Laboratoire
d'Informatique
de Robotique
et de Microélectronique
de Montpellier

LIRMM

Une nouvelle technique pour le tatouage par Dirty Paper Trellis Code (DPTC)

Marc CHAUMONT (LIRMM)

XXIIe Colloque GRETSI - Traitement du Signal et des Images - Université de Bourgogne - Dijon - 8-11 septembre 2009.

Plan

- Les schémas de tatouage à fort “payload”
- L’algorithme Dirty Paper Trellis Code (DPTC)
- Une nouvelle approche : l’algorithme RB-DPTC
- Evaluations expérimentales
- Conclusions

Les schémas de tatouage à fort “payload”

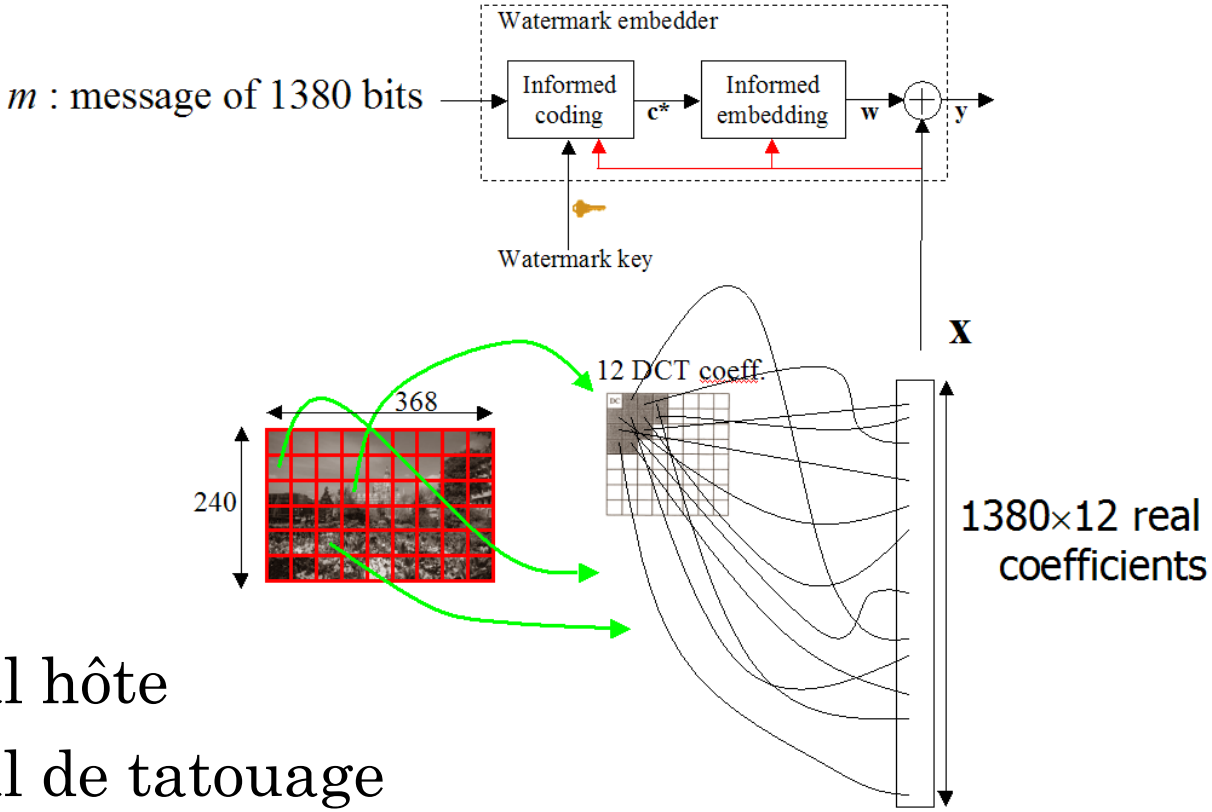
Les schémas de tatouage à fort "paylaod"

- Basés quantification:
  - DC-QIM, SCS, RDM, Perceptual-QIM…
- Basé treillis:
  - DPTC
- Mix de Quantification et Treillis:
  - T-TCQ

⇒ **payload ≈ 1 bit inséré dans 64 pixels**
(image 256×256 ⇒ 1024 bits insérés)

L'algorithme Dirty Paper Trellis Code (DPTC)

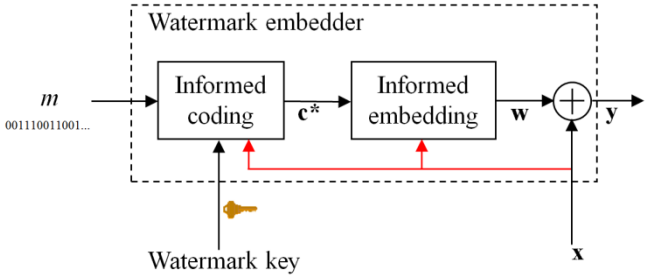
ALGORITHME DPTC [1]
- ESPACE D'INSERTION -



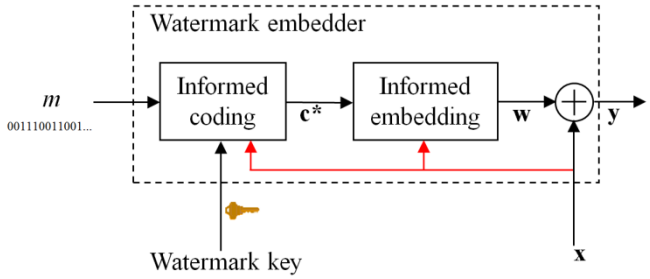
- **x** : signal hôte
- **w** : signal de tatouage
- **y** : signal tatoué
- **c*** : mot de code (proche de **x** et code le message)

[1] « Applying Informed Coding and Informed Embedding to Design a Robust, High Capacity Watermark », Miller, Doërr, and Cox, IEEE TIP'2004.

