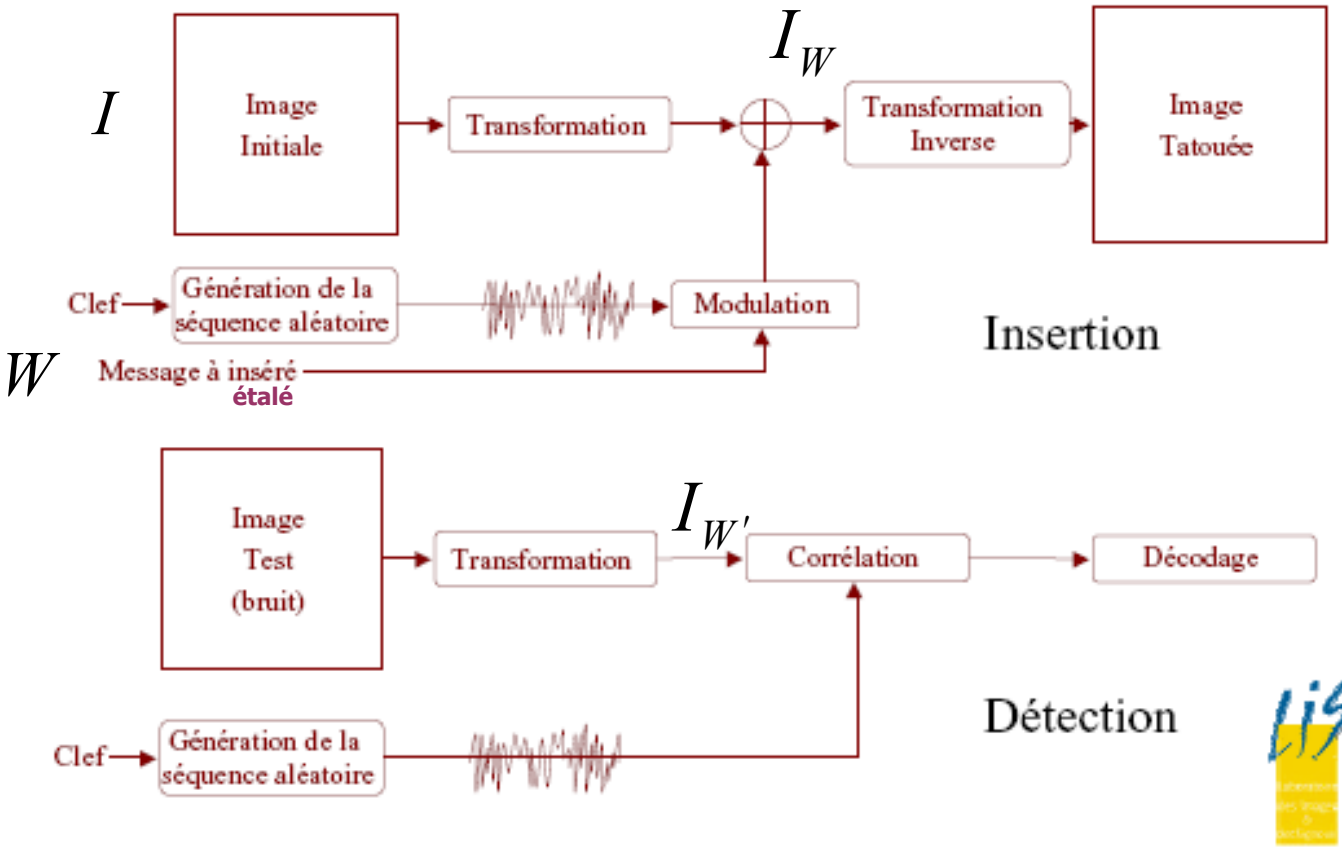
Choisir des zones des blocs fréquentiels avec la **même amplitude de valeur et les modifier.**



Inconvénients :

faible robustesse aux attaques géométriques, faible capacité (1bit/bloc)

Etalement de spectre



Etalement de spectre

- Insertion: $I_w = I \pm W,\ W(i,j) = \{-k, +k\}$
- Détection: $\langle I_w, W \rangle = \langle I, W \rangle + \langle W', W \rangle$

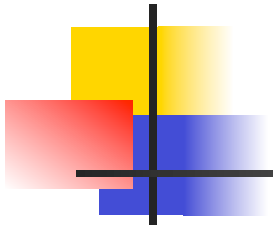
$$\# 0 \pm |W|^2 \text{ si } W' = W$$

$$\# 0 + 0 \text{ si } W' \# W$$

- Le signe de $\langle I_w, W \rangle$ permet de décoder un 0 ou un 1
- La valeur de $\langle I_w, W \rangle$ permet d'attester ou de réfuter la présence du tatouage

Tatouage vs. compression

La compression : une attaque redoutable



Tatouage vs. compression

La compression : une attaque redoutable

Objectif de la compression :

faire disparaître l'information inutile à l'œil (invisible) pour réduire la quantité de données

Objectif du tatouage :

Insérer une information invisible

Tatouage/compression conjoints

1ère approche : Utilisation d'un seul dictionnaire

Avantages : méthode aveugle, robustesse à la compression, au filtrage et au bruit

