Nom et Prénom : ELAZZABY FOUZIA
Date de soutenance : 13/05/2023
Directeur de Thèse : KABBAJ SAMIR

Sujet de Thèse :

La cryptographie dynamique des images

Résumé :

Cette thèse propose des primitives cryptographiques à clé secrète qui ont été construites selon trois axes en incorporant des fondements mathématiques et des systèmes chaotiques comme générateurs de nombre pseudo-aléatoires.

Le premier axe met l'accent sur un nouveau schéma de chiffrement des images RGB en utilisant le Groupe multiplicatif Z/nZ et la carte de modulation logistique sinusoïdale 2D .le deuxième axe propose aussi une primitive cryptographique couplant les systèmes laser chaotiques 4D et le groupe de Heisenberg GL2n+1(Z) et le dernier aborde un nouvel algorithme de cryptage que l'on est amené à effectuer un brouillage à haut rendement pour séparer les pixels adjacents à l'aide d'une transformation en zigzag horizontale et verticale.de surcroît, nous combinons deux systèmes chaotiques unidimensionnels 1-DSP et 1-DCP à l'étape de substitution pour propager un petit changement dans l'image simple à tous les pixels de l'image chiffrée en fonction de la valeur des trois bits du bit le moins significatif (LSB).

Ces contributions sont accompagnées de paramètres concrets pour évaluer la robustesse et l'efficacité de ces nouvelles primitives contre les attaques cryptographiques courantes, telles que l'histogramme, l'entropie, l'analyse de corrélation et les attaques différentielles, et de même, nous les avons comparées à diverses approches de la littérature

Abstract:

This thesis proposes secret key cryptographic primitives constructed along three axes using mathematical foundations and chaotic systems as pseudo-random number generators.

The first axis concentrates on a new RGB image encryption scheme based on the Z/nZ Multiplicative Group and the 2D Sinusoidal Logical Modulation board. The second axis also proposes a cryptographic primitive that combines 4D chaotic laser systems and the Heisenberg group GL2n+1(Z), and the final axis is a new encryption algorithm requiring high-throughput interference to separate adjacent pixels using horizontal and vertical zigzag transformations. In the substitution step, we combine two one-dimensional chaotic 1-DSP and 1-DCP systems to propagate a small change in a single image to all pixels of an encrypted image based on the three-bit value of the least significant bit (LSB).

These contributions are accompanied by concrete parameters for evaluating the robustness and efficacy of these new primitives against prevalent cryptographic attacks, such as the histogram, entropy, correlation analysis, and differential attacks, and similarly, we compared them to various literature approaches.