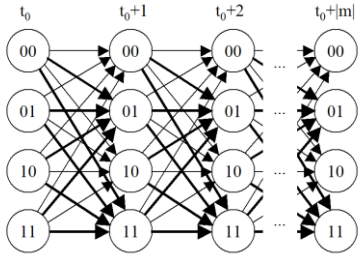
Algorithme DPTC
- Codage et Insertion -



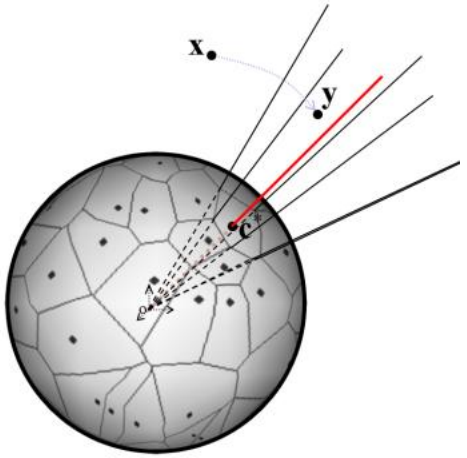
Algorithme DPTC
- Codage et Insertion -



- Informed coding:
  - Un treillis non déterministe
  - Algorithme de Viterbi pour obtenir le mot de code **c*** (codant **m**) et le plus corrélé à **x**



- Informed embedding:
  - "Déplacer" le signal **x** dans la région de Voronoï de **c*** (approche Monte Carlo)
  - **w = y - x**



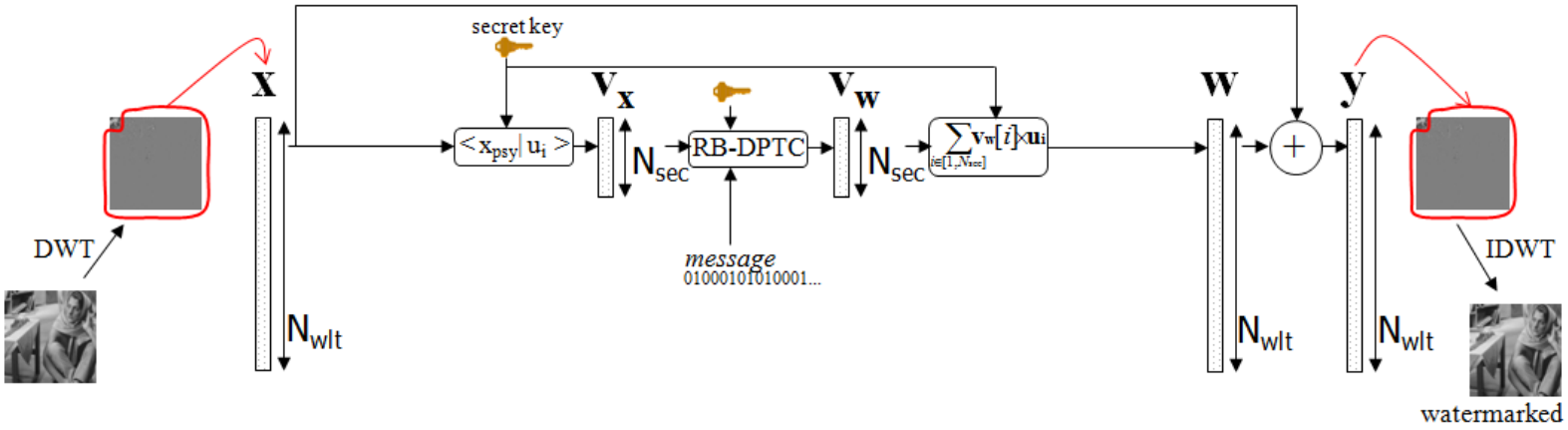
Algorithme DPTC
- Faiblesses -

- Faille de sécurité (Kerckhoffs - attaque par collusion)
  - Livre du code estimable sur version simplifiée [2].
- Etape d'insertion coûteuse en temps de calcul
  - Compromis robustesse-distorsion de Lin *et al.* [3] non satisfaisant.
- Artefacts DCT visibles.

[2] « Evaluation of an Optimal Watermark Tampering Attack Against Dirty Paper Trellis Schemes », Bas and Doërr, MM&Sec'2008.
[3] « An Efficient Algorithm for Informed Embedding of Dirty Paper Trellis Codes for Watermarking », Lin, Cox, Doërr, and Miller, ICIP'2005.

Une nouvelle approche : l'algorithme RB-DPTC

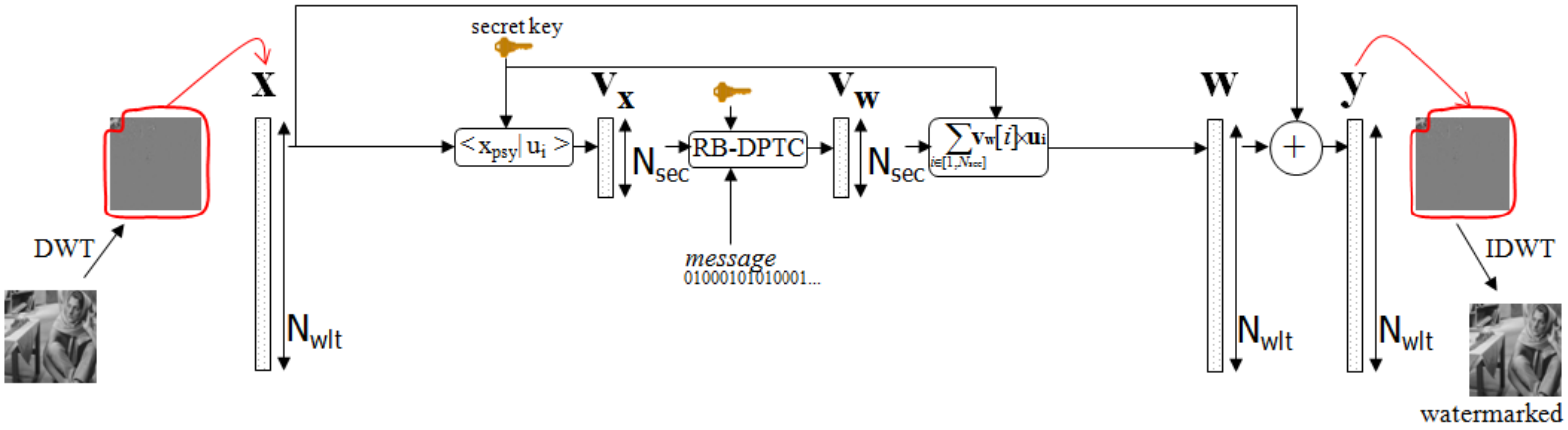
ALGORITHME RB-DPTC
- ESPACE D'INSERTION -



