Détection du copier-coller par mise en correspondance de descripteurs SIFT et filtrage à l'aide de cartes de dissimilarité locale

Gaël MAHFOUDI[1], Frédéric MORAIN-NICOLIER[2], Florent RETRAINT[1]

[1]ICD, M2S, Université de technologie de Troyes
12 Rue Marie Curie, 10300 Troyes, France

[2]CReSTIC, Université de Reims-Champagne-Ardenne, France
IUT de Troyes, 9 rue de Québec, CS 90396, 10026 Troyes CEDEX, France

gael.mahfoudi@utt.fr, frederic.nicolier@univ-reims.fr
florent.retraint@utt.fr

Résumé – Il est de plus en plus difficile de croire en l'authenticité des images numériques. Ceci est dû à la simplicité croissante de falsifier ces images à l'aide d'outils toujours plus puissants. Sur un logiciel tel que Photoshop, il est possible de supprimer un élément d'une image en quelques clics. Le copier-coller est une méthode de falsification élémentaire consistant en la duplication d'une portion de l'image. Dans ce papier nous proposons une nouvelle méthode de détection du copier-coller permettant de maintenir un taux de faux positifs bas.

Abstract – It is becoming harder and harder to believe in digital images authenticity. This is due to the increasing ease of producing forged images using retouching software more powerful than ever. On software like Photoshop, one can easily remove an element from an image with just a few clicks. Copy-move is one of the elemental forgery methods that consists in the duplication of one portion of the image. In this paper, we propose a novel method for the detection of Copy and Move forgery while maintaining a low false positive rate.

1 Introduction

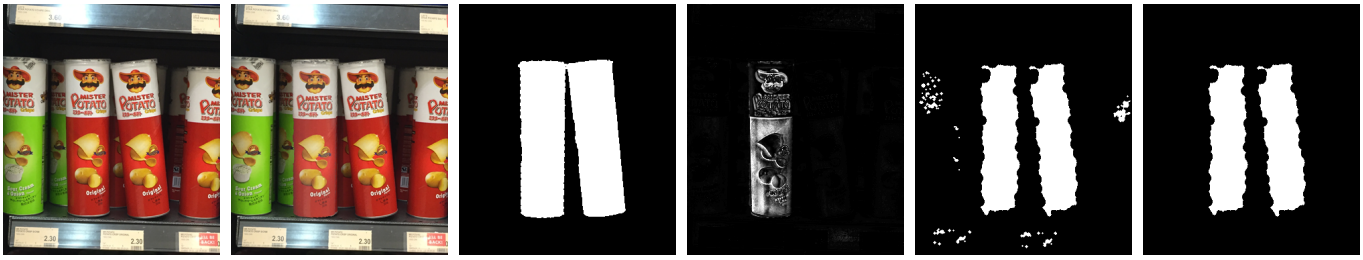
La production d'images falsifiées devient plus simple et plus accessible au grand public au travers d'outils tels que Photoshop. Une méthode très commune de falsification des images numériques est couramment appelée le copier-coller. Cette falsification élémentaire consiste en la duplication d'une portion de l'image. L'élément dupliqué n'est pas contraint en taille et peut subir une déformation affine avant d'être à nouveau collé dans l'image. Il est intéressant de pouvoir détecter un tel type de falsification puisque cette opération basique est couramment utilisée dans les photomontages. Cette méthode peut servir à la simple duplication d'un élément pour tromper sur une quantité. Une affiche de propagande pourrait ainsi tromper l'opinion publique sur les forces armées d'un état. Ou encore pour la suppression d'un élément sur une image en le cachant derrière un ou plusieurs éléments dupliqués. La détection du copier-coller est un sujet déjà bien étudié. Dans cet article nous effectuons la détection à l'aide des points clés SIFT et proposons l'utilisation d'une carte de dissimilarité locale [1] pour permettre une détection plus précise.

2 État de l'art

De nombreuses recherches ont été menées sur la détection du copier-coller. Les algorithmes de détections peuvent être séparés en trois grandes familles [2]. La détection par blocs, par points clés et les détections hybrides.

Les détections par blocs [3, 4] découpent l'image en blocs réguliers ou non puis procèdent à la mise en correspondances de ces blocs. Les détections par points clés [5, 6] se composent de deux étapes. Dans un premier temps, un ensemble de points clés est extrait de l'image. Puis ces points clés sont mis en correspondance. La détection du copier-coller s'effectue ensuite à l'aide un partitionnement des points précédemment mis en correspondance. L'objectif du partitionnement est de rejeter les éventuelles erreurs de correspondances en mettant en évidence des groupes de points ayant une structure commune typique d'un copier-coller. Enfin les détections hybrides tirent profit des deux méthodes précédentes [7].

