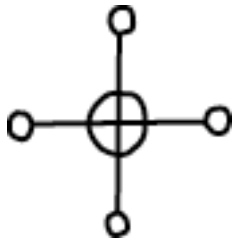
Fabriano

sécurité, tatouage, stéganographie et législation
autour des documents multimedia



Une histoire avec des voleurs, des gendarmes et des juristes.

Domaine

- Sécurité et cadre juridique des techniques de filigranes numériques.

- La stéganographie et le tatouage robuste.

Participants

- **LSS** : Laboratoire des Signaux et Systèmes,
- **LIS** : Laboratoire des Images et des Signaux,
- **CERDI** : Centre d'études et de Recherche en Droit de l'Immatériel,
- **TEMICS** : projet INRIA.

- 6 permanents, 2 postdocs (ACI-SI), 4 doctorants.

Problématique I

- Tatouage robuste
  - But :

    Cacher = lier fortement contenu et message caché.
  - Application :

    Défense du copyright, protection de copie, DRM.
  - Rôle :
    - Gendarmes : incruster un tatouage robuste et sûr.
    - Voleurs : retirer le tatouage à moindre distorsion.

Problématique II

- Stéganographie
  - But :

    Cacher = dissimuler de l'information.
  - Application :

    Spyware, terrorisme.
  - Rôle :
    - Voleurs : cacher de l'information dans des images,
    - Gendarmes : détecter la présence d'information cachée.

Problématique III

Intégration des contraintes juridiques

- Assurer la **légalité des travaux de recherche** (règles relatives à la fraude informatique, etc.)

- Vérifier la conformité des **résultats de recherche au droit en vigueur** (respect de la vie privée et des données personnelles, du secret des correspondances, droit de la preuve etc.),

- Garantir la **pérennité des techniques développées** (anticipation des évolutions législatives, analyse des implications juridiques de chaque solution)

Résultats - I

Tatouage robuste

Les voleurs

Théorie / Méthodologie

- La sécurité repose sur la clé secrète (Kerckhoffs)
- Mesure de la fuite d'information (Shannon)
  - Information mutuelle (clé = v.a. discrète),
  - Information de Fisher (clé = v.a. continue).
- Interprétation
  - Équivocation,
  - Borne de Cramèr-Rao.
- Analyse par contexte (Diffie-Hellman)

$\Rightarrow$ Adaptation des bases de la cryptanalyse au tatouage.

- Application aux techniques classiques
  - Substitution,
  - Etalement de spectre.

La pratique

- Construction d'estimateurs
  - Maximum de vraisemblance, Expectation Maximisation, Set Membership…
  - Identification entrée / sortie, Analyse en composantes indépendantes.
- Tests sur des banques d'images
  - Étalement de spectre,
  - Quantization Index modulation.

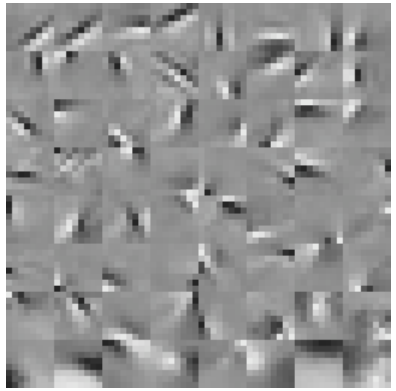
⇒ Niveaux de sécurité faibles (1000 images)

Pour en savoir plus:

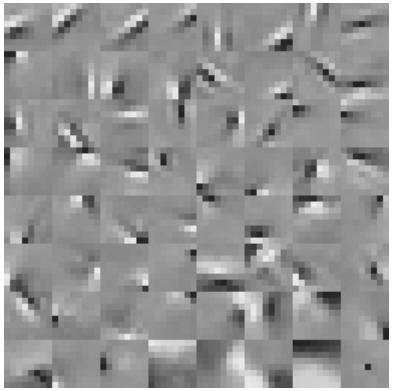
F. Cayre, C. Fontaine et T. Furon, « WATERMARKING SECURITY: THEORY AND PRACTICE », IEEE Trans. Signal Processing, Oct. 2005, vol. 53, nb. 10.