- **x** : signal hôte
- **w** : signal de tatouage
- **y** : signal tatoué
- $\{\mathbf{u}_i\}_{i=1}^{N_{sec}}$: porteuses (séquences pseudo-aléatoire bipolaires normalisées)
- $\mathbf{v_x}$: vecteur hôte = espace secret
- $\mathbf{v_w}$: vecteur de tatouage = vecteur de tatouage dans l'espace secret

[4] « A Novel Embedding Technique For Dirty Paper Trellis Watermarking", Chaumont, en cours de soumission

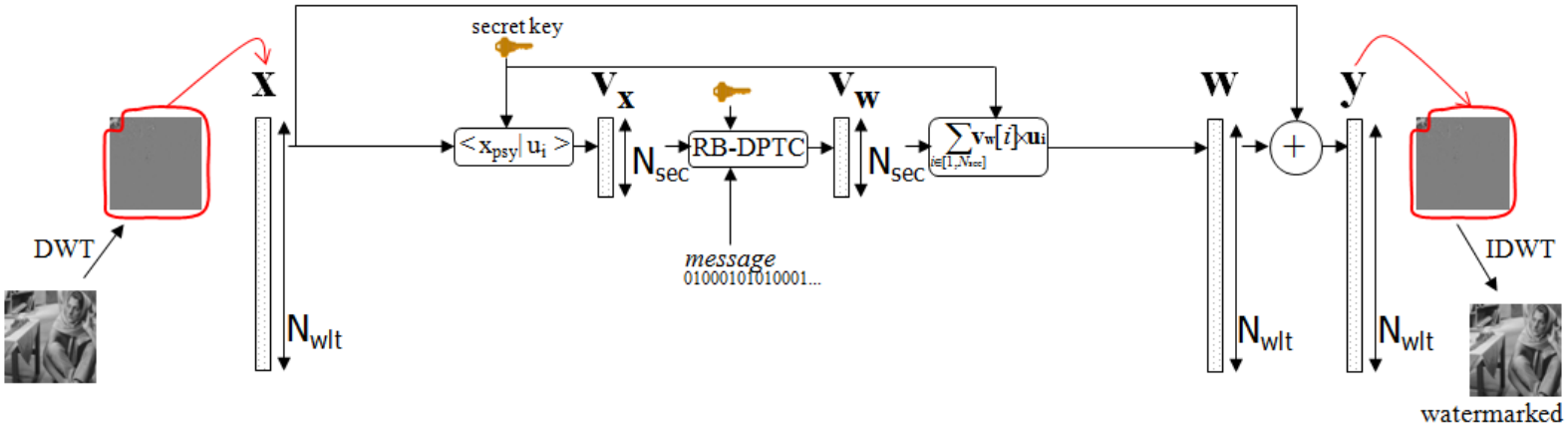
ALGORITHME RB-DPTC
- ESPACE D'INSERTION -



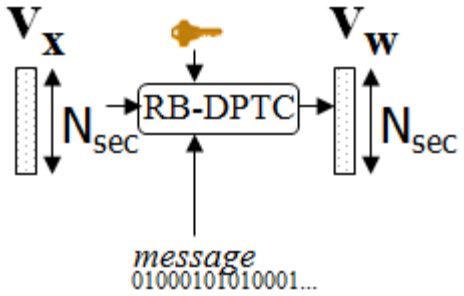
Propriétés :

- Bonne dispersion $\Rightarrow$ « moins » de super-robustesse,
- Aspect Gaussien de $\mathbf{v_x}$ $\Rightarrow$ bonne propriété canal,
- Ondelettes $\Rightarrow$ bonne propriété psycho-visuel.

