# Demande de (co-)financement d'une bourse de thèse

**Laboratoire d'accueil :** XLIM UMR CNRS 7252

**Titre de la thèse : Image forensic : from physical models to deep learning**

**Direction de thèse :**

*Christine FERNANDEZ-MALOIGNE, (christine.fernandez@univ-poitiers.fr 05 49 49 65 73)*

**Co-direction de thèse :**

*Anne-Sophie CAPELLE-LAIZE (anne.sophie.capelle@univ-poitiers.fr 05* 49 49 69 89*)*

*Philippe CARRÉ (philippe.carre@univ-poitiers.fr 05 49 49 65 76)*

**Mots clefs : imagerie couleur, image forensics, mesure d'intégrité des images**

# CONTEXTE - PROBLEMATIQUE GENERALE

Les méthodes de mesure d'authenticité, d'intégrité, des images numériques sont actuellement en plein essor. Par exemple, elles peuvent jouer un rôle essentiel pour la justice lorsque les images sont utilisées comme preuves. Les médias et réseaux sociaux dépendent aussi en grande partie des images. Or les progrès de la recherche en traitement des images ont permis le développement de logiciels permettant au néophyte de manipuler les images sans connaissances particulières. Il est donc maintenant possible d'altérer le contenu informatif d'une image sans que ces modifications soient visibles à l'oeil nu, d'où la nécessité de les détecter numériquement grâce à des algorithmes sophistiqués. En parallèle, l'apprentissage est devenu un domaine majeur dans divers problèmes de classification en traitement du signal. L'apprentissage permet aux machines d'apprendre sans recourir explicitement à une modélisation préalable du problème traité. De tels algorithmes apprennent des traits répétitifs et/ou significatifs essentiellement à partir d'exemples, voire beaucoup d'exemples, i.e. bases d'apprentissage, et sont plus tard capables de ré-identifier ces mêmes caractéristiques sur des données encore non vues. Dans le cadre de cette thèse nous nous proposons de développer une bibliothèque d'outils innovants pour certifier l'intégrité d'une image ou d'une vidéo à l'aide de méthodologies basées sur des modèles physiques de constitution des images et de méthodologies basées sur des approches de type  apprentissage profond

# PROGRAMME DE THESE et TRAVAUX ENVISAGÉS

On peut distinguer trois types d'approches pour détecter des modifications apportées à une image : a) les techniques actives, b) les techniques semi-actives et c) les techniques passives (ou aveugles). Les techniques actives supposent que la caméra, lors de la production de l'image originale, a inséré une signature ou un filigrane invisible à l'oeil (« watermak »). Les techniques semi-actives, supposent qu'une information est a priori connue (par exemple au travers du fichier EXIF) comme le modèle de la caméra. La connaissance de cette information permet de déduire le type d'algorithmes de démosaïquage, le modèle du capteur, etc. La détection de falsifications repose alors sur la détection d'incompatibilités entre cette information a priori et l'image observée. Par opposition aux techniques actives ou semi-actives, les approches passives cherchent à exploiter les propriétés (au sens large) des images naturelles. Elles reposent sur une modélisation fine des images et des opérations qui permettent leurs modifications. Les images produites par une caméra sont issues d'une chaîne qui inclue : système optique de la caméra, capteur/échantillonnage, démosaïquage, balance des blancs, enregistrement du fichier (compressé ou non) avec son EXIF. Chacune des ces opérations, combinées avec les propriétés physiques de l'optique, du capteur et de la scène observée laissent des traces qu'il est possible de distinguer. Il est possible de distinguer des incohérences dans la trame des couleurs, les aberrations de l'optique, la position du ou des éclairages ou les reflets. Par ailleurs, un certain nombre de falsifications comme un copier coller peut nécessiter des opérations préalables. Par exemple, il est souvent nécessaire de changer la forme, les proportions, la perspective et les couleurs de l'objet source pour qu'il s'insère le mieux possible dans l'image cible. Cela implique des opérations de ré-échantillonnage et de transfert de couleurs qu'il est possible de détecter. En outre, les images naturelles obéissent à des propriétés particulières (bruit, statistiques) dont on peut détecter les éventuelles incohérences et ainsi révéler une manipulation.