Exemple I

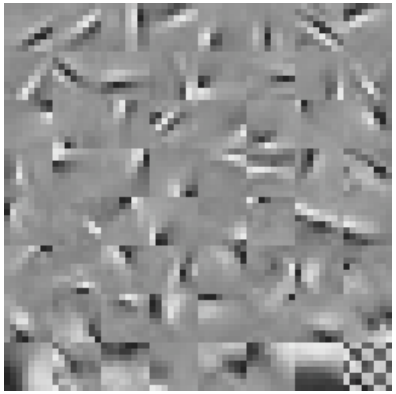
- But : Identification du domaine d'insertion
- Méthode : recherche de traces dues au tatouage par ACI.



ACI image originale



Insertion spatiale
(PSNR=50dB)



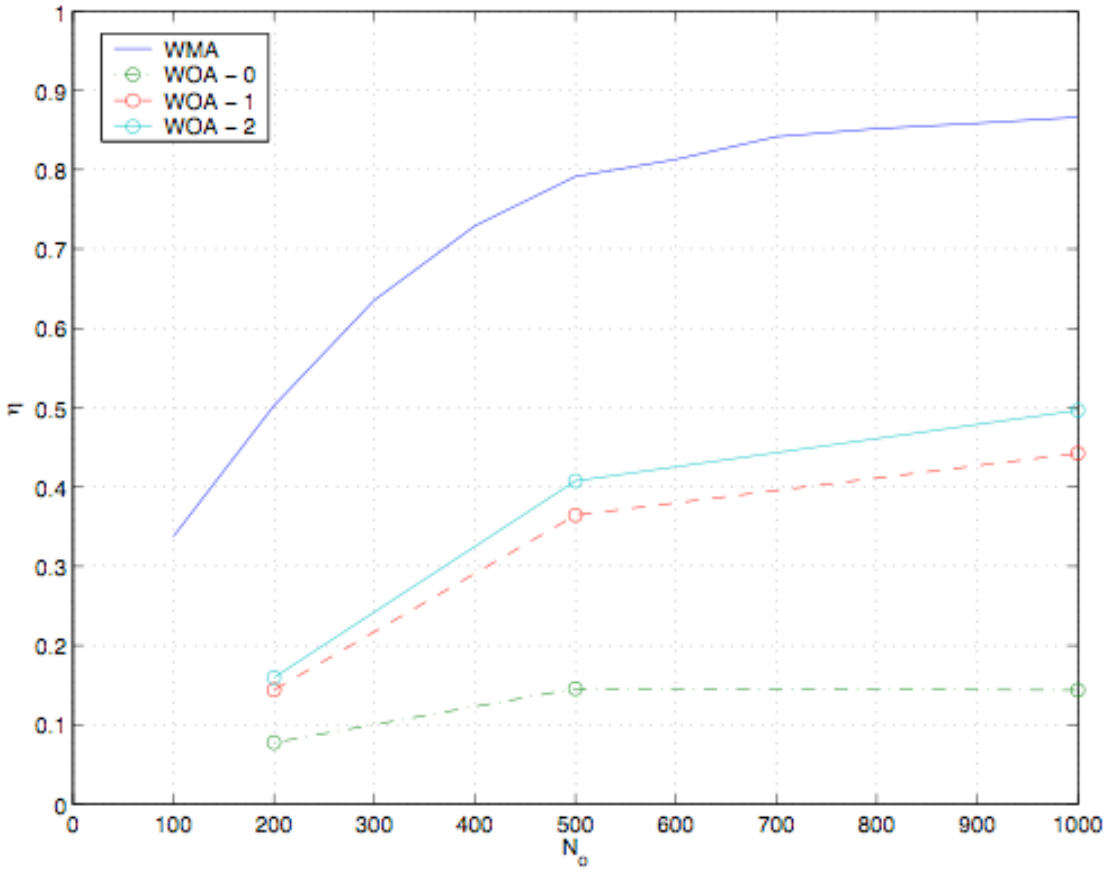
Insertion fréquentielle
(PSNR=42dB)

Pour en savoir plus:

P. Bas, J. Hurri, « SECURITY OF DM QUANTIZATION WATERMARKING SCHEMES: A PRACTICAL STUDY FOR DIGITAL IMAGES », IWDW 05, Sienne, Italie.

