

Schémas de tatouage d'images,
schémas de tatouage conjoint à la compression,
et schémas de dissimulation de données

Marc CHAUMONT

23/07/2013

La dissimulation de données



Neil F. Johnson, Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", Computing Practices

2005 - 2013 : Diverses contributions

- suivi de visage par modèle 3D déformable,

2005 - 2013 : Diverses contributions

- suivi de visage par modèle 3D déformable,
- chiffrement de vidéos,

2005 - 2013 : Diverses contributions

- suivi de visage par modèle 3D déformable,
- chiffrement de vidéos,
- **attaque par colorisation,**

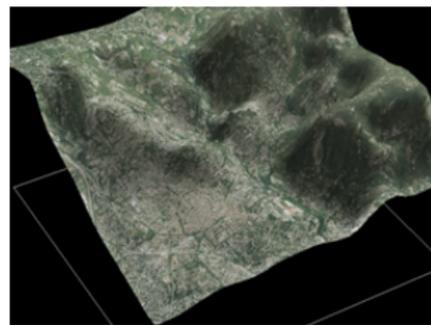
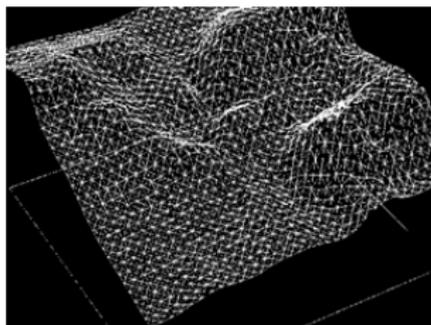
Attaque par colorisation



2005 - 2013 : Diverses contributions

- suivi de visage par modèle 3D déformable,
- chiffrement de vidéos,
- attaque par colorisation,
- dissimulation de MNT dans les images,

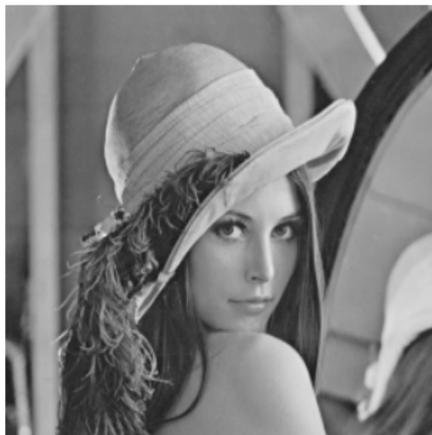
Dissimulation de MNT dans les images



2005 - 2013 : Diverses contributions

- suivi de visage par modèle 3D déformable,
- chiffrement de vidéos,
- attaque par colorisation,
- dissimulation de MNT dans les images,
- **tatouage réversible**,

Tatouage reversible



2005 - 2013 : Diverses contributions

- suivi de visage par modèle 3D déformable,
- chiffrement de vidéos,
- attaque par colorisation,
- dissimulation de MNT dans les images,
- tatouage réversible,
- **tatouage robuste aux désynchronisations,**

Tatouage robuste aux désynchronisations



2005 - 2013 : Diverses contributions

- suivi de visage par modèle 3D déformable,
- chiffrement de vidéos,
- attaque par colorisation,
- dissimulation de MNT dans les images,
- tatouage réversible,
- tatouage robuste aux désynchronisations,
- traçage de traîtres dans H.264,

2005 - 2013 : Diverses contributions

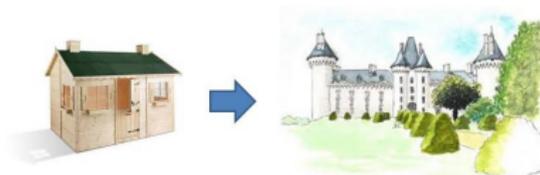
- suivi de visage par modèle 3D déformable,
- chiffrement de vidéos,
- attaque par colorisation,
- dissimulation de MNT dans les images,
- tatouage réversible,
- tatouage robuste aux désynchronisations,
- traçage de traîtres dans H.264,
- ...
- tatouage robuste, tatouage conjoint, dissimulation de la couleur,
- stéganographie par oracle, stéganalyse par ensemble classifieur.

SECURITÉ



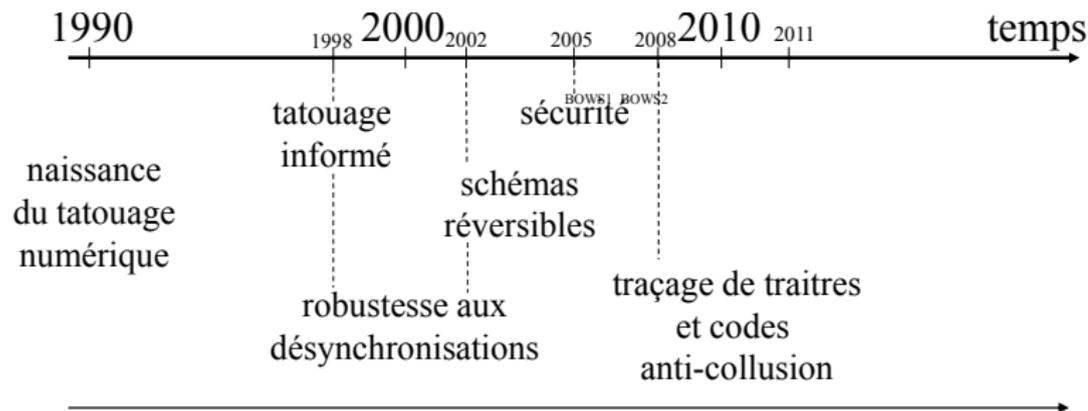
- Protection du droit d'auteur
- **Traçage de traîtres**
- Authentification
- Contrôle de copie
- Communication secrète (stéganographie)

