




## Etes vous un hacker dans l'âme ? Attaque d'un système de tatouage




M. Chaumont  
LIRMM (Laboratoire d'Informatique, de Robotique et Microélectronique de Montpellier)  
Equipe ICAR  
161 rue Ada, 34392 Montpellier cedex 5 - France  
Tel : +33 4.67.41.85.14  
Fax : +33 4.67.41.85.00  
[Marc.Chaumont@lirmm.fr](mailto:Marc.Chaumont@lirmm.fr)

**Fall** Download»




1 - Download the marked image from the above link,  
2 - Apply your attacks to remove our watermark  
3 - Upload the modified image with the form below.  
**Remember that you have to maintain the highest PSNR!!!**

**Louvre** Download»



1 - Download the marked image from the above link,  
2 - Apply your attacks to remove our watermark  
3 - Upload the modified image with the form below.  
**Remember that you have to maintain the highest PSNR!!!**

**Casimir** Download»



1 - Download the marked image from the above link,  
2 - Apply your attacks to remove our watermark  
3 - Upload the modified image with the form below.  
**Remember that you have to maintain the highest PSNR!!!**

Figure : Page de soumission des images après attaque (<http://bows2.gipsa-lab.inpg.fr/>)

La compétition BOWS-2 (Break Our Watermarking System) a débuté le 17 Juillet 2007. L'objectif est de faire disparaître le tatouage embarqué dans 3 images différentes. La compétition se décompose en trois phases : la première s'est achevée le 17 octobre 2007, la deuxième va du 17 octobre au 17 janvier 2008, la troisième du 17 janvier 2008 au 17 avril 2008. L'objectif scientifique de cette compétition est de mieux comprendre les mécanismes de sécurité du domaine du tatouage. En particulier, dans la troisième étape de cette compétition, on s'intéresse aux attaques par collusion (10000 images sont tatouées avec la même clé privée et les sources des algorithmes d'insertion et de détection sont fournis).

L'objectif du stage sera de faire un état de l'art sur les notions de sécurité ainsi que sur les attaques par collusion puis d'implémenter des solutions d'attaque.