Exemple II

But : estimation de la clé secrète d'une technique basée étalement de spectre (8 bits, 38 dB)



Message caché connu (Max. vraisemblance)

Message caché inconnu (Expectation Max.)

Impact

Robustesse
Pirate A (PSNR=22dB)

Sécurité
Pirate B (PSNR=36dB)

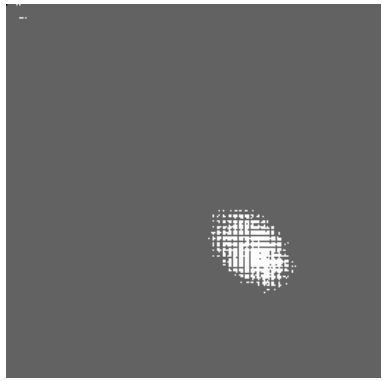
Résultats - II

Stéganographie

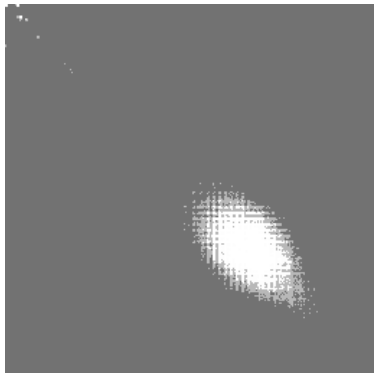
Les gendarmes

Stéganalyse “ad hoc”

- Stego-système a priori connu.
- Comparaison des statistiques des images naturelles / suspectes.



matrice de coocurrence avant insertion.



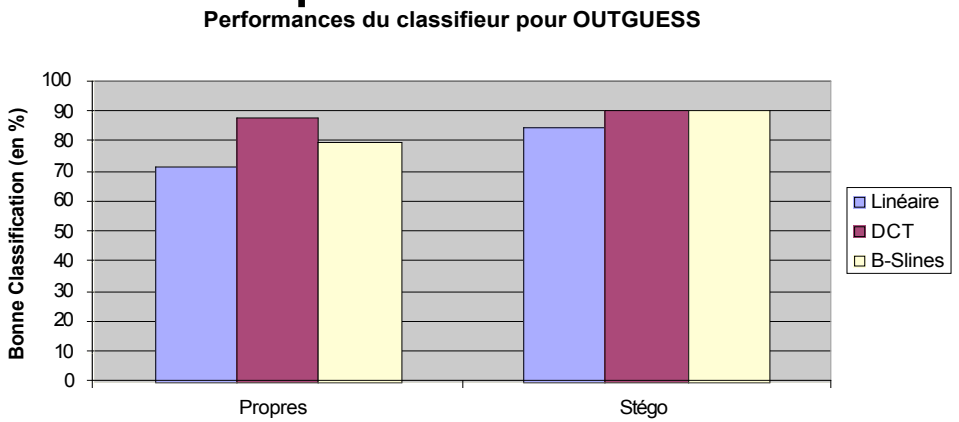
matrice de coocurrence après insertion.

Pour en savoir plus:

B. Roue, P. Bas, J-M Chassery "IMPROVING LSB STEGANALYSIS USING MARGINAL AND JOINT PROBABILISTIC DISTRIBUTION” , Multimedia and Security Workshop 2004, Magdeburg, Germany.

Stéganalyse par apprentissage

- Une méthode aveugle mais demandant un apprentissage.
- 2 étapes
  - Extraction de caractéristiques pertinentes
  - Classification par SVM.



Pour en savoir plus:

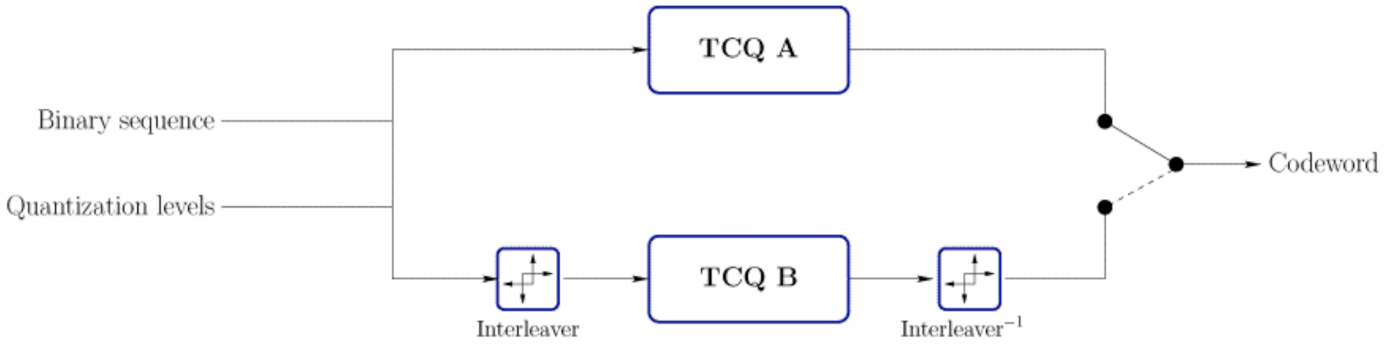
B. Roue, P. Bas and J-M. Chassery: "INFLUENCE DES VECTEURS CARACTÉRISTIQUES EN STÉGANALYSE PAR SÉPARATEURS À VASTES MARGES", Gretsi 2005, Louvain-la-Neuve, Belgique.

Résultats - III

Tatouage

Les nouveaux gendarmes

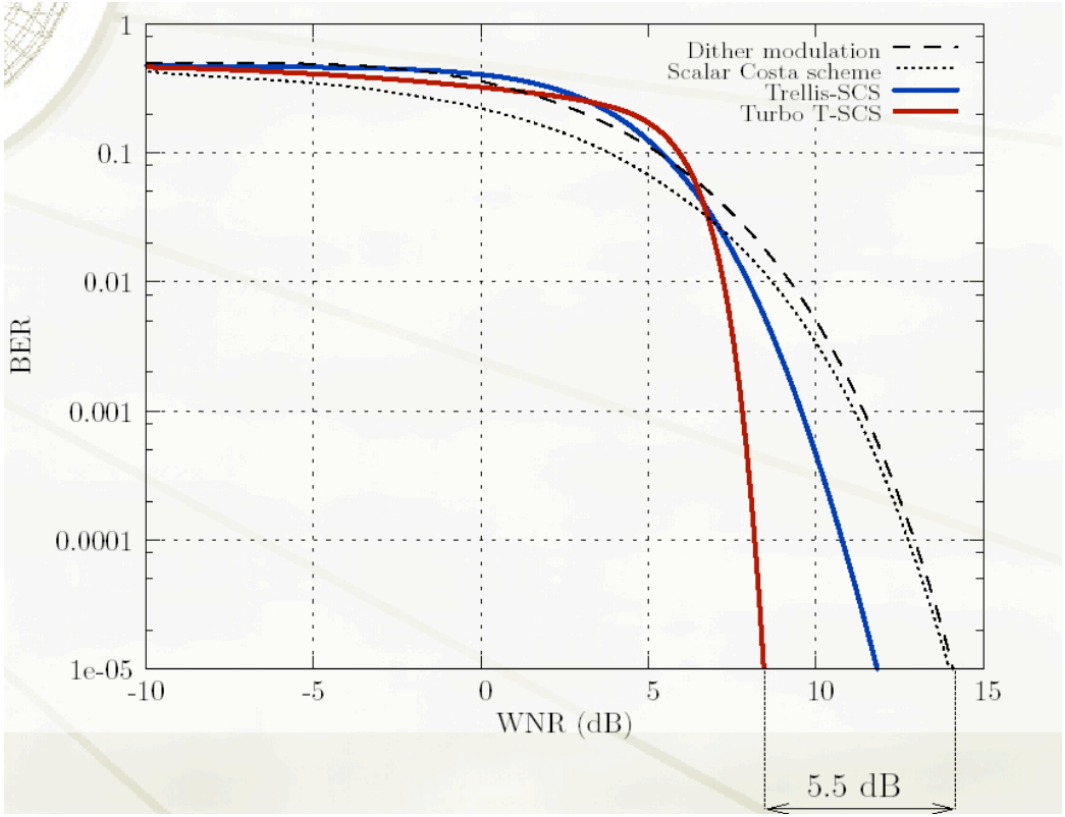
Utilisation de la Turbo - TCQ



- Décevante en codage source [Chappelier03].
- Prometteuse en tatouage.
  - Met en oeuvre élégamment le schéma de Costa (communication avec information adjacente),
  - Améliore très nettement la robustesse,
  - Echappe aux analyses sécurité vues précédemment.