AMÉLIORATION

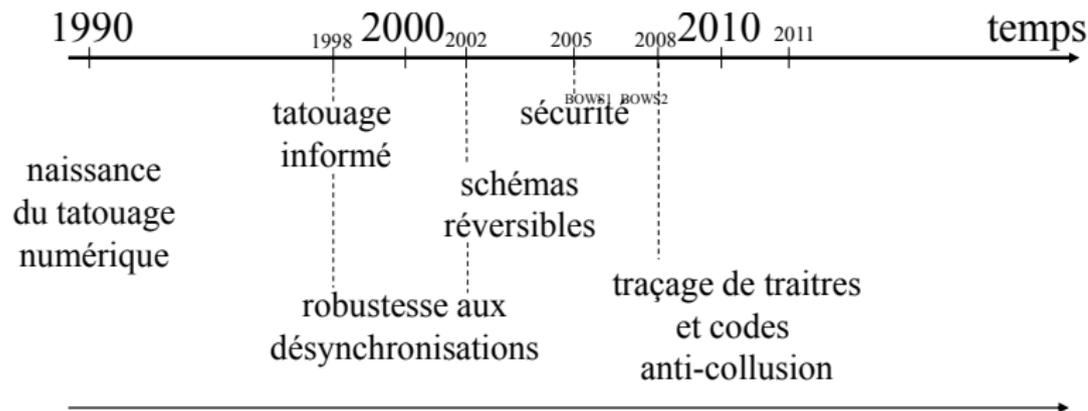


- Contrôle de périphérique
- Analyse/surveillance d'un flux numérique
- **Enrichissement: fonctionnalités, métadatas**
- Amélioration performances compression
- Correction d'erreurs après transmission

Chronologie du tatouage



Mon positionnement sur la période 2005-2011



- Le tatouage robuste à haute capacité,
- Le tatouage conjoint à la compression JP2K et H.264,
- La dissimulation de la couleur d'une image.

Contributions présentées (2005-2011)

- Le tatouage robuste à haute capacité
 - ▶ Q) Quelle est la meilleure approche ?
 - ▶ Deux grandes familles
[Chaumont, IJIPVC'2012] [Chaumont et Goudia, ICME'2011]
- La dissimulation de la couleur d'une image
 - ▶ Q) Un courant alternatif aux approches basées ondelettes ?
 - ▶ *[Chaumont et Puech, ICIP'2007]*
[Chaumont et Puech, Recent Advances in Signal Processing 2009]

Les principaux projets porteurs :

ANR TSAR 2005-2008, ANR Vooddo 2007-2010, Collaboration avec Floware 2010-2011.

Doctorants sur la période :

Thèse de Meuel 2009, Shahid 2010, Goudia 2011

Plan

1 Le tatouage robuste à haute capacité

- Introduction

- Dirty Paper Trellis Code (DPTC) et Multi Hyper Cube (MHC)
- Comparaisons des deux familles

2 Dissimulation de la couleur d'une image

- Introduction

- Deux approches : (1) par optimisation (2) 512 couleurs
- Comparaisons

3 Conclusions et perspectives

Les schémas de tatouage robustes à haute capacité

2 grandes familles de tatouage robuste multi-bits:

- Basé treillis (DPTC),
- Basé quantification (DC-QIM, SCS, RDM, P-QIM, ...).

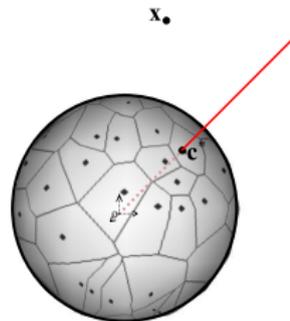
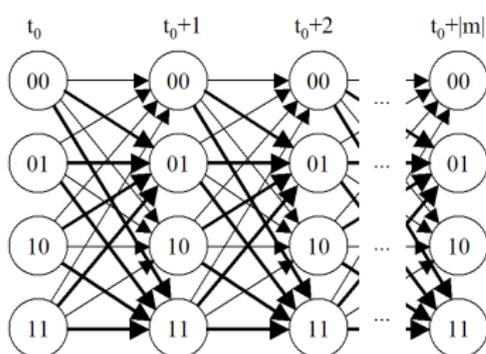
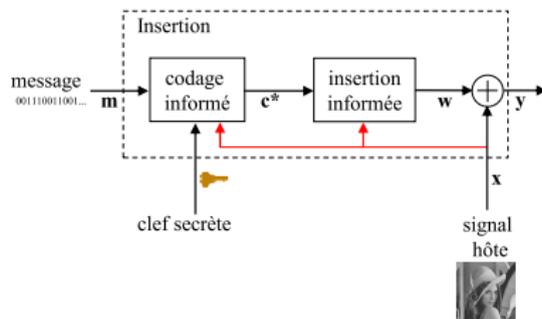
Conditions de comparaison

- faible complexité (quelques secondes),
- fort payload = 1 bit inséré dans 64 pixels (1024 bits inséré dans image 256×256),
- prise en compte l'aspect psychovisuel (SSIM de 98%),
- robustesse aux attaques valométriques,
- intégration d'un code correcteur.

Plan

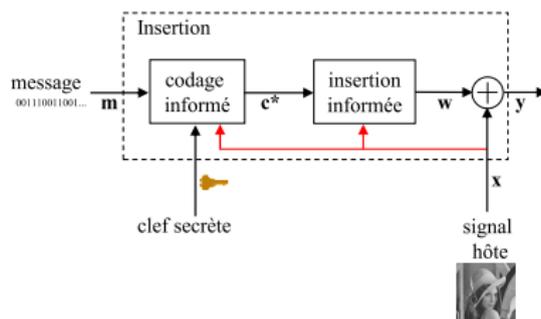
- 1 Le tatouage robuste à haute capacité
 - Introduction
 - Dirty Paper Trellis Code (DPTC) et Multi Hyper Cube (MHC)
 - Comparaisons des deux familles
- 2 Dissimulation de la couleur d'une image
 - Introduction
 - Deux approches : (1) par optimisation (2) 512 couleurs
 - Comparaisons
- 3 Conclusions et perspectives