En présence d'images dont le contenu présente des structures fortement similaires, le taux de faux positifs augmente généralement pour toutes ces méthodes. Les auteurs de [8] ont proposés la base de données COVERAGE pour l'étude des algorithmes de détection en présence d'objets fortement similaires. Deux exemples d'images de la base sont illustrés en figure 1a et 1b. Le masque binaire de la falsification (Fig. 1c) nous indique que la boite de chips la plus à droite est dupliquée sur celle de gauche pour la recouvrir. Dans [6] plusieurs algorithmes de l'état de l'art ont été évalués sur la base COVERAGE et ont obtenus de forts taux de faux positifs [6, Table II]. Dans cet article nous évaluons l'utilisation de la carte des dissimilarités locales [1] comme moyen de diminuer le taux de fausses alarmes des méthodes de détection par points clés.



(a) Image originale (b) Image falsifiée (c) Masque binaire de la falsification (d) CDL^{XYZ} entre (a) et (b) (e) Détection sans CDL^{XYZ} (f) Détection avec CDL^{XYZ}

FIGURE 1 – Exemple de CDL^{XYZ} et de détection

3 Détection SIFT

3.1 Extraction des points clés

L'extraction des points clés est effectuée à l'aide du détecteur de la méthode SIFT [9]. Plutôt que d'effectuer une détection globale des points clés sur l'image, la détection est faite au travers d'une fenêtre glissante non superposée. Les méthodes de détection du copier-coller basées sur les points clés nécessitent que les régions dupliquées soient couvertes par un nombre suffisant de points clés. Pour pallier ce problème, le seuil de rejet sur le contraste est ajusté pour extraire une quantité de points clés SIFT suffisante pour chaque portion de l'image. Ceci permet de conserver les points clés sur les contours et dans les zones de gradient faible.

3.2 Mise en correspondance

La mise en correspondance classique de descripteur SIFT décrit dans [9] est la méthode $2NN$. Pour un descripteur donné, les deux voisins les plus proches avec des distances d_1 et d_2 sont trouvés. On considère qu'une mise en correspondance est positive si le rapport $\frac{d_1}{d_2}$ est inférieur à un seuil δ. Le seuil recommandé par [9] est $0,6$. Une seule mise en correspondance est considérée par le test $2NN$. Dans le cadre de la détection du copier-coller, l'hypothèse qu'un élément ne sera dupliqué que de manière unique n'est pas raisonnable. Pour cette raison les auteurs de [5] proposent $g2NN$, une généralisation de $2NN$. Le test $2NN$ est itéré pour les k plus proches voisins d'un point clé donné. On teste alors les rapports $\frac{d_i}{d_{i+1}}$ tant que ceux-ci sont inférieurs à un seuil δ fixé. Nous avons utilisé ce test généralisé qui permet une détection du copier-coller multiple.

3.3 Partitionnement

À l'étape de mise en correspondance, le seuil δ choisi ne peut être trop strict si l'on veut pouvoir détecter un copier-coller ayant subi un quelconque post-traitement (réechantillonage, ajustement des couleurs ou du contraste ...). Ce qui entraîne l'obtention de faux positifs à ce stade. Un deuxième filtrage est nécessaire pour supprimer un maximum de fausses alarmes. Nous effectuons un partitionnement à l'aide de la méthode décrite dans [10] qui permet de grouper des éléments selon des règles d'équivalences. Soit un objet O de l'image, et O_D sa copie (figure 2). Soit A et C des points clés dans l'objet O et les points clés B et D dans O_D. Soit la mise en correspondance M_{AB} entre A et B formant le vecteur $\overrightarrow{AB}$ et la mise en correspondance M_{CD} entre C et D formant le vecteur $\overrightarrow{CD}$. Les mises en correspondance M_{AB} et M_{CD} sont considérées équivalentes et sont groupées si :

$$\|\overrightarrow{AB} - \overrightarrow{CD}\| < \delta_1 \quad (1)$$

$$\|AC\| < \delta_2 \text{ et } \|BD\| < \delta_2, \quad (2)$$

$$\text{et } \|AB\| > \delta_3 \text{ et } \|CD\| > \delta_3. \quad (3)$$

Sur la figure 2 l'objet O est dupliqué en O_D avec une légère rotation. Dans le cas d'une duplication avec une déformation simple (rotation, échelle), toutes les mises en correspondance ont une orientation et une norme similaire.