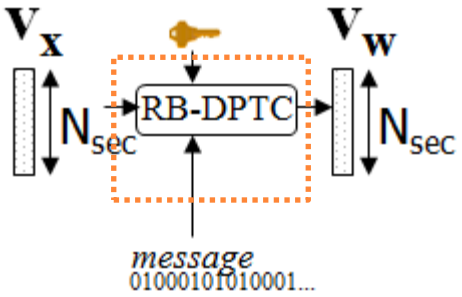
ALGORITHME RB-DPTC



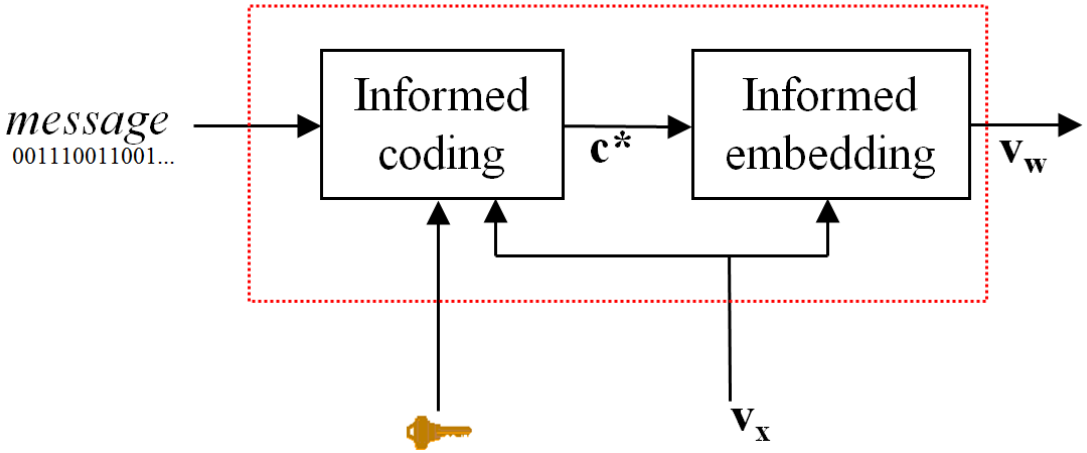
Algorithme RB-DPTC
- Codage et Insertion -



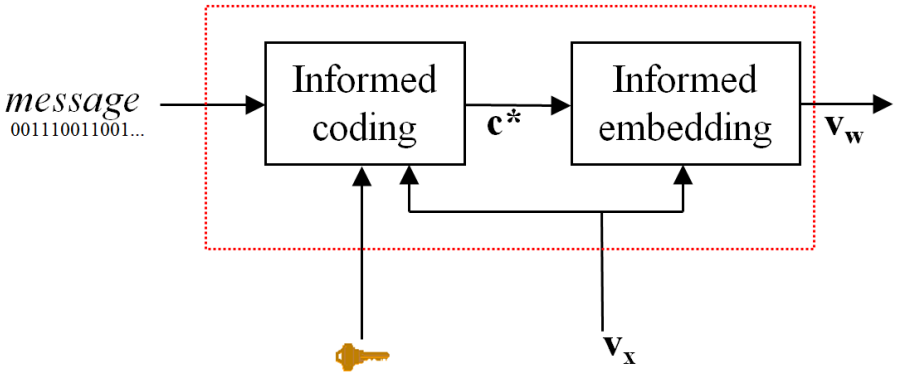
Algorithme RB-DPTC
- Codage et Insertion -



≡



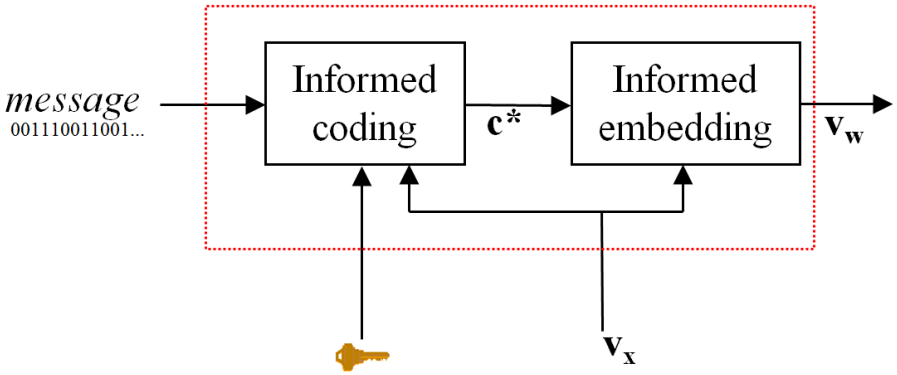
RB-DPTC watermarking scheme - Codage et Insertion -



- Codage informé :
  - identique à [1] (Treillis + Viterbi)
  - Entrées = ($\mathbf{v_x}$ et *message*), Sortie = mot de code **c***

[1] « Applying Informed Coding and Informed Embedding to Design a Robust, High Capacity Watermark », Miller, Doërr, and Cox, IEEE TIP'2004.

RB-DPTC watermarking scheme - Codage et Insertion -



- Insertion informée :

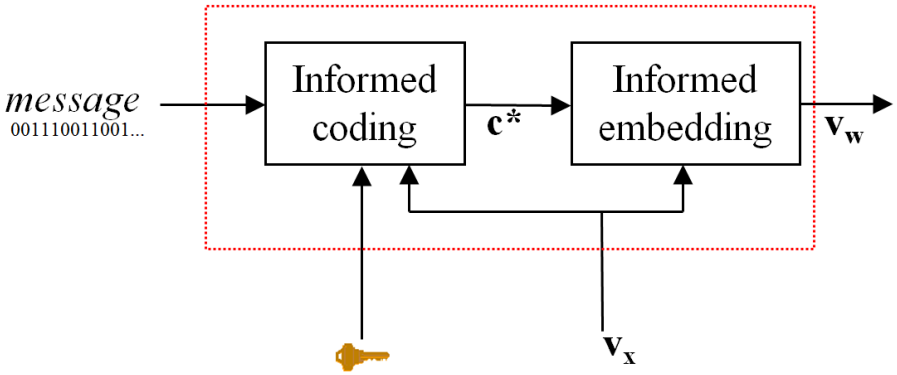
Au décodage :

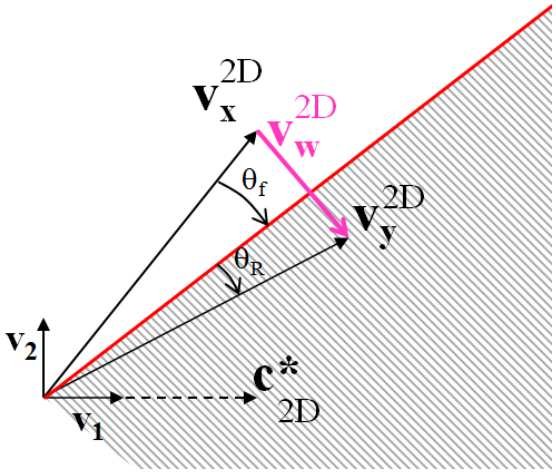
$\tilde{\mathbf{v}}_y$ est le vecteur tatoué attaqué extrait

Le décodeur extrait du livre du code C

le mot de code $\mathbf{c}$ dont l'angle $\theta = (\tilde{\mathbf{v}}_y, \mathbf{c})$ est le plus petit.