DPTC : Codage informé

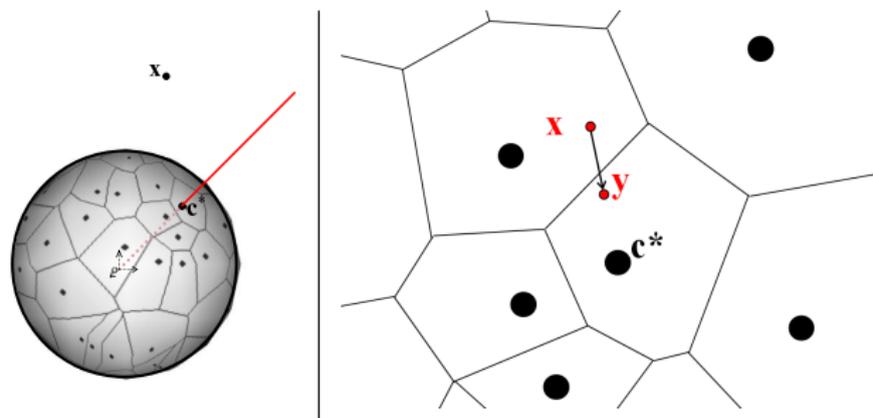


[Miller et al. 2004]

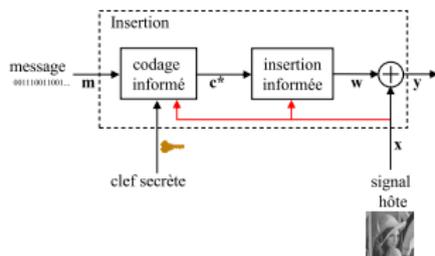
DPTC : Insertion informée



[Chaumont 2012] : Approche par rotation.

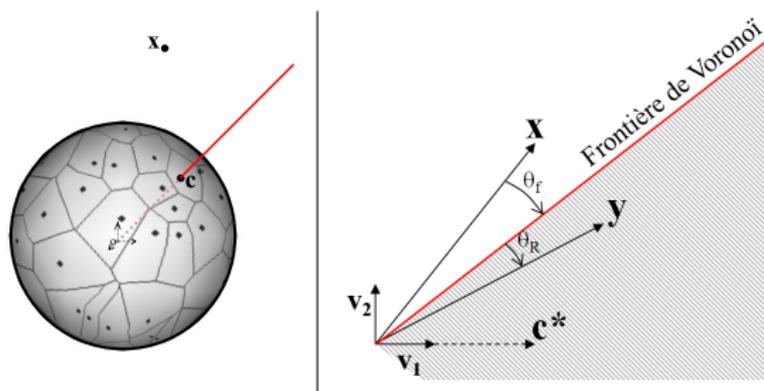


DPTC : Insertion informée

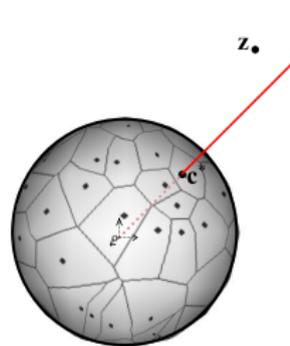
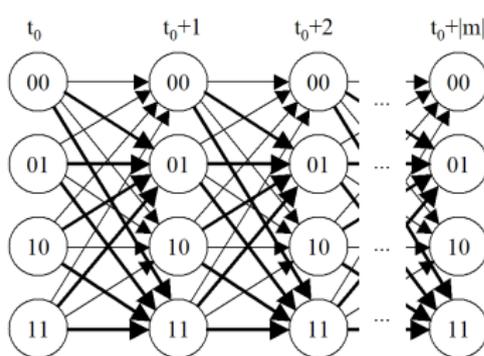
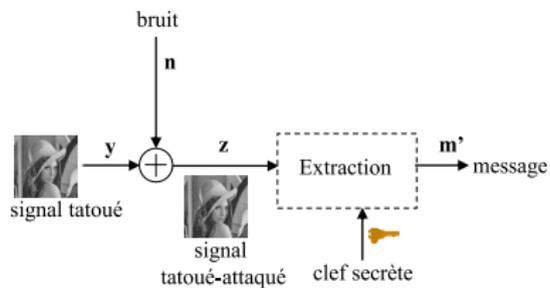


[Chaumont 2012] :

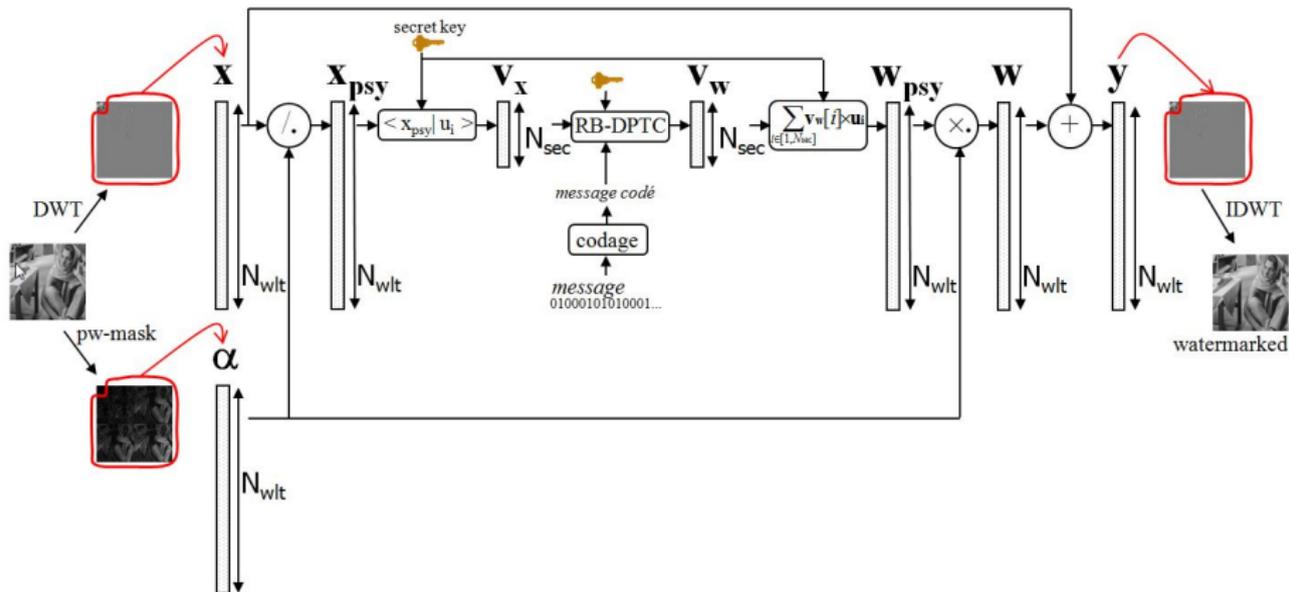
- Rotation de \mathbf{x} d'un angle $\max(\theta_f + \theta_R, (\widehat{\mathbf{x}, \mathbf{c}^*}))$.
- $\mathbf{w} = \mathbf{y} - \mathbf{x}$



