Sujet de stage Master 2/Ingénieur

DETECTION DE FALSIFICATION VIDEO

Mots-clés : apprentissage, vidéos, forensic

PREAMBULE

Le laboratoire GREYC (UMR 6072) est un laboratoire basé en Normandie, composé de plus de 230 membres dont une centaine de chercheurs ou enseignants-chercheurs permanents, dans 6 équipes de recherche couvrant de nombreux domaines de l'informatique, l'automatique et l'électronique.

L'équipe de recherche en cybersécurité SAFE du GREYC, basée à Caen, mène des activités de recherche dans le domaine de la sécurité informatique autour de 3 thèmes : 1) Biométrie, 2) Architecture et modèle de sécurité et 3) Sciences de l'investigation (Forensic). L'équipe propose un sujet de stage sur la **détection de falsification vidéo**.

Ce sujet s'inscrit dans le cadre de travaux en cours dans le thème Forensic de l'équipe. Il fait suite à la réalisation d'un premier prototype fonctionnel de détection. Afin de poursuivre ces travaux prometteurs, l'équipe recherche un étudiant de niveau Master2 pour un stage de cinq mois du 1er mars au 31 juillet 2022.

CONTEXTE

Les vidéos numériques sont l'un des vecteurs multimédia les plus répandus dans notre quotidien. Elles sont largement diffusées via des sites Web ou des réseaux sociaux tels que Facebook, Instagram, WhatsApp, YouTube, etc. La disponibilité d'outils d'édition modernes et simples à utiliser facilite la modification du contenu des vidéos.

Une vidéo est considérée comme falsifiée si son contenu a fait l'objet d'une manipulation pour tromper volontairement le spectateur permettant ainsi d'influencer ses décisions et ses pensées. Les vidéos contrefaites sont visuellement très difficiles à identifier. Dès lors, vérifier l'intégrité d'une vidéo est une tâche primordiale.

La détection de falsification vidéo (video forensics) est une analyse scientifique visant à examiner une vidéo à la recherche de modifications de contenu. Ces modifications peuvent être classées soit en intra-image, soit en inter-image en fonction du domaine de modification [1]. Les modifications intra-image se produisent dans le domaine spatial ou spatio-temporel : les images sont partiellement modifiées. Les modifications inter-images se produisent dans le domaine temporel : une image entière subit un processus de falsification. Durant ce stage, nous nous concentrons sur les contrefaçons vidéo inter-images qui sont largement utilisées car ce sont des tâches sans effort et pratiquement imperceptibles.

La finalité des falsifications inter-images dans les vidéos peut être classée en trois catégories :

1. Suppression d'événement : en appliquant une suppression de trames successives
2. Ajout d'événement : en appliquant l'insertion d'images pour ajouter un clip étranger à partir d'une vidéo différente.
3. Réplication d'événement : en appliquant une duplication de trame pour répéter un événement.

Les méthodes de détection de falsification vidéo peuvent être classées en méthodes actives et passives [1], [2]. Les méthodes actives nécessitent des informations préalables sur l'examen de la vidéo telle que la présence d'une marque dans la vidéo, comme dans le cas du tatouage [3]. La plupart des vidéos n'incluent pas ces informations, ce qui rend ces méthodes inefficaces. Les méthodes passives ou aveugles ne nécessitent pas d'informations préalables pour identifier une vidéo falsifiée. Ces méthodes sont plus adaptées aux scénarios de la vie réelle car elles utilisent les traces de contrefaçon. Cependant, la plupart des approches de vidéo qui ont été proposées sont basées sur l'extraction de caractéristiques manuelles pour retracer la contrefaçon. Or ces caractéristiques sont sensibles aux opérations de post-traitement telles que le bruit, le flou, la luminosité et la compression. De plus, la plupart des méthodes existantes ne peuvent pas détecter simultanément tous les types de falsifications inter-trames. Par conséquent, elles ne sont pas en mesure d'atteindre les exigences de performances des applications du monde réel.

OBJECTIFS

Afin de pallier ces inconvénients, vous serez amené à exploiter les inter-images afin d'extraire des caractéristiques dites profondes à l'aide d'un réseau de neurones à convolution (CNN) qui pourront être combinées à des informations spatio-temporelles et/ou directement extraites du bitstream. Un classifieur sera ensuite entrainé afin de réaliser une classification de la vidéo en deux catégories : "vidéo falsifiée" ou "vidéo non falsifiée". Une attention particulière sera portée sur la mise à l'échelle des méthodes développées, c.-à-d. la capacité à détecter des modifications indépendamment de la longueur de la vidéo, et de leur positionnement dans la vidéo.

LIEU

GREYC, équipe SAFE
Bat F, ENSICAEN
6, bd Maréchal Juin, 14 032 - Caen

Condition d'exercice : Travail en présentiel

PROFIL RECHERCHE

Etudiant.e en Master 2 Recherche ou en dernière année d'école d'ingénieur spécialisé en informatique, image et/ou intelligence artificielle.

Une solide formation en machine learning est indispensable.

Des connaissances et expériences solides en traitement d'images/vidéos, apprentissage profond et programmation (Python, TensorFlow/PyTorch) sont nécessaires.

CANDIDATURE

Pour postuler, envoyer par email aux encadrants un dossier avec CV, lettre de motivation, relevés de notes des deux dernières années de formation, ainsi que toute pièce susceptible de renforcer la candidature (lettre de recommandation, etc.).

CONTACT

Christophe Charrier (christophe.charrier@unicaen.fr)
Emmanuel Giguet (emmanuel.giguet@unicaen.fr)

REFERENCES

[1] K. Sitara, B.M. Mehtre, Digital video tampering detection: An overview of passive techniques, in Digital Investigation, Volume 18, 2016, pages 8-22,

[2] Sitara K., B.M. Mehtre, Detection of inter-frame forgeries in digital videos, in Forensic Science International, Volume 289, 2018, Pages 186-206,

[3] S. Baudry, B. Chupeau and F. Lefèbvre, "A framework for video forensics based on local and temporal fingerprints," 2009 16th IEEE International Conference on Image Processing (ICIP), 2009