Tatouage robuste et Turbo - TCQ

Performances :



Pour en savoir plus:

G. Le Guelvouit, « TTCQ codes for watermarking», gleguelv.free.fr/wt/ttcq/index.html

Résultats - IV

stéganographie

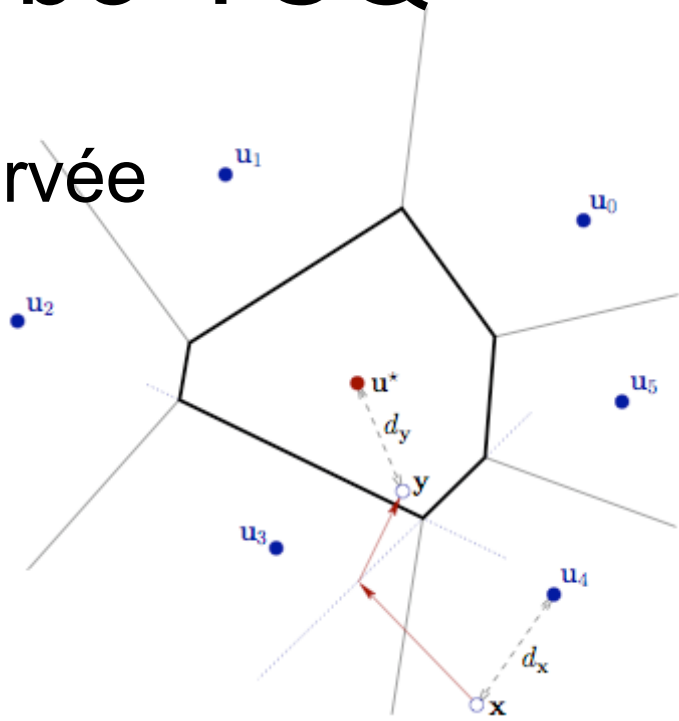
Les nouveaux voleurs

Utilisation de la Turbo-TCQ

- Statistiques du signal hôte préservée

$$d_x \sim d_y$$

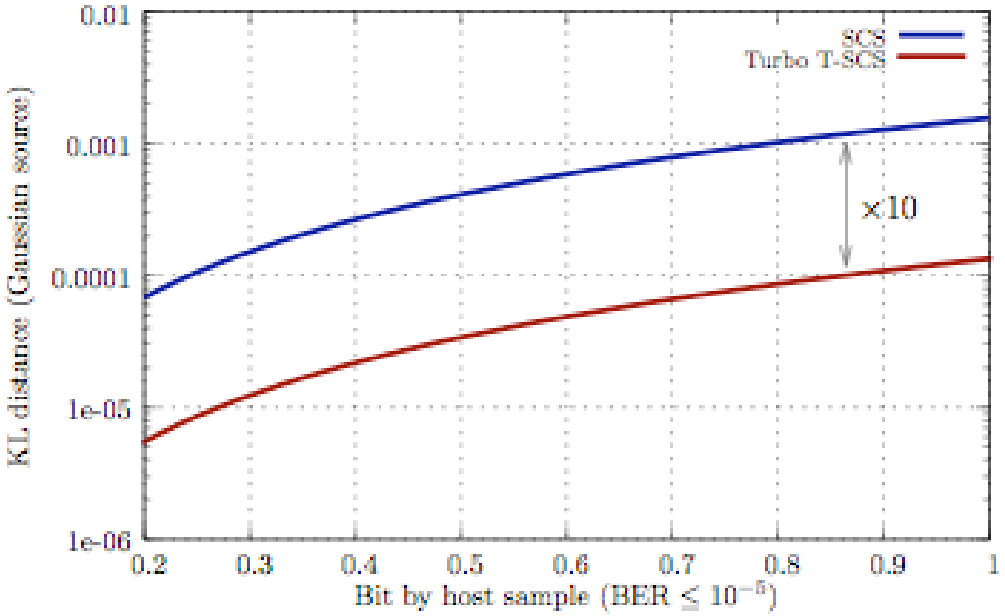
- Fonctionne pour toute pdf.



