

Centre des Etudes Doctorales Sciences et Techniques
&
Sciences Médicales

AVIS DE SOUTENANCE

ASMAA HILMI

Présentera ses travaux de recherche en vue de l'obtention du Doctorat en
Sciences et Techniques

Intitulé de la thèse :

Système cryptographique visuels basés sur la fonction XOR

<u>Date :</u>	Samedi 16 décembre 2023
<u>Heure :</u>	10 Heures
<u>Lieu :</u>	ENSA - Tanger, (Salle B 020).

Devant le jury :

Membres de jury

Pr. Mohamed MOUSSAOUI	ENSA - Tanger	Président
Pr. Anas HATIM	ENSA - Marrakech	Rapporteur
Pr. Samira KHOULJI	ENSA - Tétouan	Rapporteur
Pr. Ahmed DRISSI	ENSA - Tanger	Rapporteur
Pr. Asaad CHAHBOUN	ENSA - Tanger	Examineur
Pr. Soufiane MEZROUI	ENSA - Tanger	Co-encadrant
Pr. Ahmed EL OUALKADI	ENSA - Tétouan	Directeur de thèse

RESUME

Les techniques et les algorithmes basés sur la cryptographie classique d'une manière générale et la cryptographie visuelle d'une manière particulière sont des concepts fondamentaux très utilisés dans l'analyse et la sécurité d'image, non seulement en raison de leurs efficacités, mais aussi pour l'extraordinaire variété des sujets et des applications où ils sont éclairés. Les travaux proposés dans cette thèse s'intéressent aux développements et implémentation des techniques de cryptage et d'analyse des systèmes cryptographiques d'images basées sur les différentes théories et concepts introduits dans le domaine de la cryptographie. En conséquence, cette thèse présente des contributions théoriques qui sont accompagnées de nombreux résultats expérimentaux et des applications pratiques. Fondamentalement, nos méthodes reposent sur deux concepts clés de la cryptographie moderne : l'utilisation de systèmes chaotiques et la technique de confusion-diffusion. Nous avons élaboré deux approches qui mettent en œuvre diverses cartes chaotiques et techniques mathématiques pour embrouiller et sécuriser l'image confidentielle. De plus, nous avons introduit une autre méthode qui repose sur l'exploitation de la blockchain pour le stockage et la transmission des images de manière décentralisée. Le principe sous-jacent est de crypter simultanément plusieurs images en se basant sur leur décomposition en composants Rouge-Vert-Bleu (RVB), puis de les transmettre à travers un réseau distribué. Ensuite, nous avons exposé la mise en œuvre ainsi que l'évaluation des résultats pour les trois méthodes avancées, en se basant sur des critères tels que le PSNR, l'histogramme, l'entropie, la corrélation et les attaques différentielles. Nos conclusions ont démontré que les trois approches affichent une performance élevée en ce qui concerne la sécurité de l'image et la qualité de restauration de l'image reconstruite.

Mots clés : Cryptographie, Fonction XOR, Crypto-système, chiffrement, déchiffrement, sécurité, Cryptage d'images, théorie de chaos, les cartes chaotiques, schéma cryptographique, cryptographie visuelle, confusion et diffusion, système décentralisé, blockchain, système distribué