En parallèle, récemment, le domaine de l'apprentissage profond basé sur les réseaux de neurones a connu un essor considérable et produit des résultats remarquables dans un peu près tous les domaines de l'intelligence artificielle. L'avantage de l'apprentissage profond par rapport aux approches classiques d'apprentissage est que les caractéristiques des images ne sont plus extraites à l'avance mais apprises directement à partir des données permettant de trouver les caractéristiques les plus adaptées à chaque problème et chaque jeu de données. Plusierss techbiques ont récemment été développées à partir de ces approches dites de « deep learning » pour la dtection de l'intégrité d'une image de 2 façons : d'une part directement sur des bases d'images intègres et falsifiées et d'autre part sur des attributs extraits de ces images.

Que ce soit par ces nouvelles approches ou par des approches basées sur la physique, des bases de données dédiées à la falsification ont été rendues publiques comme les bases Casia, la base Columbia, ou encore IEEE IFS-TC. Elles pourront être exploitées dans le cadre de cette thèse dont l'objectif sera d'abord de réaliser un état de l'art le plus complet possible des approches existantes en « image forensic », puis de développer une bibliothèque d'outils innovants pour certifier l'intégrité d'une image ou d'une vidéo à l'aide d'approches physiques comme du deep learning.

# Références bibliographiques sur le sujet

**Références du laboratoire**


- Yu FAN, Philippe CARRÉ, Christine FERNANDEZ-MALOIGNE, Image splicing detection with local illulination estimation, ICIP 2015, Québec City, Canada, 27-20 septembre 2015
- Abdul Wadood, Philippe Carré, Philippe Gaborit, Error correcting codes for robust color wavelet watermark, EURASIP Journal on Information Security, Hindawi, 2013, pp.v


**Bibliographie**


- Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, and G. Serra, A SIFT-based forensic method for copymove attack detection and transformation recovery". IEEE Trans. on Info Forensics and Security, vol. 6, no. 3 (2011), pp. 1099-1110.
- B. Bayar and M. C. Stamm, A deep learning approach to universal image manipulation detection using a new convolutional layer". ACM Workshop on Information Hiding and Multimedia Security . 2016, pp. 1-6.
- T. Bianchi and A. Piva, Image forgery localization via block-grained analysis of JPEG artifacts". IEEE Trans. on Information Forensics and Security, vol. 7, no. 3 (2012), pp. 1003-1017.
- R. Bohme and M. Kirchner, Counter-forensics: Attacking image forensics, Digital Image Forensics . Ed. by H. T. Sencar and N. Memon. Springer, 2013, pp. 327-366.
- G. Cao, Y. Zhao, R. Ni, and X. Li, Contrast enhancement-based forensics in digital images, IEEE Trans. on Information Forensics and Security , vol. 9, no. 3 (2014), pp. 515-525. 24
- I.-C. Chang, J. C. Yu, and C.-C. Chang, A forgery detection algorithm for exemplar-based inpainting images using multi-region relation, Image and Vision Computing , vol. 31, no. 1 (2013), pp. 57-71.
- G. Chierchia, G. Poggi, C. Sansone, and L. Verdoliva, A Bayesian-MRF approach for PRNU-based image forgery detection, IEEE Trans. on Information Forensics and Security, vol. 9, no. 4 (2014), pp. 554-567.
- V. Chiesa, An approach for detecting global image manipulations, MA thesis. Politecnico di Milano (Advised by S. Tubaro, F. Cayre and K. Wang), 2014.
- V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, An evaluation of popular copy-move forgery detection approaches". IEEE Trans. on Information Forensics and Security, vol. 7, no. 6 (2012), pp. 1841-1854.
- D. Cozzolino, D. Gragnaniello, and L. Verdoliva, A novel framework for image forgery localization", CoRR, vol. abs/1311.6932, (2013), pp. 1-4.
- D. Cozzolino, D. Gragnaniello, and L. Verdoliva, Image forgery detection based on the fusion of machine learning and block-matching methods". CoRR , vol. abs/1311.6934, (2013), pp. 1-4.
- D. Cozzolino, G. Poggi, and L. Verdoliva, Splicebuster: A new blind image splicing detector, IEEE International Workshop on Information Forensics and Security,2015, pp. 1-6.
- J. Dong, W. Wang, and T. Tan, CASIA image tampering detection evaluation database, IEEE ChinaSIP, 2013, W. Fan., Towards Digital Image Anti-Forensics via Image Restoration". PhD thesis. Université Grenoble Alpes (Advised by J.-M. Brossier, F. Cayre, K. Wang and Z. Xiong), 2015.

