Tatouage sûr

Marc Chaumont 70%
William Puech 30%

Équipe ICAR

originale

tatouée (algo de BOWS-2)

Tatouage sûr

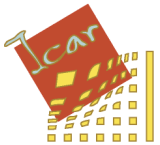
Définition :

Le tatouage est l'art d'altérer un média (une image, un son, une vidéo ...) de sorte qu'il contienne un message le plus souvent en rapport avec le média, le plus souvent de manière imperceptible et le plus souvent de manière robuste.

originale

tatouée (algo de BOWS-2)

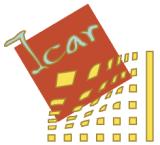
Tatouage sûr



Quelques dates clefs :

- 1990 : Naissance du tatouage numérique,
- 1998 : Théorisation et apparition des schémas informés,
- 2005 : Mise en évidence de la notion de **sécurité** et de **fuite d'information**.

Tatouage sûr

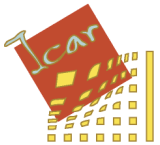


Constat :

- Algorithme zéro-bit :
  Broken Arrows [BOWS-2 2008].
  ⇒ évaluation non terminée en terme de sécurité.

- Algorithmes multi-bits informés :
  SCS [Eggers et al. 2003] , Treillis [M.L Miller et al. 2004], Tatouage naturel [Bas et Cayre 2006], Tatouage circulaire [Mathon et al. 2007].
  ⇒ évaluation encore moins avancée en terme de sécurité.

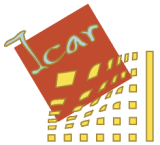
Tatouage sûr



L'objectif de cette thèse :

étudier et proposer :
- des attaques,
- des contres-attaques,
- de nouveaux schémas de tatouage à faible et forte capacité qui soient robustes et également sûrs.

Tatouage sûr



Déroulement de la thèse :

- Étude du schéma Broken Arrows (zero-bit) [Furon et Bas 2008],
- Création d'attaques génériques et efficaces en s'inspirant des travaux sur la régression [Westfeld 2008], sur l'attaque à la sensibilité [Comesaña et Pérez-González 2007] ainsi que la séparation de source [Mathon et al. 2007].
- Étude des schémas à forte capacité,
- Adapter des précédents résultats,
- Proposition de nouvelles attaques, ou de nouveaux schémas.

Exemple : les travaux menés par Bas et Doërr [P. Bas, Doërr 2007], [Bas et Doërr 2008] montrent qu'il est possible, en simplifiant le schéma de tatouage original basé treillis, de mener une attaque " Watermak Only Attack (WOA)". Cependant, pour l'attaquant, il reste encore à régler le problème de " randomisation " des coefficients. Ce problème pourra être abordé en s'inspirant de l'attaque à la sensibilité [Comesaña et Pérez-González 2006] et de l'estimation des porteuses par séparation de sources [Mathon et al. 2007].