Projet : OEIL statistiques rObustEs pour l'apprentIssage Léger Challenge DEFALS

anr agence nationale de la recherche

Appel : Challenge DEtection de FALSifications dans des images et vidéos
Année : 2022

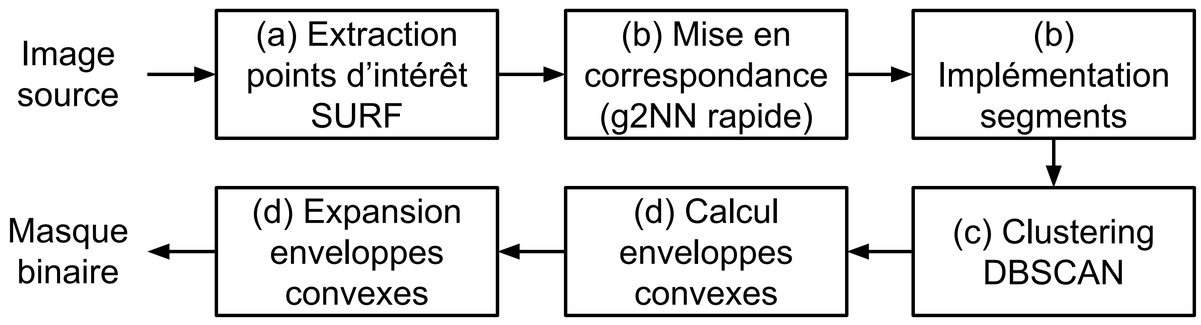
Instrument : Challenges

Contact : laura.bertojo@lirmm.fr, william.puech@lirmm.fr

COORDINATEUR : William Puech — **PARTENAIRE : Université de Montpellier**

La méthode proposée est un détecteur de falsifications de type copié-déplacé basé sur l'utilisation des points d'intérêt. Celle-ci introduit un nouvel algorithme efficace d'appariement afin de pouvoir analyser rapidement de grandes images telles que des images 4K tout en détectant avec précision les différentes zones de falsifications.

METHODE



(a) Extraction des points d'intérêt SURF

A partir de l'image source, on extrait :
- *n* points d'intérêts $P = \{p_1, ..., p_n\}$ classés selon leur orientation,
- *n* orientations $\Theta = \{\theta_1, ..., \theta_n\}$,
- *n* vecteurs caractéristiques $F = \{f_1, ..., f_n\}$.

(b) Mise en correspondance rapide

Appariement des points d'intérêt dans les méthodes classiques : **complexité quadratique** ($O(n^2)$).

Idée : Effectuer le test g2NN [10] seulement entre les points d'intérêt ayant une orientation similaire. On définit ainsi une **fenêtre d'angle** à l'aide d'un seuil τ_θ.

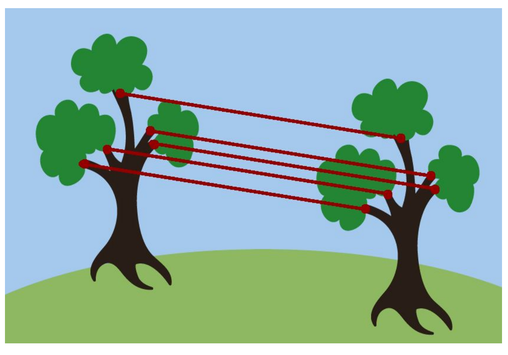
$$P = \{p_1, \ldots, p_{l-1}, \underbrace{p_l, \ldots, p_i, \ldots, p_m}_{\{p_l,\ldots p_m\}\in\{p_k\in P/|\theta_i-\theta_k|\leq\tau_\theta\}}, p_{m+1}, \ldots, p_n\} \quad (1)$$

Un segment est implémenté pour chaque mise en correspondance, où les bornes sont les points appariés. Un segment est défini par son **point de départ** et son **point d'arrivée**.

(c) DBSCAN

Nous nous plaçons dans l'hypothèse de copié-déplacé ayant subi une **translation simple** ou une **faible rotation et/ou mise à l'échelle**.

Les segments liés à une même falsification:
- sont quasiment **parallèles**,
- sont quasiment de **même longueurs**,
- ont approximativement les **mêmes zones de départ et d'arrivée**.



L'algorithme *DBSCAN* regroupe les segments liés à une même falsification dans un cluster grâce à une pseudo-distance adaptée. Les segments isolés (non liés à une falsification) sont éliminés.