- Stego-système à clé publique
  - Initialisation à faible rendement:
    - le message caché est un aléa chiffré par un crypto-système à clé publique.
  - Permanent à haut rendement :
    - la clé secrète est l'aléa.

Performances (permanent)

Sécurité 10 fois supérieure [Furon'02]



Pour en savoir plus:

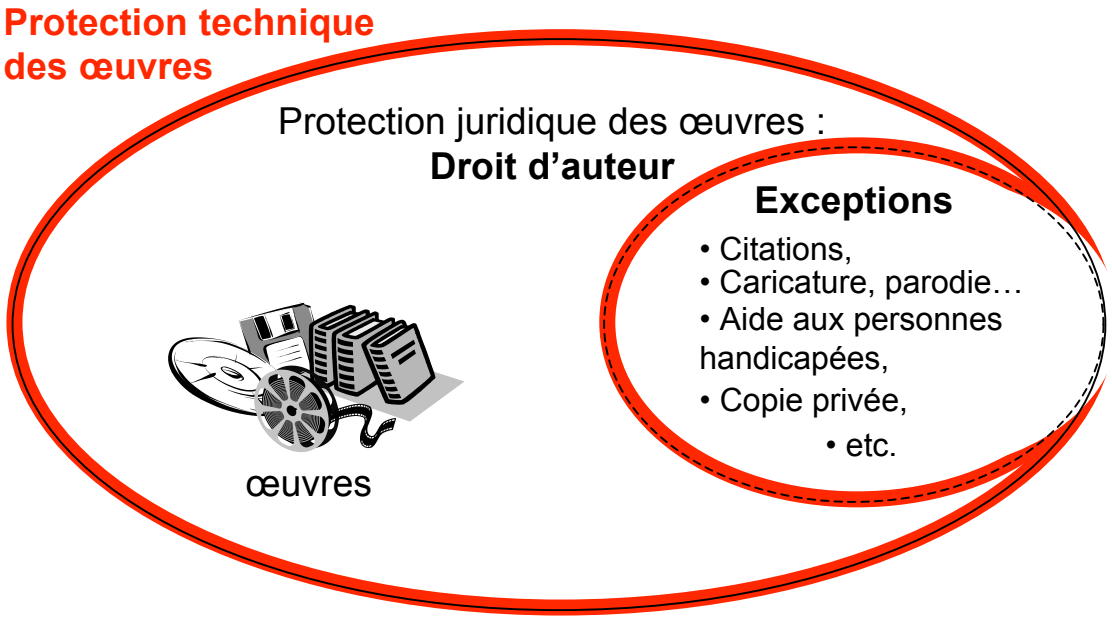
G. Le Guelvouit, « TRELLLIS-CODED QUATIZATION FOR PUBLIC-KEY WATERMARKING», ICASSP, Mars 2005.