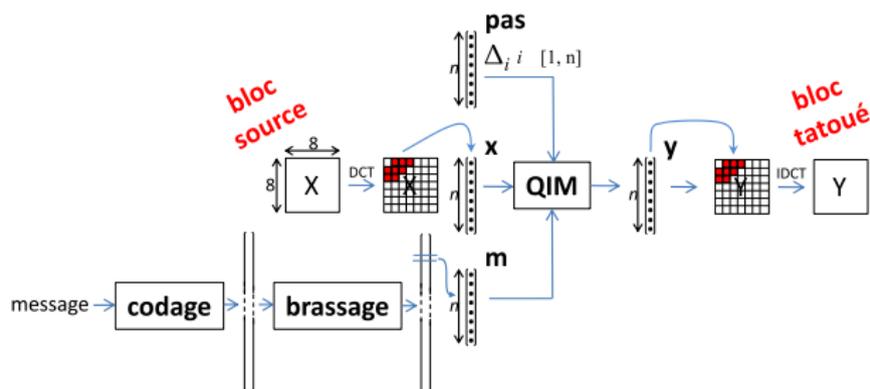
DPTC : Extraction



RB-DPTC : Contexte Image



P-QIM \rightarrow MHC : Multi-Hyper-Cube



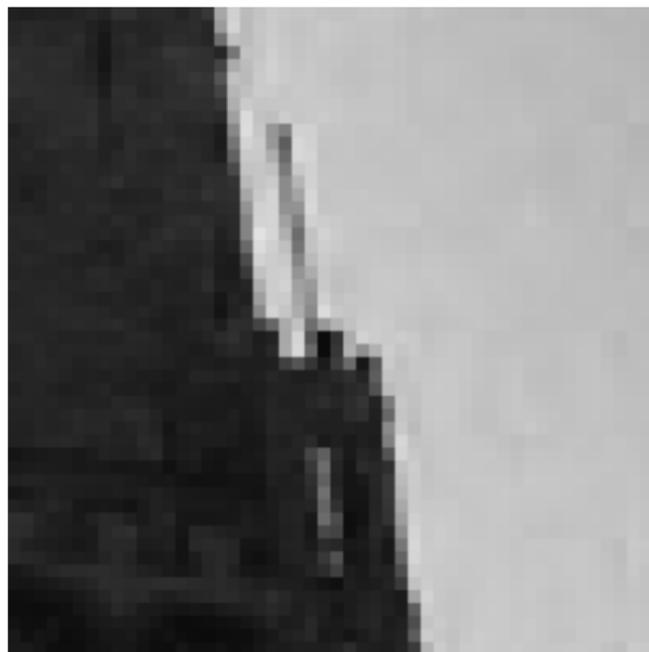
MHC : Multi-Hyper-Cube [Chaumont et Goudia ICME'11]

- QIM remplacé par TCQ,
- Décodage souple,
- Réduction des effets de blocs.

Illustration de l'effet de blocs

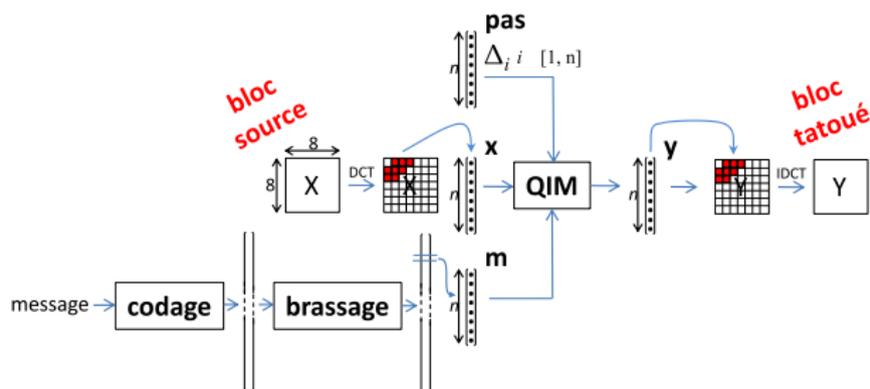


P-QIM



Hyper-Cube

P-QIM → MHC : Multi-Hyper-Cube



MHC : Multi-Hyper-Cube [Chaumont et Goudia ICME'11]

- QIM remplacé par TCQ,
- Décodage souple,
- Réduction des effets de bloc.

Plan

1 Le tatouage robuste à haute capacité

- Introduction
- Dirty Paper Trellis Code (DPTC) et Multi Hyper Cube (MHC)
- Comparaisons des deux familles

2 Dissimulation de la couleur d'une image

- Introduction
- Deux approches : (1) par optimisation (2) 512 couleurs
- Comparaisons

3 Conclusions et perspectives

Robustesse et Temps CPU

T-TCQ : valumétrique = NO; JPEG = OK; filtre/AWGN = OK
RB-DPTC : valumétrique = OK; JPEG = NO; filtre/AWGN \approx OK
MHC : valumétrique \approx OK; JPEG \approx OK; filtre/AWGN \approx OK

- Processeur Intel 2, Duo CPU, 2.4GHz, 4Go de RAM,
- Image 8 bits 256×256 , 1/64 bpp, SSIM = 98%.