RB-DPTC watermarking scheme - Codage et Insertion -





- Algorithme d'insertion informée :
  1. Calculer le plan de "Miller, Cox, Bloom"
  2. Trouver dichotomiquement la frontière (θ_f) de Voronoï
  3. Tourner $\mathbf{v_x}$ d'un angle orienté $\max(\theta_f + \theta_R, (\widehat{\mathbf{v_x}, \mathbf{c}^*}))$

$\mathbf{v_w} = \mathbf{v_y} - \mathbf{v_x}$

Evaluations expérimentales

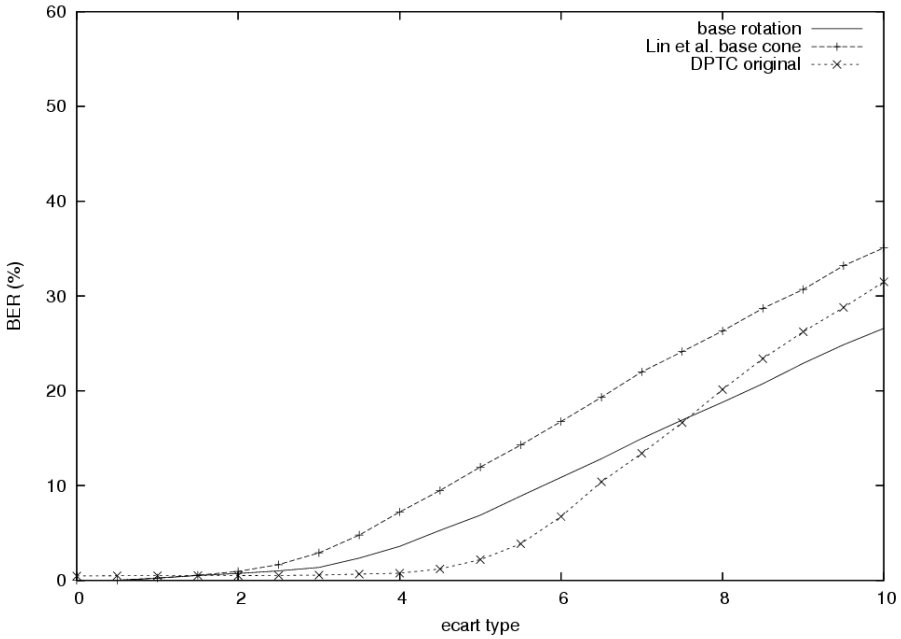
Protocole d'évaluation

- 100 images 256×256
- Payload = 1 bit inséré dans 64 pixels
  $\Rightarrow$ 1024 bits insérés
- Labels des arcs de sortie : distribution Gaussienne
- 12 coefficients par arc

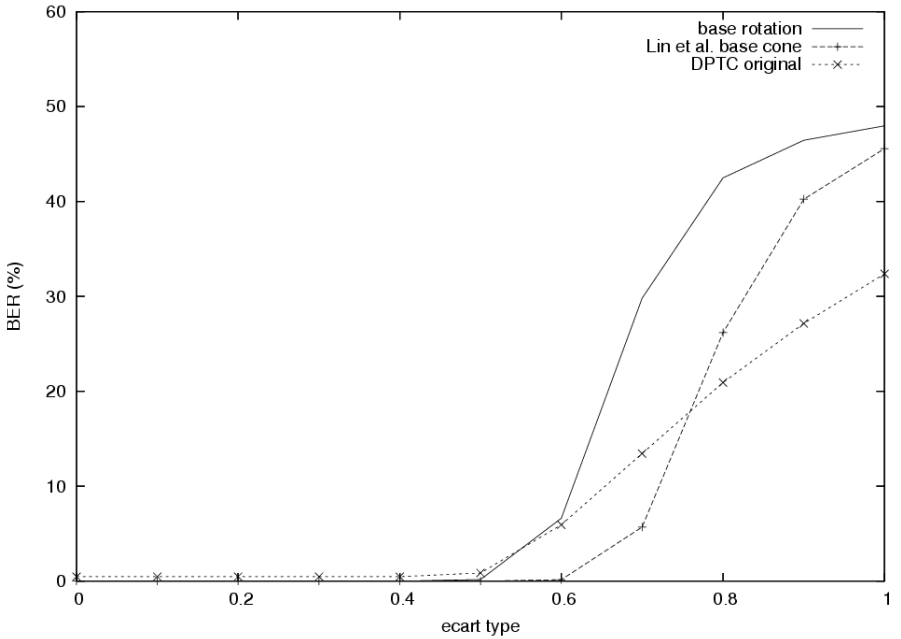
Algorithmes

- 3 Algorithmes en compétition (PSNR moyen= 42.6 dB) :
  - DPTC **original** (DCT - 64 états et 64 arcs par état)
  - ~~Lin *et al.* – **basé cône** (ondelette - 128 états, 128 arcs/état)~~
    PSNR moyen max = 34.2 dB
  - RB-DPTC – **basé rotation** (ondelette - 128 états, 128 arcs /état)
- 4 attaques :
  - Bruit Gaussien,
  - Filtrage Gaussien,
  - « Scaling » valumétrique,
  - Attaque Jpeg.

