Partage d'images JPEG secrètes

Pauline Puteaux*[1]

[1]CNRS, CRIStAL, Lille – Centre National de la Recherche Scientifique - CNRS – France

Résumé

De nombreuses méthodes de sécurisation des images JPEG ont été proposées pour lutter contre les menaces sur Internet. En particulier, des méthodes de chiffrement ont été spécialement conçues pour sécuriser visuellement les images JPEG : on parle alors de "crypto-compression". L'inconvénient des méthodes de crypto-compression est de ne dépendre que d'une seule clé secrète. Dès lors, si cette clé est perdue, la totalité du contenu de l'image originale secrète l'est également. Dans nos travaux, nous avons proposé une approche de partage d'images JPEG secrètes. Lors de la compression JPEG, le schéma de partage de secret de Shamir sur les corps de Galois est utilisé pendant l'étape de codage de Huffman. Cela garantit la sécurité visuelle de l'image secrète dans le domaine compressé, tout en résolvant le problème de la perte de la clé secrète. Notre approche est entièrement conforme au format JPEG et préserve la taille par rapport à une compression JPEG standard d'une image originale secrète.

*Intervenant