Algorithme	coût CPU (secondes)
MHC [Chaumont et Goudia, ICME'11]	0.98
T-TCQ [LeGuelvouit TS'09]	5.73
RB-DPTC [Chaumont, IJIPVC'12]	12.74

Plan

- 1 Le tatouage robuste à haute capacité
 - Introduction
 - Dirty Paper Trellis Code (DPTC) et Multi Hyper Cube (MHC)
 - Comparaisons des deux familles
- 2 Dissimulation de la couleur d'une image
 - Introduction
 - Deux approches : (1) par optimisation (2) 512 couleurs
 - Comparaisons
- 3 Conclusions et perspectives

Illustration possible : Protection de la couleur

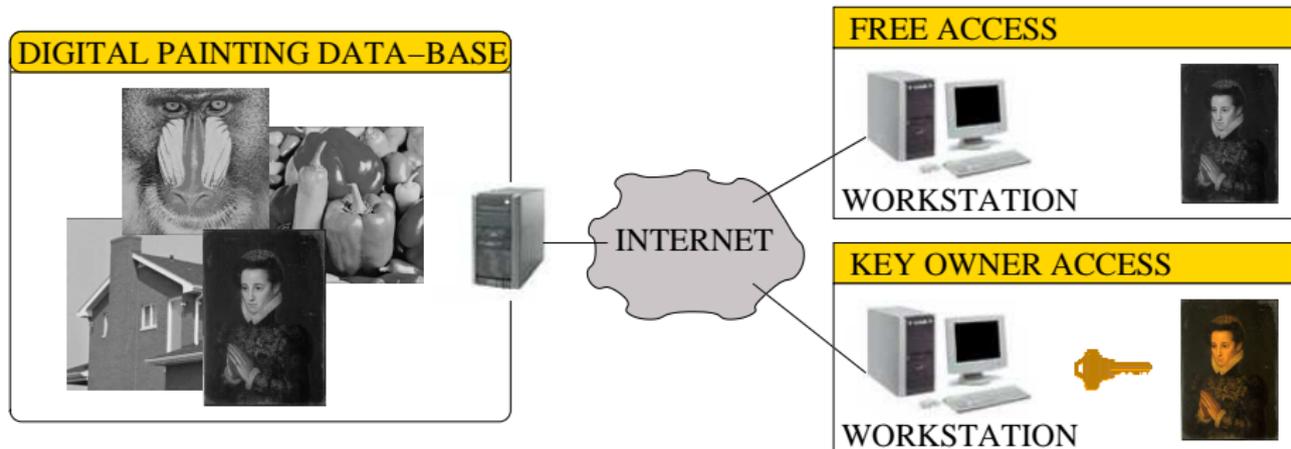
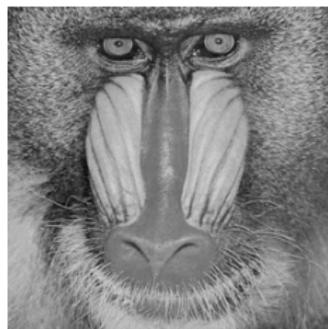
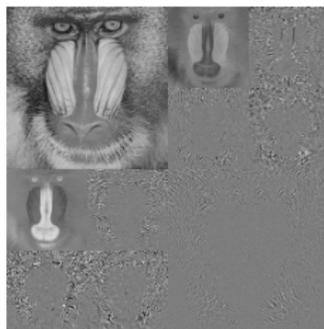


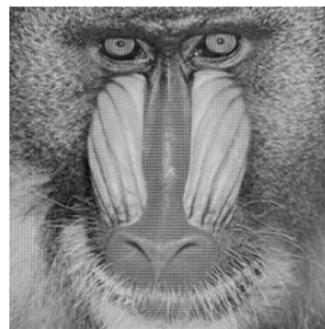
Illustration des approches basées substitution