Le seuil δ_1 permet de limiter l'écart entre deux vecteurs formés par deux paires de points mis en correspondance. Ceci permet de grouper les mises en correspondance d'orientation proches. Un seuil δ_1 faible tendra à augmenter le nombre de partitions. Un objet dupliqué subissant une rotation sera décomposé en plusieurs partitions de plus petite taille. Un seuil δ_1 important tendra à diminuer le nombre de partitions. Des faux positifs risquent alors d'être inclus dans les partitions des objets dupliqués. Ce seuil ne dépend pas de la taille de l'image analysée. Dans toutes nos expérimentations, δ_1 est fixé à 10.

La distance entre A et C est limitée par la taille de l'objet O dupliqué. Le seuil δ_2 fixe la taille maximale de l'objet dupliqué que l'on pourra détecter. Un seuil δ_2 trop grand tendra à ajouter des faux positifs dans les partitions des objets dupliqués. Celui-ci ne peut être trop faible non plus en raison de la densité parfois plus faible de point SIFT extrait.

A et B sont nécessairement à une distance supérieure à un seuil donné , de même pour C et D, si l'on veut dupliquer O intégralement. Le seuil δ_3 fixe la distance minimale entre l'objet O et sa copie O_D que l'on souhaite détecter. La valeur de δ_3 sera principalement choisi en fonction de la taille de l'image analysée. Dans nos expérimentations, les valeurs de δ_2 et δ_3 sont fixées à 50.

Les choix des valeurs δ_1, δ_2 et δ_3 n'est pas critique si le seuil sur le contraste en 3.1 est choisit arbitrairement bas.

À l'issue du partitionnement, les partitions comportant trop peu éléments (moins de trois paires de points mises en correspondance) sont écartées.

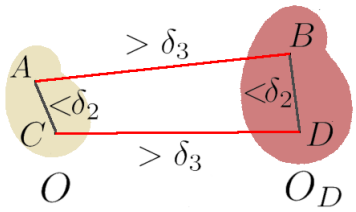


FIGURE 2 – Duplication de l'objet O et relation entre les points mis en correspondance

4 Filtrage avec la carte de dissimilarité locale

Le descripteur SIFT est l'histogramme des gradients orientés autour du point clé. Ce descripteur ne contient pas suffisamment d'information sur la structure locale autour du point clé. Dans le cadre de la détection du copier-coller, de nombreux faux positifs peuvent être produits dans le cas d'une image avec des structures répétitives (façade d'un bâtiment, textes ...). L'utilisation des informations de couleurs et de structures permettrait de rejeter de faux positifs évidents. Nous proposons d'utiliser la carte de dissimilarité locale (CDL) afin de filtrer ces faux positifs.

4.1 Rappel sur la CDL

La carte de dissimilarité locale [1] permet de mesurer les écarts locaux entre deux images binaires. Pour ce faire, une version modifiée de la distance de Hausdorff est proposée. Pour deux images binaires A et B, la CDL est définie de $\mathbb{R}^2 \times \mathbb{R}^2$ dans $\mathbb{R}^2$ par

$$\mathrm{CDL}_{\mathrm{bin}}(A,B)(p) = \mid A(p) - B(p) \mid \max(d_A(p), d_B(p)) \quad (4)$$

avec $p = (x, y)$ et $d_X(p)$ la transformée en distance de X au point p.

Une extension de la CDL aux images en niveau de gris est utilisée [11]. Les images sont dans un premier temps découpées en un ensemble d'images binaires. La CDL en niveau de gris est alors l'accumulation des CDL entre chacune de ces images binaires. Soient A et B deux images en niveau de gris, CDL_N est alors définie de $\mathbb{R}^2 \times \mathbb{R}^2$ dans $\mathbb{R}^2$ par

$$\mathrm{CDL}(A,B)(p) = \frac{1}{N} \sum_{i=1}^{N} \mathrm{CDL}_{\mathrm{bin}}(\mathrm{A_i}, \mathrm{B_i})(\mathrm{p}) \quad (5)$$

où N est le nombre de coupes, A_i (resp. B_i) est une version binaire de A (resp. B_i), obtenue par seuillage global $A > s_i$. Les seuils s_i sont régulièrement espacés entre 0 et le maximum m de chaque image. Par exemple, pour $A : s_i = \frac{i}{N} m_A, i \in [1..N]$.