Résultats - V

Protection de copie

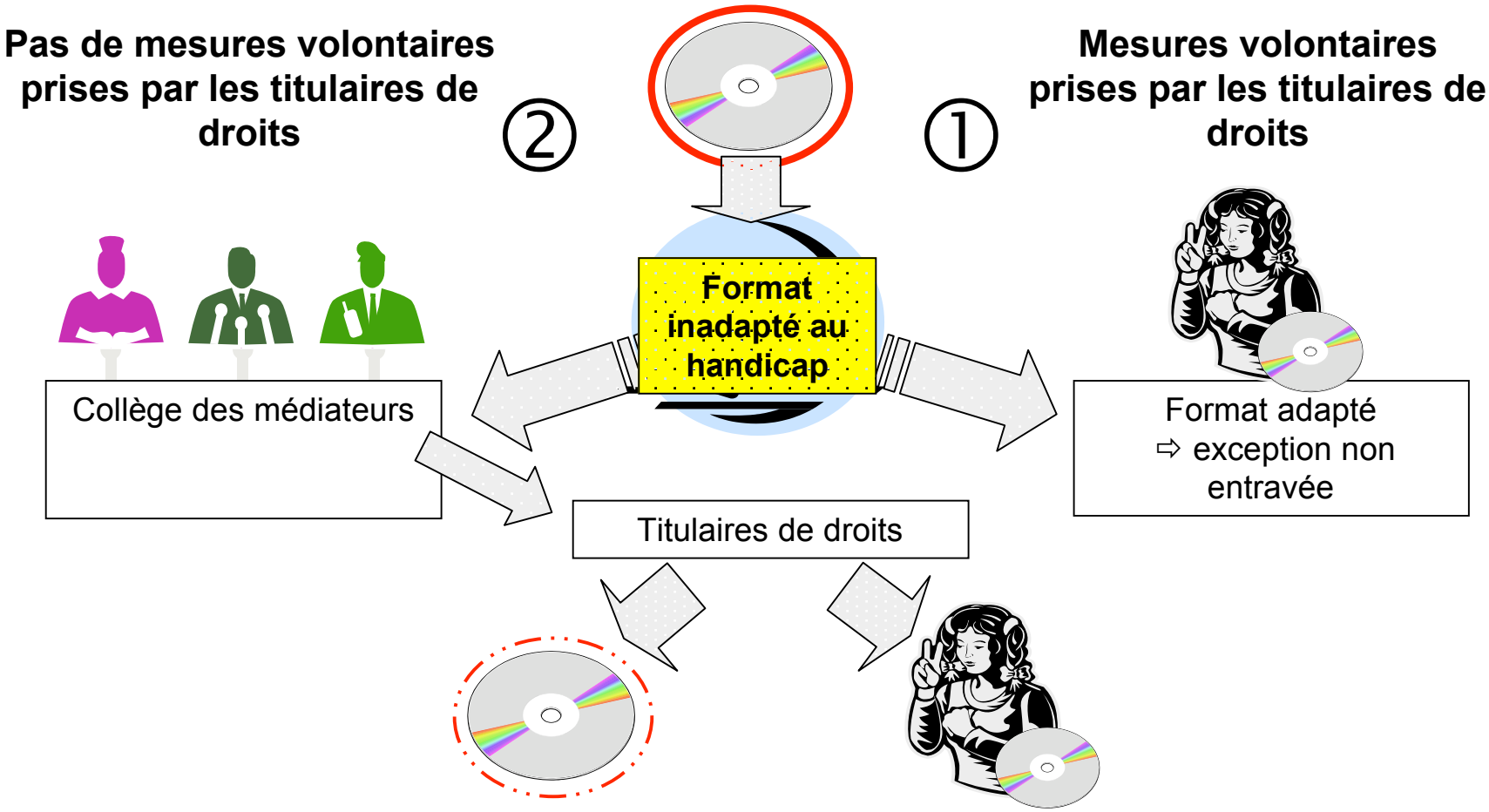
Les juristes

Cadre juridique de la protection technique des œuvres



Les mesures techniques de protection des œuvres doivent respecter la « balance des intérêts » définie par le Législateur.

Illustration : l'exception au profit des personnes handicapées



Digital Rights and Exemptions Management Systems

- Principe

  Intégrer dès l'origine la garantie des exceptions aux systèmes de protection et de gestion électronique des droits (DRM).

- Avantages :
  - connaître et maîtriser l'ensemble des paramètres de sécurité du système,
  - économiser sur les coûts de gestion des demandes des utilisateurs (mesures volontaires) et, le cas échéant, de procédure (collège des médiateur)

Pour en savoir plus:

T. Maillard & T. Furon, « TOWARDS DIGITAL RIGHTS AND EXEMPTIONS MANAGEMENT SYSTEMS», Computer Law & Security Report, Vol. 20, no. 4, 2004, p. 281-287.

http://www.mtpo.org/content/0407011.pdf

Travaux futurs

- Etude critique de la faisabilité des choix législatifs (transposition de la directive sur droit d'auteur).

- Niveaux de sécurité des nouvelles techniques de tatouage robuste basées TTCQ.

- Stéganalyse des stego-systèmes basés TTCQ.

Conclusion : sécurité et tatouage

- Chaud
  - Maintenant que les techniques sont robustes, il devient urgent d'analyser la sécurité.
- Sous-estimé
  - La communauté tatouage n'est pas encore consciente.
- Amusant
  - Nouveau domaine : la sécurité avec des outils traitement du signal.

Conclusion : sécurité et tatouage

- Ce ne sont que les débuts
  - Autres applications : authenticité, fingerprint

- Nous ne sommes pas des hackers.
  - On ne casse rien, on estime les niveaux de sécurité.
  - Notre but est d'avertir la communauté tatouage.