

AVIS DE PRESENTATION DE THESE EN SOUTENANCE POUR L'OBTENTION DU DIPLOME NATIONAL DE DOCTEUR

Monsieur Vinh Loc CU

Présentera ses travaux intitulés :

**« Utilisation de techniques de reconnaissance des formes pour la dissimulation de données
Application à la sécurisation des documents »**

Spécialité : Informatique et applications

Le 19 juillet 2019 à 9h00

Lieu :

**La Rochelle Université
Pôle Communication, Multimédia et Réseaux
Amphithéâtre
44 Av. Albert Einstein
17000 LA ROCHELLE**

Composition du jury :

M. BURIE Jean-Christophe	Professeur, la Rochelle Université
M. GARAIN Uptal	Professeur, Indian Statistical Institute, Kolkata - India
M. OGIER Jean-Marc	Professeur, la Rochelle Université
M. PUECH William	Professeur, Université de Montpellier
M. SHAFAIT Faisal	Professeur, National University of sciences and technology Islamabad - Pakistan
Mme VINCENT Nicole	Professeure, Université Paris Descartes

Résumé :

Au cours des dernières années, la croissance rapide des technologies de l'information et de l'usage du numérique a rendu les images de documents plus omniprésentes que jamais. Dans les faits, il existe une grande variété de documents administratifs et commerciaux ayant une valeur «juridique» tels que les certificats, les diplômes, les contrats, les factures, etc. Ces documents sont utilisés par les institutions, les banques, les assurances, les établissements d'enseignement, etc. Par souci de simplicité, ces documents sont souvent échangés par des canaux numériques (la messagerie électronique, transfert de fichiers). L'interception de ces documents et leur potentielle falsification est devenue une question inévitable, en particulier avec le développement de la cybercriminalité. Par conséquent, la fiabilité de ces documents numériques peut être remise en question avec un impact important sur la confiance et entraîner des conséquences pénales, économiques et sociales en cas de fraudes avérées. Pour protéger ces documents numériques contre toute ingérence non autorisée, le domaine de la lutte contre la fraude a évolué et attiré l'attention des chercheurs de la communauté de l'analyse et de la reconnaissance de documents. Une solution efficace pour lutter contre la fraude consiste à dissimuler des données en utilisant des techniques de reconnaissance de formes.

L'objectif de ce travail est de développer des approches fiables pour dissimuler des informations et être capable de vérifier si un document est authentique ou falsifié. Les problématiques abordées dans cette thèse concernent: (1) l'extraction de caractéristiques stables dans les documents, même en présence de distorsions; et (2) la capacité à détecter avec précision les informations cachées pour sécuriser les documents notamment lorsque les documents «protégés» sont soumis à des distorsions causées par des processus tels que impression / numérisation ou impression / photocopie / numérisation. La première problématique est abordée en tirant parti des techniques conventionnelles de reconnaissance des formes et d'approches basées sur les apprentissages profonds (deep learning). Plus précisément, nous utilisons des détecteurs de la littérature pour détecter les points caractéristiques au sein des documents et proposons un nouveau détecteur de points caractéristiques pour développer une méthode de stéganographie. Afin d'améliorer la stabilité des caractéristiques face aux distorsions réelles, nous proposons plusieurs approches de tatouage (watermarking) utilisant des régions stables du document au lieu des points caractéristiques. Ces approches combinent des techniques conventionnelles et les réseaux entièrement connectés (FCN). Les réseaux antagonistes génératifs (GAN) sont également utilisés pour produire un document de référence, et générer des caractères alternatifs utilisés pendant le processus de tatouage. Nous proposons ainsi deux approches pour dissimuler et détecter des informations. La première repose sur la modification de l'intensité des pixels, l'autre sur la forme des caractères.

Les évaluations montrent que nos approches sont capables de détecter correctement les informations cachées lorsque les documents «protégés» sont soumis à diverses distorsions. Une comparaison avec les méthodes de la littérature montre que nos approches offrent des performances compétitives en termes de robustesse pour sécuriser différents types de documents.