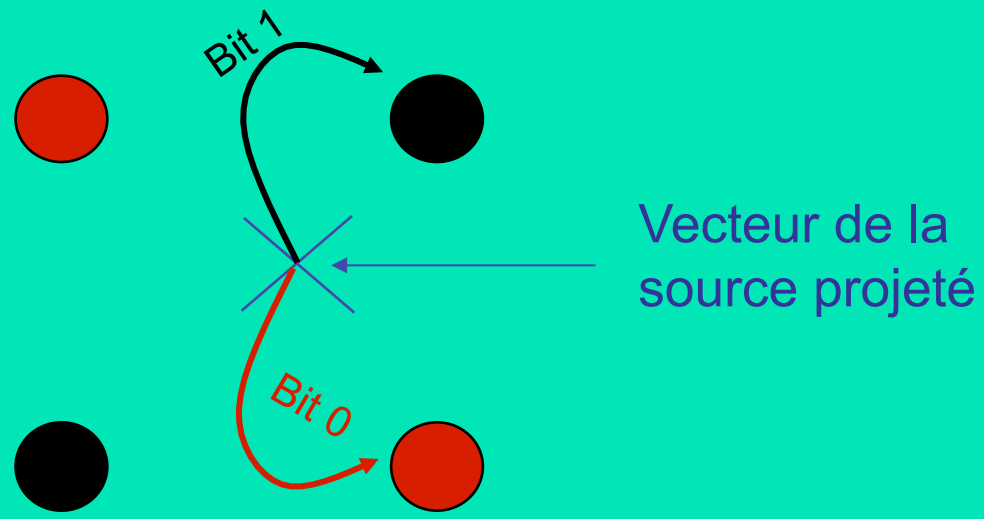
Inconvénients : sensibilité aux attaques géométriques, capacité limitée

2ème approche : QVA Modulée

Compression tatouage conjoints : 2ème approche

Vecteurs du dictionnaire associés au bit 0

Vecteurs du dictionnaire associés au bit 1



Insertion d'un message binaire par QIM*

QIM = partition du dictionnaire en **m sous-dictionnaires**

⇒ insertion **d'un message m-aire**

*QIM = quantification par modulation d'index (*Chen et Wornel*)

Tatouage/compression conjoints

2ème approche : Utilisation de 2 dictionnaires (QVAM)

Avantages : méthode aveugle, robustesse à la compression, au filtrage et au bruit, forte capacité

Inconvénients : sensibilité aux attaques géométriques

Tatouage vidéo

Caractéristiques essentielles

• bande passante de dissimulation plus grande que pour les images fixes
(Attention : elle n'est pas égale au nombre d'images multiplié par la bande passante de chacune d'elles)

• contrainte de temps réel cruciale (algorithme peu complexe)

• attaques beaucoup plus difficiles que pour les images fixes

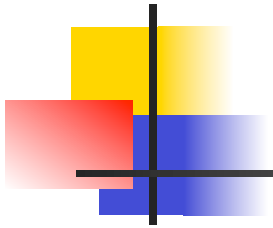
• les méthodes de tatouage s'appliquent souvent à des flux compressés

Quelques applications

• **protection des droits d'auteur (anti-copie DVD, cinéma numérique,…)**

• **transport de métadonnées**

• **authentification et intégrité des vidéos (vidéosurveillance, …)**



Tatouage vidéo

Quelques méthodes sur flux non compressé

- **spatiales** : méthode dérivée de celle de Koch et Zhao (coefficients de la DCT), …
- **spatio-temporelles** : méthode de Swanson basée sur les ondelettes (temporel) et la DCT (spatial), …
- **temporelles** : utilisées pour la protection du cinéma numérique (tatouage = modification des très basses fréquences spatiales de chaque image qui entraîne une grande dégradation de la vidéo récupérée)

Quelques méthodes sur flux compressé

- modification des vecteurs mouvement (composantes vx et vy paires si bit 0 impaires sinon)
- modification de la structure du GOP (images P = bit 0, images B = bit 1)

Conclusion tatouage

- Tatouage **fragile** : authentification
- Tatouage **robuste** : protection des droits d'auteur, …

Quelques enjeux essentiels

Protection de la propriété intellectuelle des données numériques

Méta-documents (images « intelligentes », commerce électronique, …)

Authentification de documents

JPEG2000, MPEG4 et DVD font apparaître le « watermarking »

Une multitude de nouvelles applications : web spider, …

Bibliographie

- F. Davoine, S. Pateux, « Tatouage de documents audiovisuels numériques », Traité IC2, Editions Hermès Lavoisier, 2004.
- J-L Dugeley et S. Roche, « Introduction au tatouage d'images », *http://www.eurecom.fr/~image*
- P. Bas, « Compression d'Images Fixes et de Séquences Vidéo», cours ENSERG/INPG, LIS Grenoble, Patrick.Bas@inpg.fr
- La cryptographie expliquée : http://www.bibmath.net/crypto/plan.php3
- Stirmark : http://www.petitcolas.net/fabien/kerckhoffs/la_cryptographie_militaire_i.htm#desiderata
- http://www.i3s.unice.fr/~crescenz/publications/watermarking-linfo-diaporama-2004-06.pdf
- http://www.yuvsoft.com/

Bibliographie

- K. Sayood, « Introduction to data compression », Second Edition, *Morgan Kaufman Publishers,* 2000.
- A. Mostefaoui, F. Prêteux, V. Lecuire, JM. Moureaux, « Gestion des données Multimédias », Traité IC2, Editions Hermès Lavoisier, 2004.
- A. Gersho, R.M. Gray, « Vector Quantization and Signal Compression», *Kluwer Academic Publishers*, 1992.
- N. Moreau, « Techniques de Compression des Signaux », *Ed. Masson*, 1995.
- M. Antonini, T. Gaidon, M. Barlaud, P. Mathieu, « Wavelet Transform and Image Coding », *Wavelets in Image Communication, Ed. Elsevier*, 1994.