(d) Calcul enveloppe convexe et expansion

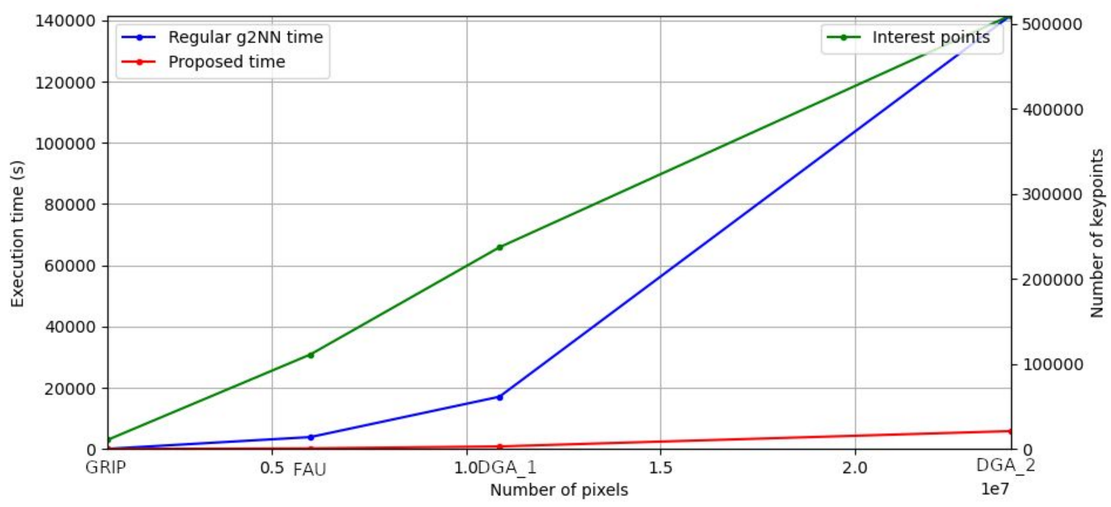
Pour chaque cluster, les **enveloppes convexes** des points de départ et des points d'arrivée sont calculées puis **étendues** afin de générer le masque binaire final.

RESULTATS : Comparaison avec l'état de l'art

GRIP [2]		FAU [11]	
Méthodes	F1-score (Pixel)	Méthodes	F1-score (Pixel)
Cozzolino *et al.* [2]	0.9299	Huang *et al.* [3]	0.6354
Li *et al.* [4]	0.2774	Shivakumar and Baboo [7]	0.6954
Bravo *et al.* [1]	0.8482	Zandi *et al.* [9]	0.8607
Silva *et al.* [8]	0.6662	Li *et al.* [4]	0.7447
Zandi *et al.* [9]	0.6444	Pun *et al.* [6]	0.8997
Li *et al.* [5]	0.9466	Li and Zhou [5]	0.8838
Méthode proposée	0.9606	Méthode proposée	0.8963

RESULTATS : Analyse du temps de calcul

(temps en seconde)	Total	Pt. Int.	Appariement	Segments	Cluster	Env. Conv	Masque	Extension Mas.
g2NN	3880.18	1.625	3871.229	0	4.917	0	0	1.271
g2NN rapide	187.70	2.208	177.5	0	5.041	0	0	1.7916



CONCLUSION

Méthode :
- **Rapide** : Analyse rapide des images de grande taille telles que les images 4K
- **Performante** : Résultats comparables à ceux de l'état de l'art
- **Robuste** : Résultats peu dégradés lors d'une attaque par compression JPEG ou par ajout de bruit

Axes de recherche :
- Rendre la méthode robuste contre les **attaques géométriques** (rotation, mise à l'échelle ...)

RESULTATS : Détection d'une zone copiée-déplacée

REFERENCES

[1] S. Bravo-Solorio and A. K. Nandi, "Passive Forensic for detecting duplicated regions affected by reflexion, rotation and scaling", *2009 17th EUSIPCO*, 2009.
[2] D. Cozzolino, G. Poggi, and L. Verdoliva, "Efficient dense-field copy-move forgery detection", *IEEE Transactions on Information Forensics and Security*, 2015.
[3] H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using sift algorithm", 2008 *IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, 2008.
[4] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy-move forgery detection scheme", *IEEE Transactions on Information Forensics and Security*, 2015.
[5] Y. Li, and J. Zhou, "Fast and effective image copy-move forgery detection via hierarchical feature point matching", *IEEE Transactions on Information Forensics and Security*, 2019
[6] C.-M. Pun, X.-C. Yuan, and X.-L. Bi , "Image forgery detection using adaptive oversegmentation and feature point matching", IEEE Transactions on Information Forensics and Security, 2015.
[7] B. L. Shivakumar, and S. Santhosh Baboo, "Detection of region duplication forgery in digital images using surf", *International Journal of Computer Science Issues*, 2011.
[8] E. Silva, T. Carvalho, A. Ferreira, and A. Rocha, "Going deeper into copy-move forgery detection: exploring image telltales via multi-scale analysis and voting processes", *Journal of Visual Communication and Image Representation*, 2015.
[9] M. Zandi, A. Mahmoudi-Aznaveh, and A. Talebpour, "Iterative copy-move forgery detection based on a new interest point detector", *IEEE Transactions on Information Forensics and Security*, 2016.
[10] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-Based Forensic Method For Copy-Move Attack Detection and Transformation Recovery", *IEEE Transactions on Information Forensics and Security,* 2011
[11] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches", *IEEE Transactions on information forensics and security,* 2012