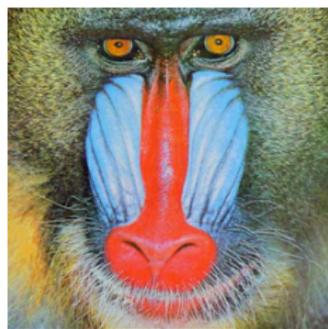
Luminance



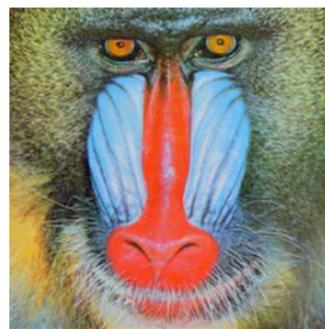
Substitution ondelette



Dissimulation



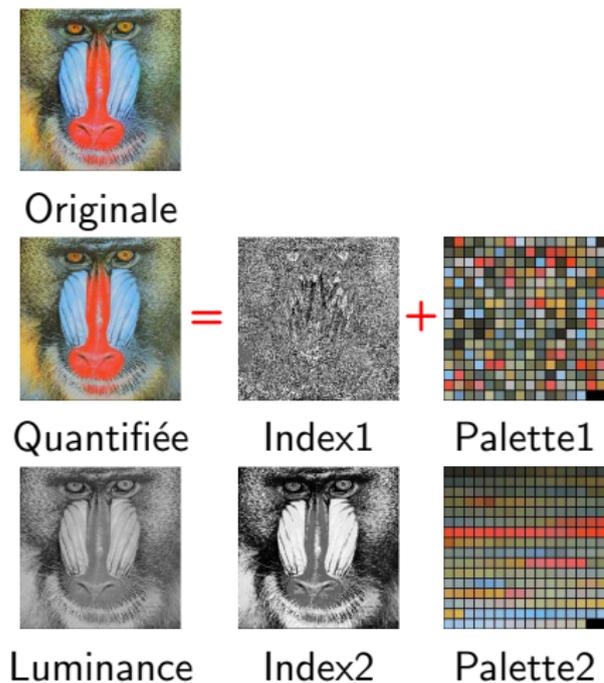
Originale



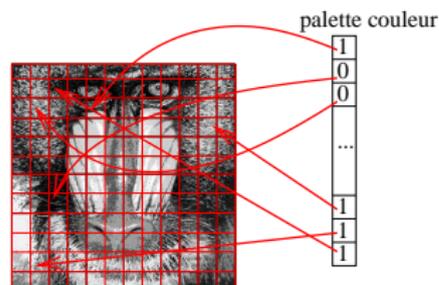
Reconstruite

[Campisi *et al.*'02]

Illustration des approches basées palette



$$Index_m(i) = Index(i) - Index(i) \bmod 2 + m[j],$$



Plan

- 1 Le tatouage robuste à haute capacité
 - Introduction
 - Dirty Paper Trellis Code (DPTC) et Multi Hyper Cube (MHC)
 - Comparaisons des deux familles
- 2 Dissimulation de la couleur d'une image
 - Introduction
 - Deux approches : (1) par optimisation (2) 512 couleurs
 - Comparaisons
- 3 Conclusions et perspectives

Approche par optimisation de fonctionnelle



C(Index)



Originale **I**

≈

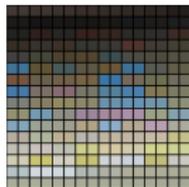


Index



Luminance **Y**

≈



Palette **C**

$$E1 = \underbrace{\sum_{i=1}^N \text{dist}^2(\mathbf{C}(\text{Index}(i)), \mathbf{I}(i))}_{\text{premier terme}}$$

$$+ \lambda_1 \underbrace{\sum_{i=1}^N \text{dist}^2(\text{Index}(i), \mathbf{Y}(i))}_{\text{deuxième terme}}$$

$$+ \lambda_2 \underbrace{\sum_{k|k \in [1..K] \text{ et } k \text{ impair}} \text{dist}^2(\mathbf{C}(k), \mathbf{C}(k+1))}_{\text{troisième terme}}.$$

Approche par optimisation de fonctionnelle

Boucle jusqu'à stabilisation énergie E2

$$E2 = \sum_{i=1}^{i=N} \sum_{k=1}^{k=K} \mathbf{P}_{i,k}^{\gamma} \text{dist}^2(\mathbf{C}(k), \mathbf{I}(i)) + \lambda_1 \sum_{i=1}^{i=N} \sum_{k=1}^{k=K} \mathbf{P}_{i,k}^{\gamma} (\mathbf{Y}(i) - k)^2 + \lambda_2 \sum \text{dist}^2(\mathbf{C}(k), \mathbf{C}(k+1))$$

Calcul de \mathbf{C} par résolution du système linéaire $\mathbf{A} \cdot \mathbf{C} = \mathbf{B}$:

$$\mathbf{A} = \begin{pmatrix} \lambda_2 + \sum_{i=1}^{i=N} \mathbf{P}_{i,1}^{\gamma} & -\lambda_2 & 0 & \dots \\ -\lambda_2 & \lambda_2 + \sum_{i=1}^{i=N} \mathbf{P}_{i,2}^{\gamma} & 0 & \dots \\ 0 & 0 & \lambda_2 + \sum_{i=1}^{i=N} \mathbf{P}_{i,3}^{\gamma} & \dots \\ 0 & 0 & -\lambda_2 & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix}, \mathbf{B} = \begin{pmatrix} \sum_{i=1}^{i=N} \mathbf{P}_{i,1}^{\gamma} \mathbf{I}(i) \\ \sum_{i=1}^{i=N} \mathbf{P}_{i,2}^{\gamma} \mathbf{I}(i) \\ \dots \\ \sum_{i=1}^{i=N} \mathbf{P}_{i,K-1}^{\gamma} \mathbf{I}(i) \\ \sum_{i=1}^{i=N} \mathbf{P}_{i,K}^{\gamma} \mathbf{I}(i) \end{pmatrix}.$$

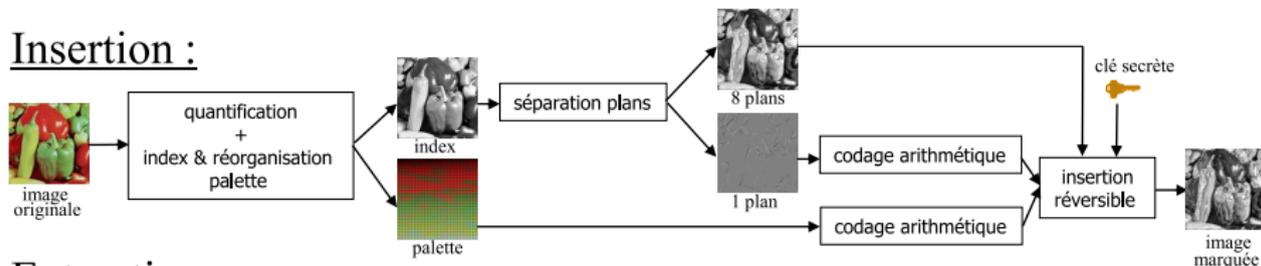
Calcul des $\mathbf{P}_{i,k}$:

$$P_{i,k} = \frac{\left(\sum_{l=1}^{l=K} \frac{1}{2 \times (\text{dist}^2(\mathbf{C}(l), \mathbf{I}(i)) + \lambda_1 (\mathbf{Y}(i) - l)^2)} \right)^{-1}}{2 \times (\text{dist}^2(\mathbf{C}(k), \mathbf{I}(i)) + \lambda_1 (\mathbf{Y}(i) - k)^2)}.$$