Attaques (1)

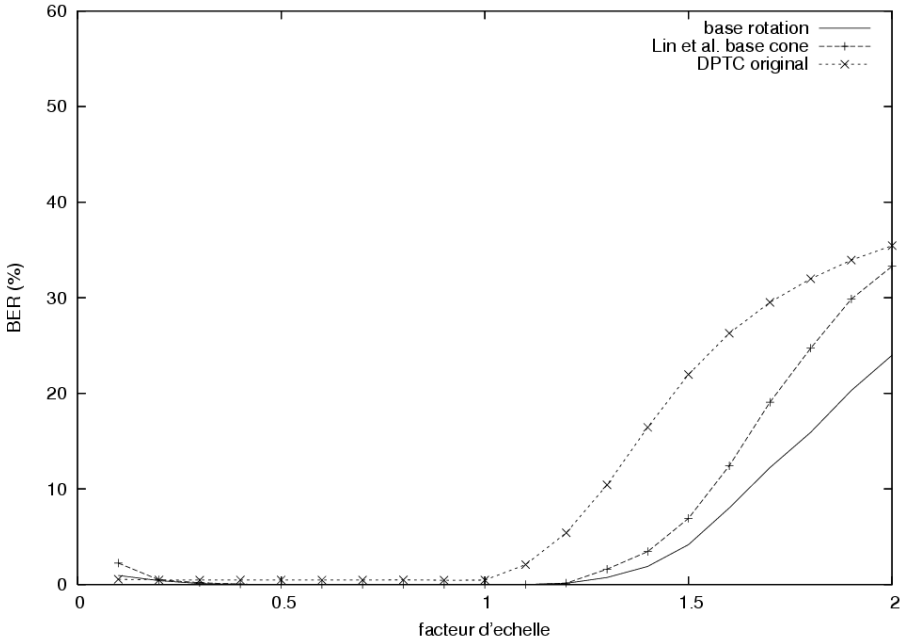


Attaque par bruit Gaussien

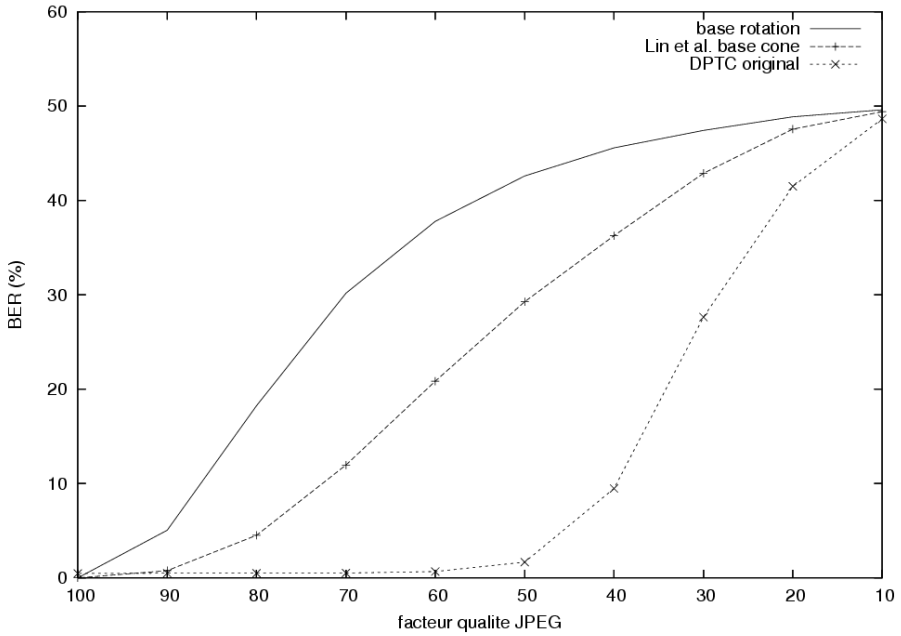


Attaque par filtrage Gaussien

Attaques (2)



Attaque par scaling valumétrique



Attaque Jpeg

Conclusion & discussion

Conclusion & Discussion
- RB-DPTC -

- Un espace secret ayant de bonnes propriétés
  (psychovisuelles, canal, moins de super-robustesse)

- Une insertion basée rotation :
  - de faible complexité calculatoire (/ à DPTC original),
  - ayant un bon compromis robustesse-distorsion,
  - de sécurité « au moins équivalente » à DPTC original

- Performances comparables au DPTC original (sauf jpeg)

Conclusion & Discussion
- RB-DPTC -

- Problèmes abordés :
  - Complexité calculatoire des projections [5]
  - Utilisation d'espace psychovisuel [6]

- Problèmes ouverts :
  - Sensibilité à l'attaque Jpeg,
  - Sensibilité à l'attaque par régression de Westfeld [7],
    (remarque: contre attaque proposée dans [8])
  - Etude de la sécurité.

[5] « A Fast Embedding Technique For Dirty Paper Trellis Watermarking,», Chaumont, IWDW'2009.
[6] « Psychovisual Rotation-based DPTC Watermarking Scheme», Chaumont, EUSIPCO'2009.
[7] « A Regression-Based Restoration Technique for Automated Watermark Removal », Westfeld, MM&Sec'2008.
[8] « Expectation Maximization decoding of Tardos probabilistic fingerprinting code », Charpentier et al., SPIE'2009

Laboratoire
d'Informatique
de Robotique
et de Microélectronique
de Montpellier

LIRMM

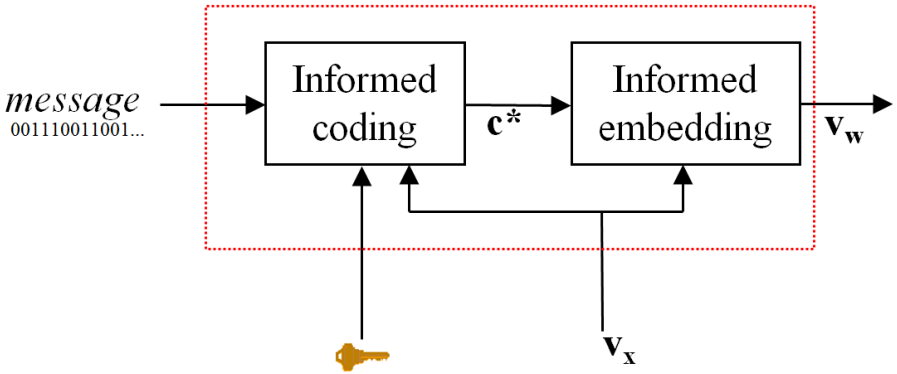
Une nouvelle technique pour le tatouage par Dirty Paper Trellis Code (DPTC)

Marc CHAUMONT (LIRMM)

XXIIe Colloque GRETSI - Traitement du Signal et des Images - Université de Bourgogne - Dijon - 8-11 septembre 2009.

