

Introduction générale

Depuis le début des civilisations, le besoin de dissimuler préoccupe l'humanité, la confidentialité apparaissait notamment nécessaire lors des luttes pour l'accès au pouvoir.

Aujourd'hui, de plus en plus d'applications nécessitent la sécurité des données transitant entre deux interlocuteurs via un vecteur d'information comme le réseau de télécommunication actuel, les images sont des données particulières du fait de la quantité importante d'information et de leur disposition bidimensionnelle, la transmission des images soulève donc un nombre conséquent de problèmes qui ne sont pas tous encore résolus, de plus les réseaux informatiques sont complexes et les écoutes illégales nombreuses.

Afin de comprendre l'approche de notre travail de recherche, nous voyons le Problématique abordée. Le major problème concernant à l'aspect sécurité des images sauvegardé ou transmises sur des réseaux, l'image circulant peut être capturée, lue et/ou modifiée, les problèmes abordés dans cette étude sont :

- Ø Comment appliquer les algorithmes cryptographiques sur des données de type image ?
- Ø Quels sont les algorithmes cryptographiques fiables par rapports aux autres ?

D'une manière précise la contribution de notre travail, représenté par les travaux suivant :

- ü Garantir et protéger les images numériques durant le stockage ou la transmission, en utilisant les avantages des deux types de chiffrement (symétrique / asymétrique) : rapidité de chiffrement et la fiabilité de sécurité.
- ü Implémenter une application regroupant plusieurs algorithmes de cryptage et puis les exécuter afin d'obtenir quelques résultats qui vont servir à mener une étude comparative entre ces algorithmes. Ces résultats basés sur calcul de temps d'exécution de chaque cryptosystème et la qualité d'image chiffré.

Plan du mémoire

Le travail réalisé dans ce manuscrit organise en quatre chapitres :

Le premier chapitre présente une introduction aux images numériques, plus précisément, nous présentons quelques terminologies et quelques notions pertinentes dans le domaine des images numériques.

Le deuxième chapitre présente la notion de la cryptographie, les deux principaux schémas de chiffrement en cryptographie standard, le chiffrement à clef publique et le chiffrement symétrique, et autre type de chiffrement « hybride ».

Dans le troisième chapitre nous expliquerons comment appliquons un cryptosystème hybride sur une image pour assurer la confidentialité de l'image numérique.

Dans le quatrième chapitre, on implémente les algorithmes de chiffrement en utilisant le langage Java. Aussi, on présente les résultats expérimentaux concernant le chiffrement d'image et la sécurisation de la clé symétrique.

Pour finir, une conclusion générale sera donnée pour faire le point sur l'ensemble des travaux effectués, nous y présenterons également les perspectives d'études et d'améliorations de notre travail.