Projet Image Compression

Détection de falsifications dans des images

Compte-rendu 1

Louis JEAN
Ayoub GOUSSEM
Master 1 IMAGINE
Université de Montpellier

3 mars 2024

Table des matières

1 Introduction

La détection de falsifications d'images est un champ de recherche en constante évolution qui aborde les problématiques liées à l'authenticité et à l'intégrité des contenus visuels. Dans un monde où les images jouent un rôle crucial dans la communication, la sécurité et la prise de décision, la capacité à distinguer les images authentiques de celles qui ont été manipulées est devenue une nécessité impérieuse. Dans le cadre d'un projet d'études qui vise à implémenter un logiciel de détection de manipulations d'images, nous établirons un état de l'art puis discuterons des avancées prochaines du projet.

2 État de l'art

Cette partie examine les techniques établies et les avancées récentes dans la détection de falsifications d'images, dans le cadre d'un projet d'études qui vise à implémenter un logiciel de détection de manipulations d'images.

2.1 Analyse des pixels

2.1.1 Analyse de cohérence des pixels

Ces méthodes consistent à rechercher des incohérences dans le bruit des pixels ou dans les motifs de pixels, qui pourraient indiquer une manipulation.

La méthode proposée dans [1] utilise la fonction de niveau de bruit (NLF), qui décrit la variance du bruit dépendant de l'irradiance en fonction de l'irradiance, pour inférer les caractéristiques du bruit à chaque pixel à travers un modèle probabiliste. Les pixels falsifiés, provenant d'autres caméras vidéo, peuvent être ainsi différenciés.

2.1.2 Détection de clonage

La détection de clonage repose sur l'identification des zones de l'image qui semblent avoir été dupliquées ou clonées à partir d'autres zones de la même image.

L'algorithme décrit dans [2] utilise une méthode de hachage sensible à la cohérence pour établir des correspondances de caractéristiques dans une image. Les résultats expérimentaux indiquent que la méthode proposée est

efficace en temps réel ou quasi temps réel et offre de très bons résultats de détection, même dans des conditions difficiles.

2.1.3 Analyse de la consistence de la couleur

Comme expliqué dans [3], il est possible de calculer le vecteur de cohérence de couleur (CCV) pour déterminer la similarité entre les blocs d'une image. Le CCV permet d'identifier la cohérence des couleurs dans une région donnée. Les résultats des expériences montrent que cette méthode peut détecter des zones falsifiées même si l'image a été modifiée par un flou gaussien pour dissimuler la falsification.

2.2 Analyse en fréquence

Il est possible de mener des analyses en fréquence pour identifier les modifications en détectant les irrégularités dans le domaine fréquentiel de l'image.

2.2.1 Transformée de Fourier

L'usage de la FFT comme décrit dans [4] permet d'identifier les altérations potentielles en examinant comment les caractéristiques de texture et les modèles de fréquence diffèrent des parties authentiques de l'image.

2.2.2 Filtres de haute fréquence

L'article [5] décrit l'utilisation de filtres bilatéraux passe-haut (BiHPF) pour amplifier l'effet des artefacts au niveau de la fréquence, notamment sur les bords et les textures qui ne correspondent souvent pas au reste de l'image.

2.3 Analyse des métadonnées

On peut aussi analyser les métadonnées de l'image pour obtenir des informations clés.

2.3.1 Examen des données EXIF

L'article [6] propose une nouvelle méthodologie pour la détection de falsification d'images numériques en combinant l'analyse des informations du format de fichier d'image échangeable (EXIF) à des études statistiques.

2.4 Estimation de la source de lumière

En analysant les ombres et les directions de la lumière à partir d'une simple image, on peut détecter des incohérences.

La méthode de l'article [7] se concentre sur l'utilisation de patches de pixels pour estimer le vecteur de lumière provenant de sources lumineuses présentes dans la scène, et elle est capable de détecter les manipulations d'images en analysant l'angle d'élévation α obtenu à partir d'une source de lumière et de la normale de surface.

2.5 Watermarking et signature numérique

Il est possibel d'utiliser des watermarks invisibles ou des signatures numériques intégrées pour vérifier l'intégrité de l'image.

La technique décrite dans [8] sépare le premier plan de l'arrière-plan, puis applique un watermarking utilisant la transformation en ondelettes discrètes, la transformation en cosinus discrète, et la décomposition en valeurs singulières pour intégrer des watermarks distincts dans ces deux composantes. La détection de la falsification est réalisée en observant les différences dans les valeurs singulières obtenues.

