Centre d'Etudes Doctorales : Sciences et Techniques et Sciences Médicales

Avis de Soutenance

THESE DE DOCTORAT

Présentée par

Monsieur MOHAMED JARJAR

Discipline : Informatique
Spécialité : Informatique

Sujet de la thèse

Cryptographie et échange sécurisé des données volumineuses

Formation Doctorale " Sciences de l'Ingénieur, Sciences Physiques, Mathématiques et Informatique"

Thèse présentée et soutenue **le samedi 24 juin juin 2023 à 10h** à la Faculté des Sciences et Techniques de Fès, devant le jury composé de :

Nom et Prénom	Titre	Etablissement	
Mohamed BERRADA	PES	Ecole Nationale des Sciences Appliquées de Fès	Président
Abdelhamid BENAZZI	PES	Ecole Supérieure de Technologie d'Oujda	Rapporteur
Fatiha MRABTI	PES	Faculté des Sciences et Techniques de Fès	Rapporteur
Faiq GMIRA	PH	Ecole Supérieure de Technologie de Fès	Rapporteur
Hakim EL FADILI	PES	Ecole Nationale des Sciences Appliquées de Fès	Examinateur
Said NAJAH	PES	Faculté des Sciences et Techniques de Fès	Directeur de thèse
Khalid ZENKOUAR	PES	Faculté des Sciences et Techniques de Fès	Co-Directeur de thèse
Said HRAOUI	PA	Ecole Nationale des Sciences Appliquées de Fès	Invité

Laboratoire de recherche : Systèmes Intelligents et Applications
Etablissement : Faculté des Sciences et Techniques de Fès

Résumé de la thèse

De nos jours, avec la croissance rapide des technologies de l'information et de la communication, et avec le développement d'Internet et l'explosion des médias numériques (sons, images et vidéos) partagés sur différents réseaux de communication tels que les réseaux sociaux, la protection des informations est très demandée, la cryptographie et la stéganographie jouent un rôle important dans la sécurisation et la vérification des informations échangées via les canaux de communication publics. Les images transmises sur ces canaux de communication sont des données spéciales en raison de certaines caractéristiques intrinsèques des images telles que : une grande capacité de données (données volumineuses), une forte corrélation entre les pixels adjacents, verticaux et horizontaux et une grande redondance de l'information. Au cours de cette thèse, nos travaux de recherche ont conduit à la création de trois nouvelles approches pour sécuriser l'information et le transfert des données chiffrées en toute sécurité. La première approche est un crypto-système symétrique par bloc pour le cryptage d'images basé sur l'algorithme de Vigenère avec une profonde amélioration dans la création de grandes S-Box et de fortes fonctions de substitutions attachées aux nouvelles tables. De plus, de nouvelles fonctions de chainages reliant les blocs chiffrés et le bloc clair suivant pour une meilleure protection contre toute attaque différentielle. Ce premier algorithme est constitué de deux tours pour augmenter la complexité d'attaque. La deuxième décrit de profondes améliorations apportées à la technique classique de Hill en surmontant le problème d'invisibilité des matrices de grandes tailles. Un troisième algorithme mis au point en implémentant quelques opérateurs génétiques comme (Mutation, croisement, réversion…) pour le chiffrement d'images couleurs appliqué en utilisant les propriétés génétiques et numérique de l'ADN et de l'ARN. L'analyse des performances de la sécurité basée sur les tests standards les plus significatifs à savoir : l'espace clé de cryptage, la sensibilité à la clé secrète, les tests statistiques (entropie, histogramme, corrélation des pixels adjacents) sur l'image claire et l'image chiffrée, et le temps d'exécution, montre l'efficacité et l'efficience des techniques proposées dans nos algorithmes.

Mots clés : Cryptographie, crypto-systèmes, confusion, permutation, diffusion, chiffrement, déchiffrement, systèmes dynamiques chaotiques, chiffre de Vigenère, chiffre de Hill., algorithmes génétiques, opérateurs génétiques.