



AVIS DE SOUTENANCE DE THESE

Le Doyen de la Faculté des Sciences Dhar El Mahraz –Fès – annonce que

Mr **ES.SABRY Mohammed**

Soutiendra : **le Jeudi 11/05/2023 à 10H00**

Lieu : **FSDM – Centre Visioconférence**

Une thèse intitulée :

**Nouvelles approches de sécurité de données à base des algorithmes
cryptographique**

En vue d'obtenir le Doctorat

FD : Sciences et Technologies de l'Information et de la Communication

Spécialité : Informatique

Devant le jury composé comme suit :

Nom et prénom	Etablissement	Grade	Qualité
Pr MAHDOU Najib	Faculté des Sciences et Techniques, Fès	PES	Président
Pr SATORI Khalid	Faculté des Sciences Dhar El Mahraz, Fès	PES	Directeur de thèse
Pr EL AKKAD Nabil	Ecole Nationale des Sciences Appliquées, Fès	PH	Co-directeur de thèse
Pr HALLI Akram	Faculté des Sciences Juridiques Economiques et Sociales, Meknès	PH	Rapporteur
Pr LAZAAR Mohamed	ENSIAS, Rabat	PH	Rapporteur
Pr NFAOUI El Habib	Faculté des Sciences Dhar El Mahraz, Fès	PES	Rapporteur
Pr SATORI Hassan	Faculté des Sciences Dhar El Mahraz, Fès	PES	Examineur
Pr EL ABDERRAHMANI Abdellatif	Faculté des Sciences Dhar El Mahraz, Fès	PH	Examineur
Pr BOULAALAM Abdelhak	Ecole Nationale des Sciences Appliquées, Fès	PH	Examineur



Résumé :

Ces dernières années, le développement rapide du réseau numérique est devenu une tendance inévitable de la communication moderne. Les données multimédias (images, vidéos, animations, audios, etc.) transmises sur ces réseaux sont des données particulières car elles contiennent beaucoup d'informations. La transmission d'images pose donc un certain nombre de problèmes qui ne sont pas encore entièrement résolus. Il existe plusieurs types de données qui sont très sensible telles que les images médicales, les images militaires, les vidéos conférences et même aussi les images personnelles privées. Le défi c'est de faire la transmission de ces données entre les différents types de périphériques, tout en gardant la confidentialité, l'authenticité et intégrité de ces données.

L'objectif visé par cette thèse est de développer des algorithmes sécurisés et rapides pour la cryptographie des images couleurs, en se basant sur des fonctions chaotiques de type 1D (Logistic Map, Sine Map, Chebyshev Map, et Tent Map) avec des formes géométriques basiques telles que les carrés et le cube. Pour la partie de la confusion, nous avons utilisé une autre transformation de type 2D nommée (Arnold Cat Map), cette transformation nous permet de changer les positions des pixels cryptés.

Pour vérifier l'efficacité et la robustesse de nos algorithmes, nous avons utilisé plusieurs attaques et tests pour la cryptographie des images, tels que : les attaques différentielles, les attaques statistiques, les attaques entropiques, et bien d'autres. Les différents résultats obtenus par nos algorithmes montrent ses performances et sa fiabilité en termes de sécurité, de précision, de confidentialité et de robustesse.

Mots clés :

Cryptage d'images ; Décryptage d'images ; Sécurité ; Fonctions chaotiques ; Cryptographie.



NEW DATA SECURITY APPROACHES BASED ON CRYPTOGRAPHIC ALGORITHMS

Abstract :

In recent years, the rapid development of the digital network has become an inevitable trend in modern communication. The multimedia data (images, videos, animations, audios, etc.) transmitted over these networks are particular data because they contain a lot of information. Image transmission, therefore, poses a number of problems that have not yet been fully resolved. Several types of data are very sensitive, such as medical images, military images, video conferences, and private personal images. The challenge is to transmit this data between different types of devices while maintaining the confidentiality, authenticity, and integrity of this data.

This thesis aims to develop secure and fast algorithms for the cryptography of color images, based on chaotic functions of the 1D type (Logistic Map, Sine Map, Chebyshev Map, and Tent Map) with geometric shapes basics such as squares and the cube. For the confusing part, we used another 2D type transformation named (Arnold Cat Map), this transformation allows us to change the positions of the encrypted pixels.

To verify the efficiency and robustness of our algorithms, we used several attacks and tests for image cryptography, such as differential attacks, statistical attacks, entropic attacks, and many others. The different results obtained by our algorithms show its performance and reliability in terms of security, precision, confidentiality, and robustness

Key Words :

Image encryption ; Image decryption ; Security ; Chaotic Maps ; Cryptography