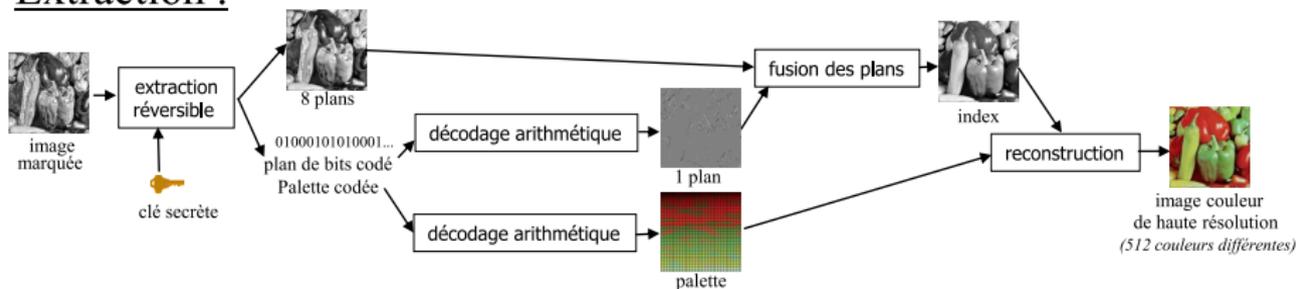
Obtention de \mathbf{C} et **Index** | $\forall i, \mathbf{Index}(i) = \arg \max_k \mathbf{P}_{i,k}$

512 couleurs [Chaumont et Puech, chap. livre InTech'09]

Insertion :



Extraction :



Plan

- 1 Le tatouage robuste à haute capacité
 - Introduction
 - Dirty Paper Trellis Code (DPTC) et Multi Hyper Cube (MHC)
 - Comparaisons des deux familles
- 2 Dissimulation de la couleur d'une image
 - Introduction
 - Deux approches : (1) par optimisation (2) 512 couleurs
 - Comparaisons
- 3 Conclusions et perspectives

Comparaisons

Images	Queiroz et Braun	Campisi <i>et al.</i>	Flou	Réarrangement	512 couleurs
	[Queiroz <i>et al.</i> 06]	[Campisi <i>et al.</i> 02]	[Chaumont <i>et al.</i> 07c]	[Chaumont <i>et al.</i> 07b]	[Chaumont <i>et al.</i> 08a]
baboon	23.93 dB	29.8 dB	27.90 dB	33.31 dB	35.86 dB
peppers	28.82 dB	32.36 dB	31.68 dB	36.32 dB	38.95 dB
lena	30.31 dB	36.75 dB	37.87 dB	38.63 dB	40.93 dB
house	30.75 dB	31.76 dB	35.45 dB	39.27 dB	41.67 dB
airplane	28.56 dB	32.58 dB	33.66 dB	39.90 dB	42.96 dB



Campisi



Originale



512

Plan

- 1 Le tatouage robuste à haute capacité
 - Introduction
 - Dirty Paper Trellis Code (DPTC) et Multi Hyper Cube (MHC)
 - Comparaisons des deux familles
- 2 Dissimulation de la couleur d'une image
 - Introduction
 - Deux approches : (1) par optimisation (2) 512 couleurs
 - Comparaisons
- 3 Conclusions et perspectives

- **Tatouage robuste haute capacité**

- ▶ Approche par rotation pour DPTC (peu complexe),
- ▶ Approche par TCQ pour P-QIM (robuste),

- **Dissimulation de la couleur**

- ▶ Approche par optimisation (beau mais complexe),
- ▶ Approche 512 couleurs (performant),

- **Tatouage robuste haute capacité**

- Q) **Meilleure approche ?**

- ▶ Approche basée quantification (SS-QIM, MHC)

- **Dissimulation de la couleur**

- Q) **Alternative ondelettes ?**

- ▶ Approche 512 couleurs & Améliorations possibles.

- **Insertion dans JP2K et H.264**

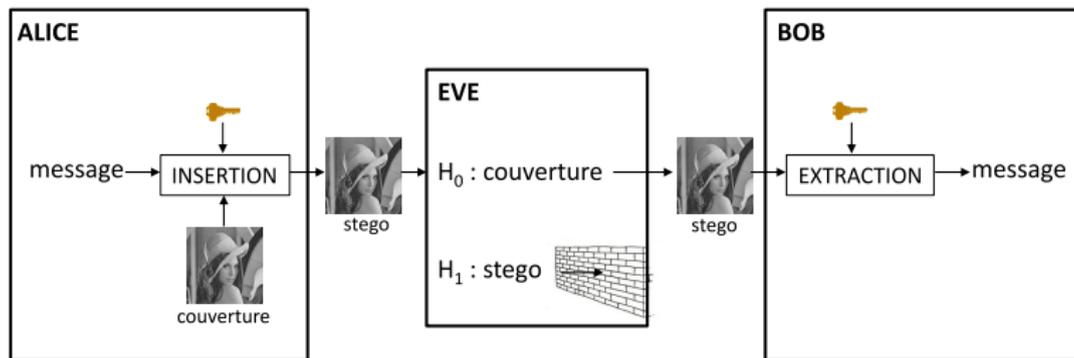
- Q) **Robustesse ? Complexité ?**

- ▶ + Ajoute peu de complexité,
 - ▶ - Peu robuste aux désynchronisations, Sécurité pas assez évaluée, nécessite de l'information adjacente (taux de compression, seuils)

Evolution de la discipline, évolution annexe au tatouage :

- La sécurité et le traçage de traîtres (théorie info, et crypto),
- La robustesse aux désynchronisations (théorie info, et TS),
- Autres média, autres formats,
- Aspects psychovisuels.