- W. Fan, K. Wang, F. Cayre, and Z. Xiong, 3-D lighting-based image forgery detection using shape-fromshading, European Signal Processing Conference,2012, pp. 1777-1781.
- W. Fan, K. Wang, F. Cayre, and Z. Xiong, A variational approach to JPEG anti-forensics, IEEE International Conference on Acoustics, Speech, and Signal Processing . 2013, pp. 3058-3062.
- W. Fan, K. Wang, F. Cayre, and Z. Xiong, JPEG anti-forensics with improved tradeo_ between forensic undetectability and image qualitt, IEEE Trans. on Information Forensics and Security, vol. 9, no. 8 (2014), pp. 1211-1226.
- W. Fan, K. Wang, and F. Cayre, General-purpose image forensics using patch likelihood under image statistical models, IEEE International Workshop on Information Forensics and Security. 2015, pp. 1-6.
- W. Fan, K. Wang, F. Cayre, and Z. Xiong, Median filtered image quality enhancement and anti-forensics via variational deconvolution, IEEE Trans. on Information Forensics and Security, vol. 10, no. 5 (2015), pp. 1076-1091.
- H. Farid, A survey of image forgery detection, IEEE Signal Proc Magazine , vol. 26, no. 2 (2009), pp. 16-25.
- S. Giraudot, Characterization of sensor noise in image acquisition systems for forensics applications". MA thesis. Grenoble INP (Advised by F. Cayre), 2011.
- Z. He, W. Lu, W. Sun, and J. Huang. Digital image splicing detection based on Markov features in DCT and DWT domain". Pattern Recognition , vol. 45, (2014), pp. 4292-4299.
- J. Li, X. Li, B. Yang, and X. Sun, Segmentation-based image copy-move forgery detection scheme, IEEE Trans. on Information Forensics and Security , vol. 10, no. 3 (2015), pp. 507-518.
- X. Pan and S. Lyu, Region duplication detection using image feature matching, IEEE Trans. on Information Forensics and Security, vol. 5, no. 4 (2010), pp. 857-867.
- T. Pevny, T. Filler, and P. Bas, Using high-dimensional image models to perform highly undetectable steganography, Information Hiding 2010 ,Calgary, Canada, 2010.
- X. Qiu, H. Li, W. Luo, and J. Huang, A universal image forensic strategy based on steganalytic model"., ACM Workshop on Information Hiding & Multimedia Security, 2014, pp. 165-170.
- Olga Russakovsky, Jia Deng, Hao Su, Jonathan Krause, Sanjeev Satheesh, Sean Ma, Zhiheng Huang, Andrej Karpathy, Aditya Khosla, Michael Bernstein, Alexander C. Berg, and Li Fei-Fei, ImageNet Large Scale Visual Recognition Challenge". International Journal of Computer Vision (IJCV), vol. 115, no. 3 (2015), pp. 211{252. doi : 10.1007/s11263-015-0816-y .
- S.-J. Ryu, M. Kirchner, M.-J. Lee, and H.-K. Lee, Rotation invariant localization of duplicated image regions based on Zernike moments, IEEE Trans. on Information Forensics and Security, vol. 8, no. 8 (2013), pp. 1355-1370.
- A. Sarkar, L. Nataraj, and B. S. Manjunath., Detection of seam carving and localization of seam insertions in digital images, ACM Workshop on Multimedia and security . 2009, pp. 107-116.
- Y.Q. Shi, C. Chen, and G. Xuan, Steganalysis versus splicing detection". In: Proc. of International Workshop on Digital Watermarking , 2008, pp. 158{172.
- M. C. Stamm, M. Wu, and K. J. R. Liu, Information forensics: An overview of the first decade, IEEE Access , vol. 1, (2013), pp. 167- 200
- A. Swaminathan, M. Wu, and K. J. Ray Liu, Digital image forensics via intrinsic _ngerprints, IEEETrans. on Information Forensics and Security , vol. 3, no. 1 (2008), pp. 101-117.
- D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, CoMoFoD - new database for copy-move forgery detection"., International Symposium ELMAR . 2013, pp. 49-54.
- B. Xu, J. Wang, G. Liu, and Y. Dai, Image copy-move forgery detection based on SURF, International Conference on Multimedia Information Networking and Security, 2010, pp. 889-892.
- H.-D. Yuan, Blind forensics of median fillteringn digital images". IEEE Trans. on Information Forensics and Security, vol. 6, no. 4 (2011), pp. 1335-1345.