2.6 Réseaux de neurones convolutifs (CNN)

Les CNN sont largement utilisés pour la classification d'images, la reconnaissance de motifs et la détection de falsifications. Ils peuvent être entraînés pour identifier les caractéristiques des images qui indiquent une manipulation, voir [9].

2.7 Réseaux antagonistes génératifs (GAN)

Les GAN peuvent être utilisés pour détecter les falsifications en entraînant deux réseaux simultanément : un générateur qui crée des images falsifiées et un discriminateur qui apprend à distinguer entre les images réelles et les images générées par le générateur.

3 Bases de données

Afin de tester notre programme, nous pourrons nous appuyer sur une multitude de jeu de données très adaptés voir spécialement conçus pour la détection de falsifications des images, que nous avons découvert graĉe à ce git qui les répertorie : https://github.com/greatzh/Image-Forgery-Datasets-List. En voici une liste non-exhaustive :

- **CASIA v1.0 :** contient des images authentiques et des images manipulées avec différentes techniques (splicing, copy move, removal). Voir aussi **CASIA v2.0**.
- **CoMoFoD :** spécialement conçu pour la détection de la falsification par copy-move.
- **Wild Web :** ensemble de données composé d'images récoltées sur Internet, conçu pour la détection de manipulations dans des conditions plus réalistes et variées.

4 Prévisions pour la semaine à venir

À l'heure actuelle, nous pensons implémenter l'intégralité du logiciel en Python, avec éventuellement des bindings C/C++ pour les opérations lourdes. Nous pensons que des librairies plus accessibles seront utiles en Python si nous nous aventurons vers l'apprentissage profond (PyTorch). Nous nous demandons si nous devons nous-même écrire les fonctions permettant de lire tous les formats d'images ou si nous pouvons utiliser la bibliothèque Pillow pour cela. Nous demanderons à notre enseignant mardi. D'ici à la semaine prochaine, le but est de pouvoir lire tous les formats d'images, d'avoir définitivement choisi la première méthode de détection des falsifications à mettre en œuvre et d'avoir commencé à l'implémenter. Nous avons déjà choisi le nom de notre programme : **Pixel Patrol**.

Merci pour le temps et l'attention que vous avez consacrés à la lecture de ce compte-rendu.

Références

[1] Michihiro Kobayashi, Takahiro Okabe, and Yoichi Sato. Detecting forgery from static-scene video based on inconsistency in noise level functions.

IEEE Transactions on Information Forensics and Security, 5(4):883–892, Dec 2010.

[2] Xiuli Bi and Chi-Man Pun. Fast copy-move forgery detection using local bidirectional coherency error refinement. *Pattern Recognition*, 81:161–175, 2018.

[3] Guzin Ulutas and Mustafa Ulutas. Image forgery detection using color coherence vector. In *2013 International Conference on Electronics, Computer and Computation (ICECCO)*, pages 107–110, Nov 2013.

[4] Navdeep Kanwal, Akshay Girdhar, Lakhwinder Kaur, and Jaskaran Singh Bhullar. Detection of digital image forgery using fast fourier transform and local features. In *2019 International Conference on Automation, Computational and Technology Management (ICACTM)*, pages 262–267, April 2019.

[5] Yonghyun Jeong, Doyeon Kim, Seungjai Min, Seongho Joe, Youngjune Gwon, and Jongwon Choi. Bihpf: Bilateral high-pass filters for robust deepfake detection. In *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (WACV)*, pages 48–57, January 2022.

[6] J. Harish Kumar and T. Kirthiga Devi. Fingerprinting of image files based on metadata and statistical analysis. In Gunasekaran Manogaran, A. Shanthini, and G. Vadivu, editors, *Proceedings of International Conference on Deep Learning, Computing and Intelligence*, pages 105–118, Singapore, 2022. Springer Nature Singapore.

[7] Sangeet Srivastava Manoj Kumar and Nafees Uddin. Forgery detection using multiple light sources for synthetic images. *Australian Journal of Forensic Sciences*, 51(3):243–250, 2019.

[8] Wu-Chih Hu, Wei-Hao Chen, Deng-Yuan Huang, and Ching-Yu Yang. Effective image forgery detection of tampered foreground or background image based on image watermarking and alpha mattes. *Multimedia Tools and Applications*, 75, 01 2015.

[9] Khalid M. Hosny, Akram M. Mortda, Mostafa M. Fouda, and Nabil A. Lashin. An efficient cnn model to detect copy-move image forgery. *IEEE Access*, 10:48622–48632, 2022.