Annexe

RB-DPTC watermarking scheme - Codage et Insertion -



- Insertion informée :

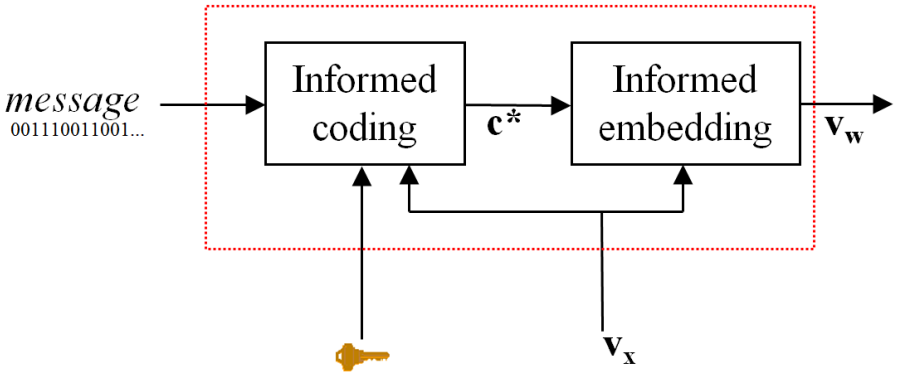
  Déplacer $\mathbf{v}_x$ pour que $\mathbf{v}_y$ (= $\mathbf{v}_x$ + $\mathbf{v}_w$) soit dans la région de Voronoï du mot de code **c***

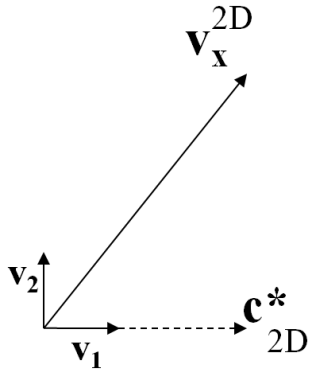
  Au décodage :

  - C : livre du code,
  - $\tilde{\mathbf{v}}_y$: vecteur tatoué et attaqué
  - $\mathbf{c}$: mot-de-code décodé :

    $$\mathbf{c} = \arg_{\mathbf{c}^i} \max_{\forall \mathbf{c}^i \in \mathcal{C}} (||\tilde{\mathbf{v}}_y||.||\mathbf{c}^i||.cos\theta_i)$$

RB-DPTC watermarking scheme - Codage et Insertion -

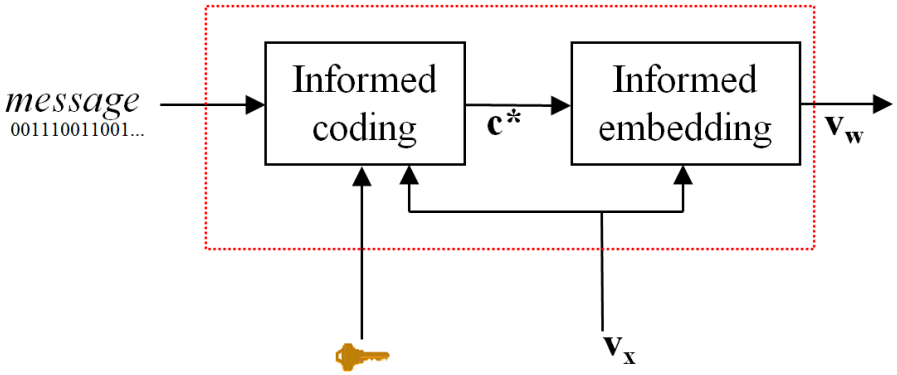


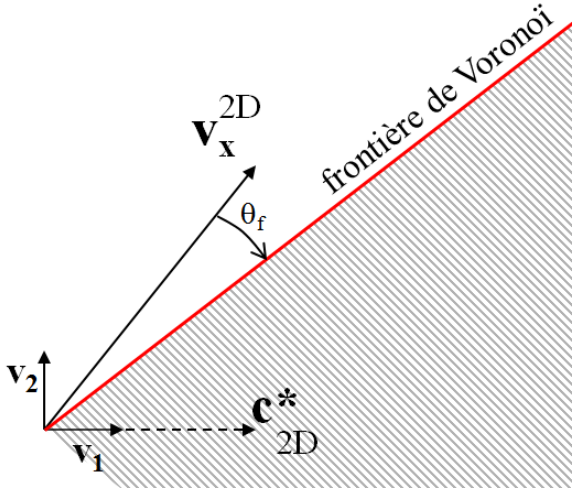


- <u>Algorithme d'insertion informée :</u>
  1. Calculer le plan de "Miller, Cox, Bloom"
     - Base ortho-normalisée (v1, v2)
     - $\mathbf{v_x}$ et **c*** appartiennent à ce plan
     - Algorithme de Gram-Schmidt:

$$\mathbf{v_1} = \frac{\mathbf{c}^*}{||\mathbf{c}^*||} \qquad \mathbf{v_2} = \frac{\mathbf{v_x} - (\mathbf{v_x}.\mathbf{v_1})\mathbf{v_1}}{||\mathbf{v_x} - (\mathbf{v_x}.\mathbf{v_1})\mathbf{v_1}||}$$

