

Forgery_Breaker

Marin Yann, Lanson Guillaume

Compte-rendu 1



UNIVERSITÉ
DE MONTPELLIER



L'objectif de ce compte-rendu est de présenter le sujet et de faire un état de l'art sur la détection de falsifications dans les images.

Nous nous intéresserons particulièrement aux falsifications opérées par copier-déplacer et copier coller dans une image.

État de l'art :

Pour cette partie nous nous basons principalement sur l'excellent article [1] qui propose même une étude sur la popularité des différentes techniques utilisées.

Nous nous concentrerons sur les falsifications dites « **dépendantes** » : copier-coller une région de l'image dans une autre région de l'image voire sur une autre image.

On peut organiser la détection de falsification d'image en deux approches différentes : **active** et **passive**.

L'approche **active** demande plus d'information comme des éventuels tatouages ou signatures sur l'image. Elle ne s'applique donc pas au cas d'image « inconnue » comme des images trouvées sur le web.

L'approche **passive** ne demande pas d'information supplémentaire sur l'image, au lieu de cela elle se base sur l'extraction d'information intrinsèque. C'est cette deuxième approche que l'on va utiliser.

I) Falsification copy-move :

Cette méthode de falsification consiste à dupliquer un élément déjà existant dans l'image et placer la copie à un autre endroit.

Pour détecter une falsification « Copy-move » la routine générale consiste en 4 phases :

- Pre-processing (optionnelle) (ex : conversion ndg ou YCbCr)
- Extraction d'éléments.
- Correspondance.
- Visualisation (optionnelle).

L'étape la plus intéressante pour nous est l'extraction d'éléments.

Pour cela, deux choix s'offrent à nous : diviser l'image par blocs et comparer les blocs par rapport à la présence d'élément important ou manipuler directement les points importants.

1) Techniques basées sur la décomposition par blocs :

Pour ces techniques, on découpe l'image en blocs de taille fixe, qui peuvent se superposer ou non. Des valeurs dépendant de la méthode utilisée sont extraites de ces blocs et comparées pour détecter des similarités. Les méthodes d'extraction les plus courantes sont les suivantes :

- a) Transformée fréquentielle, notamment par DCT (Direct Cosine Transform)
- b) Texture et intensité
Basé sur les changements de texture dans une image pour reconnaître les falsifications. Peut être perçu comme une mesure des variations de surface de l'image.
- c) Invariant de mouvement
Des points clés invariant aux transformations géométrique usuelles (ie : translation, rotation...)
Utile pour la reconnaissance de forme.
- d) Transformation $(x,y) \rightarrow (x,h)$ log-polar
- e) Réduction dimensionnelle

2) Techniques basées sur les points-clé :

Le but ici est de trouver des points-clés, par exemple par l'un des algorithmes suivants :

- SIFT (Scale Invariant Feature Transform)
 - Détecter dans une image des zones circulaires intéressantes centrées autour d'un point-clé
- SURF (Speeded up Robust Features)
 - Amélioration de SIFT utilisant les ondelettes de Haar
- Points de Harris

et de détecter des correspondances entre deux (ou plus) ensembles de points grâce à des méthodes comme le nearest-neighbour ou le clustering.

III) Falsification splicing :

Le splicing consiste à copier un élément d'une image pour l'insérer dans une autre image et ainsi obtenir une image falsifiée.

Ce type de falsification est principalement détectée en utilisant des réseaux de neurones convolutifs.

II) Bases de données utilisées :

Copy-Move :

www.micc.unifi.it/downloads/MICC-F220.zip

<https://www5.cs.fau.de/research/data/image-manipulation/>

Splicing :

<https://www.ee.columbia.edu/ln/dvmm/downloads/AuthSplicedDataSet/AuthSplicedDataSet.htm>

Références :

- [1] :[Copy-move forgery detection: Survey, challenges and future directions \[Nor Bakiah Abd Warif, Ainuddin Wahid Abdul Wahab, Mohd Yamani Idna Idris, Roziana Ramli, Rosli Salleh, Shahaboddin Shamshirband, Kim-Kwang Raymond Choo\]](#)
- [2] :[State of the art of copy-move forgery detection techniques: a review \[Salam Abdulnabi Thajeel, Ghazali Sulong\]](#)
- [3] :[Digital Image Forgery Detection Based on Lens and Sensor Aberration \[Ido Yerushalmy, Hagit Hel-Or\]](#)
- [4] :[Copy-move forgery detection via texture description \[Edoardo Ardizzone, Alessandro Bruno, Giuseppe Mazzola\]](#)
- [5] :[Copy Move Forgery using Hus Invariant Moments and Log Polar Transformations \[Tejas Krishna Reddy, Swathi Chintala, Rajesh Muthu\]](#)
- [6] :[A robust detection algorithm for copy-move forgery in digital images \[Yanjun Cao, Tiegang Gao, Li Fan, Qunting Yang\]](#)
- [7] :[Image splicing detection based on convolutional neural network with weight combination strategy \[Jinwei Wang, Qiye Ni, Guangjie Liu, Xiangyang Luo, Sunil Kr. Jha\]](#)
- [8] :[A deep learning approach to detection of splicing and copy-move forgeries in images \[Yuan Rao, Jiangqun Ni\]](#)