

RESUME

L'utilisation de plus en plus excessive de réseaux de soins impose la préservation l'intégrité et l'authenticité des informations médicales, concernant les patients. La transmission d'informations médicales, et particulièrement les images à travers des réseaux publics, n'est pas sans poser des problèmes de sécurité et de confidentialité. Pour répondre à ce double besoin de sécurité, deux grandes familles de technologies complémentaires se développent. La première s'appuie sur une protection via le cryptage des images. La seconde famille base la protection sur l'insertion de données cachées (IDC) dont le but est d'insérer de manière secrète un message à l'intérieur d'un média, dans notre cas l'image médicale et les données médicales auxiliaires.

Le cryptage sélectif est une manière d'adapter le niveau de sécurité des données à chiffrer à un niveau de protection désiré. Il permet de réduire les ressources informatiques utilisées et les temps de traitement des données surtout pour des applications sensibles. C'est en effet le cas des images médicales prises depuis un appareil médical et devant être envoyées sur le réseau afin d'établir un diagnostic à distance. Cette image doit être transmise rapidement et sûrement : un cryptage sélectif est alors la meilleure solution répondant au compromis (temps/sécurité).

Comme nous nous intéressons au chiffrement sélectif dans le domaine compressé, les techniques proposées doivent répondre à quelques propriétés notamment une compressibilité équivalente et la sécurité.

L'IDC est une technique qui permet d'insérer une capacité très élevée de données dans une image numérique de manière imperceptible. Elle peut être utilisée dans plusieurs domaines, en particulier en imagerie médicale.

Dans le cadre de cette thèse, nos travaux de recherche ont conduit à la création de nouvelles techniques de chiffrement sélectif, dans le codeur JPEG 2000, basées sur des fonctions cryptographiques ne nécessitant parfois pas, la transmission de la clé de chiffrement.

De même, nous avons développé de nouvelles techniques réversibles pour l'Insertion de Données Cachées permettant d'assurer la protection des données sans dégrader l'image. Ces techniques s'adaptent aux fonctionnalités de la norme JPEG 2000.

Mots Clés : Cryptographie, Stéganographie, Cryptage/Chiffrement Sélectif, Compression, JPEG 2000, Insertion de Données Cachées, images médicales, fonctions cryptographiques.