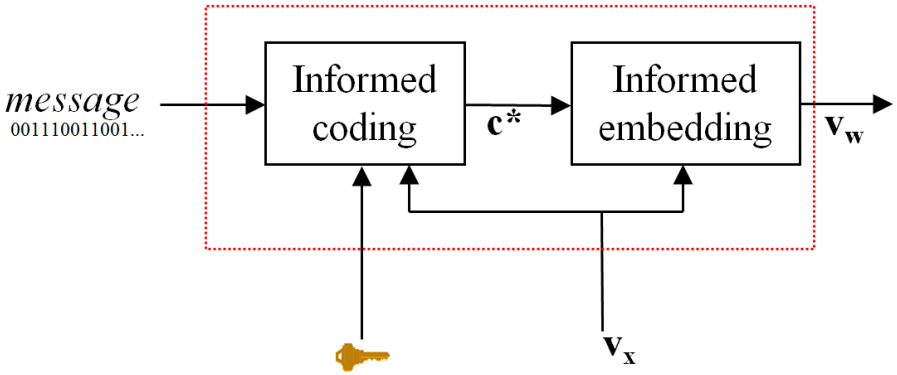
RB-DPTC watermarking scheme - Codage et Insertion -

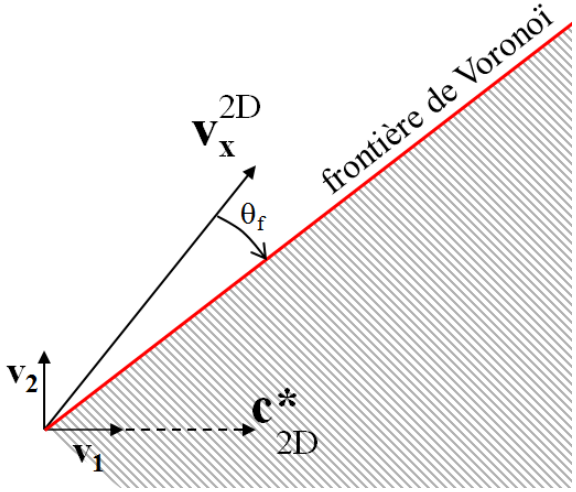




- <u>Algorithme d'insertion informée :</u>
  1. Calculer le plan de "Miller, Cox, Bloom"
  2. Trouver dichotomiquement la frontière (θ_f) de Voronoï

RB-DPTC watermarking scheme - Codage et Insertion -





- <u>Algorithme d'insertion informée :</u>
  1. Calculer le plan de "Miller, Cox, Bloom"
  2. Trouver dichotomiquement la frontière (θ_f) de Voronoï :

ITERER

tourner $\mathbf{v_x}$ de $(\theta^{min}_f + \theta^{max}_f)/2$ et obtenir un $\mathbf{v_y}$ temporaire

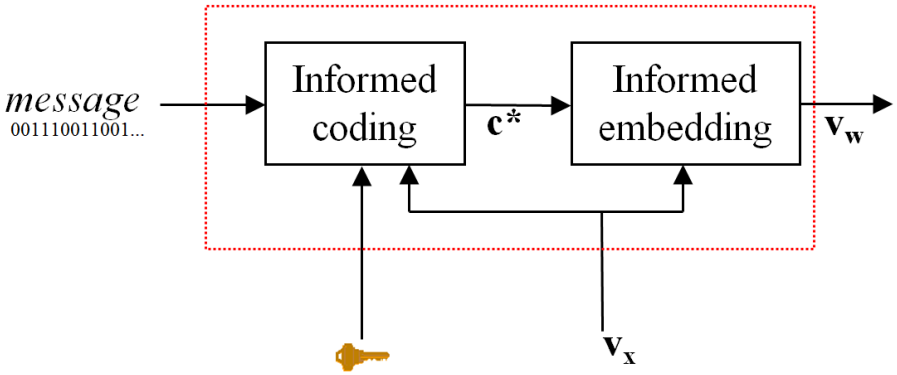
trouver le mot de code $\mathbf{c}$ le plus proche de $\mathbf{v_y}$ (Viterbi)

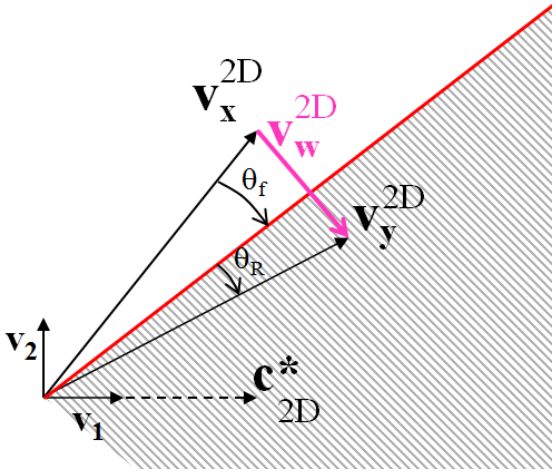
si ($\mathbf{c} == \mathbf{c^*}$)

alors $\theta^{max}_f \leftarrow (\theta^{min}_f + \theta^{max}_f)/2$

sinon $\theta^{min}_f \leftarrow (\theta^{min}_f + \theta^{max}_f)/2$

RB-DPTC watermarking scheme - Codage et Insertion -





- <u>Algorithme d'insertion informée :</u>
  1. Calculer le plan de "Miller, Cox, Bloom"
  2. Trouver dichotomiquement la frontière (θ_f) de Voronoï
  3. Tourner $\mathbf{v_x}$ d'un angle orienté $\max(\theta_f + \theta_R, (\widehat{\mathbf{v_x}, \mathbf{c}^*}))$

$\mathbf{v_w} = \mathbf{v_y} - \mathbf{v_x}$