

**Pôle des Etudes Doctorales**  
**Centre des Etudes Doctorales Sciences et Techniques et Sciences Médicales**

## **AVIS DE SOUTENANCE DE THESE DE DOCTORAT**

**Madame CHIHI Hasnae**  
**Présentera ses travaux de recherche en vue de l'obtention du Doctorat**



**Formation Doctorale : Sciences et Techniques de l'Ingénieur**  
**Discipline : Informatique**  
**Spécialité : Sécurité Informatique et Machine Learning**

**Le 16/05/2026 à 13H00 à la Salle de Conférence du Pr. Otman Filali  
Meknassi, Ecole Nationale des Sciences Appliquées de Tanger, UAE**

**Sous le thème**

**Les Systèmes Cryptographiques Visuels et leurs Applications**

**Devant le jury composé de :**

| <b>Nom et Prénom</b>    | <b>Etablissement</b> | <b>Qualité</b> |
|-------------------------|----------------------|----------------|
| Pr. EL BRAK Mohamed     | FST de Tanger, UAE   | Président      |
| Pr. EL HAJI Essaid      | FP de Larache, UAE   | Rapporteur     |
| Pr. SERRAJ Taoufik      | FS d'Oujda, UMP      | Rapporteur     |
| Pr. ZOUGARI Tarek       | ENSA de Tanger, UAE  | Rapporteur     |
| Pr. DRISSI Ahmed        | ENSA de Tanger, UAE  | Examineur      |
| Pr. EN-NAIMI El Mokhtar | FST de Tanger, UAE   | Examineur      |
| Pr. CHAHBOUN Asaad      | ENSA de Tanger, UAE  | Directeur      |

*Structure de recherche : Mathematics and Intelligent Systems (MASI)*

## Résumé



La généralisation des systèmes intelligents connectés, tels que les objets connectés, les environnements domotiques et les systèmes de contrôle d'accès intelligents, a profondément transformé les usages numériques tout en introduisant de nouveaux enjeux de sécurité. Dans ce contexte, les mécanismes d'authentification traditionnels, notamment les mots de passe classiques et les CAPTCHA conventionnels, montrent des limites croissantes face aux progrès rapides de l'intelligence artificielle, en particulier des techniques d'apprentissage profond et des réseaux neuronaux convolutionnels.

Cette thèse s'intéresse à la conception de mécanismes d'authentification robustes capables de résister aux attaques automatisées basées sur l'intelligence artificielle, tout en restant utilisables et légers pour une intégration efficace dans des systèmes intelligents connectés. Elle propose un cadre d'authentification fondé sur des principes perceptuels, exploitant l'asymétrie intrinsèque entre la perception humaine et les capacités de reconnaissance des modèles neuronaux.

Les contributions de ce travail sont multiples. Tout d'abord, un nouveau système d'authentification par mot de passe perceptuel est conçu, visant à limiter l'efficacité des attaques automatisées tout en conservant une bonne ergonomie pour l'utilisateur humain. Ensuite, ce système est appliqué à la conception et à l'implémentation d'un dispositif de serrure intelligente sécurisée, démontrant sa pertinence dans un scénario réel de contrôle d'accès. Enfin, le cadre proposé est étendu à la construction de CAPTCHA résistants aux attaques par intelligence artificielle, spécifiquement conçus pour contrer les algorithmes de reconnaissance basés sur l'apprentissage profond.

Une évaluation expérimentale approfondie est menée afin d'analyser la robustesse des mécanismes proposés face à différents modèles d'attaques neuronales, incluant des réseaux convolutionnels et des architectures hybrides. Les résultats obtenus montrent une réduction significative des taux de succès des attaques automatisées, tout en maintenant une bonne capacité de résolution pour les utilisateurs humains.

En conclusion, cette thèse apporte une contribution à la sécurisation des systèmes intelligents connectés en proposant des mécanismes d'authentification adaptés aux menaces émergentes liées à l'intelligence artificielle, et ouvre des perspectives pour le développement de solutions de sécurité exploitant les limites actuelles des modèles neuronaux.

**Mots clés :** Cryptographie visuelle, Intelligence artificielle, Authentification perceptuelle, Systèmes intelligents connectés