Perspectives : Stéganographie, Forensic, Segmentation

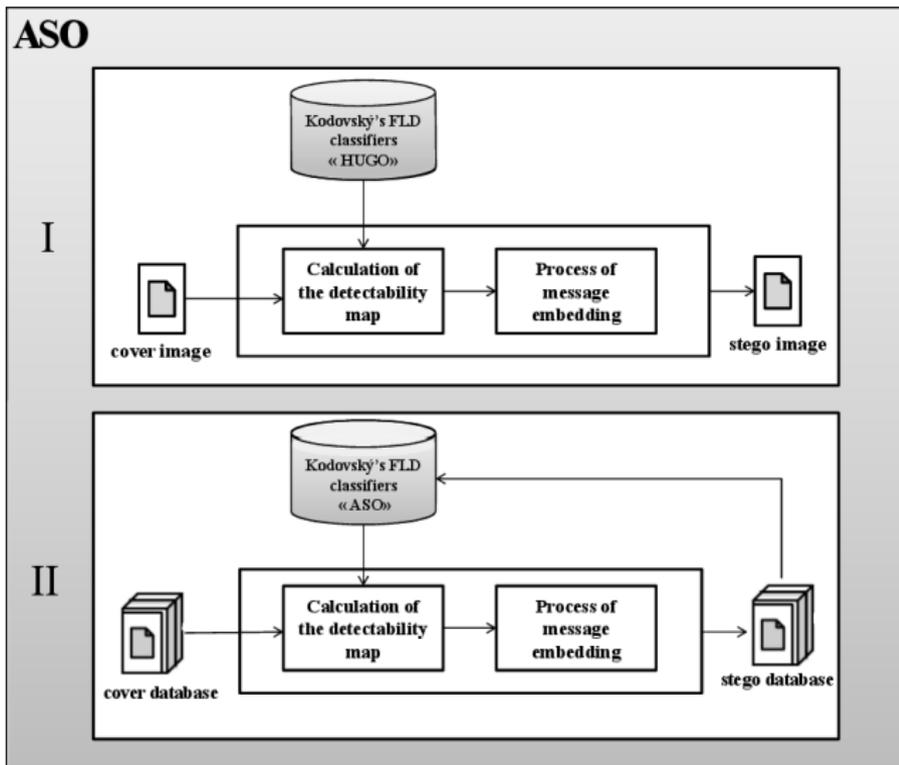


Ph.D Sarra Kouider (soutenance dec. 2013).

Axes futurs:

- Stéganalyse plus réaliste,
- Stéganographie à gardien actif,
- Steganographie théorie des jeux et codes correcteurs,
- Recherche de preuves (criminalistique, *forensic*); Ph.D. Amel SAEED TUAMA,
- Segmentation d'image aérienne; Ph.D. Jérôme PASQUET.

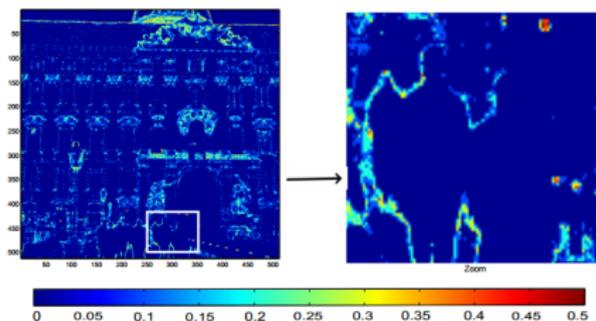
ASO : Adaptive Steganography by Oracle



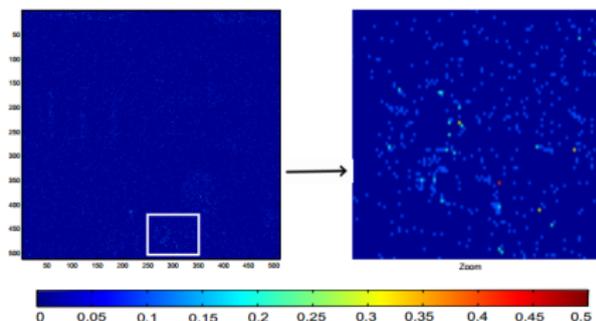
ASO : Adaptive Steganography by Oracle



(a) Grayscale cover image

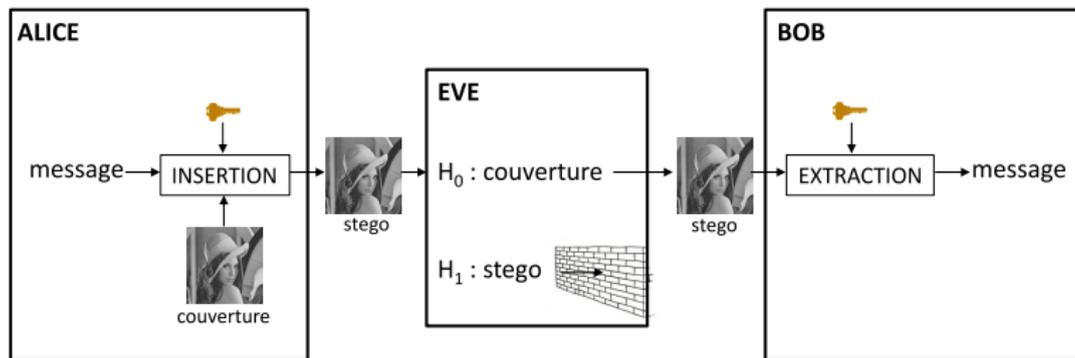


(b) HUGO 0.2 bpp



(c) ASO 0.2 bpp

Perspectives : Stéganographie, Forensic, Segmentation



Ph.D Sarra Kouider (soutenance dec. 2013).

Axes futurs:

- Stéganalyse plus réaliste,
- Stéganographie à gardien actif,
- Steganographie théorie des jeux et codes correcteurs,
- Recherche de preuves (criminalistique, *forensic*); Ph.D. Amel SAEED TUAMA,
- Segmentation d'image aérienne; Ph.D. Jérôme PASQUET.

Fin



Slides may be downloaded at: <http://www.lirmm.fr/~chaumont/Publications.html>

e-mail : marc.chaumont@lirmm.fr