4.2 CDL pour des images avec C canaux

Pour le copier-coller, nous proposons une extension directe de la CDL pour des images avec C canaux. Dans notre cas les images sont converties dans l'espace colorimétrique CIE XYZ, qui propose une répartition des couleurs se rapprochant de celle du système visuel humain. Soit A^k le canal $k \in (\mathrm{X}, \mathrm{Y}, \mathrm{Z})$ de l'image A, la CDL est définie comme :

$$\mathrm{CDL}^{\mathrm{XYZ}}(A,B)(p) = \frac{1}{3} \sum_{k} \mathrm{CDL}_N(A^k, B^k)(p). \quad (6)$$

4.3 Filtrage des dernières partitions avec les CDL

À l'issue du partitionnement décrit en 3.3, la plupart des fausses mises en correspondance obtenue en 3.2 sont éliminées. Dans la figure 1e on peut voir le résultat de la détection avant filtrage à l'aide des CDL. Des éléments semblables sont à tort considérés comme étant du copier-coller. Pour supprimer ces derniers faux positifs, les partitions restantes vont être validées à l'aide des CDL. Pour chaque paire de points clés mis en correspondances de la partition, deux fenêtres, F_1 et F_2, sont extraites pour chacun des points clés. Les fenêtres sont centrées sur les points clés et leurs tailles sont fixées par l'échelle des points clés associés. Le contenu des deux fenêtres est aligné en fonction de l'angle des points clés associés. Finalement, la paire de points est supprimée de la partition si

$$\|\mathrm{CDL}^{\mathrm{XYZ}}(F_1, F_2)\|_2 > \delta_{\mathrm{CDL}}. \quad (7)$$

Comme pour 3.3, la partition est finalement supprimée si elle contient moins de trois paires de points clés. On peut voir le résultat de la détection après filtrage dans la figure 1f.

5 Application numérique

Des expérimentations ont été menées sur les bases FAU [12] et GRIP [4] ainsi que sur la base COVERAGE [8]. Pour les bases FAU et GRIP le seuil δ_{CDL} est fixé à 7 et les seuils δ_1, δ_2 et δ_3 sont fixées pour chacune des bases pour maximiser le taux de vrais positifs. Pour la base COVERAGE, les seuils δ_1, δ_2 et δ_3 sont fixes et δ_{CDL} varie.

L'algorithme de détection est appliqué sur chaque image de la base. On évalue le taux de faux positifs et de vrais positifs au niveau image sans le filtrage avec la CDL^{XYZ} puis avec. Sur la figure 3 sont reportés les taux de faux positifs, de vrais positifs et le score F_1 lorsque le seuil de rejet δ_{CDL} évolue.

Sans filtrage à l'aide des CDL^{XYZ} on obtient un taux de vrais positifs de 100%, un taux de faux positifs de 93% et un score F_1 de 69%. Ces performances initiales sont reportées dans la figure 3 par les trois lignes horizontales en pointillés. Bien que le taux de vrais positifs soit maximum, on constate que le détecteur se comporte très mal face aux images de COVERAGE présentant des objets très similaires.

L'apport de la $\mathrm{CDL}^{\mathrm{XYZ}}$ est évalué en faisant varier progressivement le seuil de rejet δ_{CDL}. Pour un seuil de rejet très strict fixé à 2, la $\mathrm{CDL}^{\mathrm{XYZ}}$ permet d'obtenir un taux de faux positifs nul. Ceci au prix d'une performance en détection bien moindre, 30% de vrais positifs et un score F_1 de 45%. Avec le seuil δ_{CDL} qui augmente à 7, le taux de vrais positifs augmente de 30% à 70% tout en maintenant le taux de faux positif

TABLE 1 – Taux de vrais positifs, faux positifs et F_1 sur les bases FAU [12] et GRIP [4]

Méthode	FAU [12]			GRIP [4]		
	TPR	FPR	F_1	TPR	FPR	F_1
Amerini [5]	66.67	10.42	75.29	70	20	73.68
Cozzolino [4]	97.92	8.33	94.95	98.75	8.75	95.18
J. Li [3]	72.92	22.92	74.47	83.75	35	76.57
Y. Li [6]	100	2.08	98.97	100	0	100
Proposée	100	0	100	100	0	100

à 7% pour un score F_1 maximum de 78%. Par la suite, le taux de vrais positifs, de faux positifs et le score F_1 tendent progressivement vers les performances sans filtrage. L'impact au niveau du temps de traitement dépend grandement du nombre restant de partitions à valider à l'issue de 3.3 ainsi que de la taille des fenêtres à comparer. Pour les images de la base COVERAGE, le temps de traitement global sans le filtrage par la CDL est d'environ 400 secondes. Avec la CDL le temps de traitement est de 815 secondes soit environ 1 seconde de traitement supplémentaire pour la CDL.

6 Conclusion

Dans cet article, nous proposons une nouvelle méthode de détection du copier-coller. La détection est effectuée à l'aide des descripteurs SIFT. Le résultat de la détection est ensuite filtré à l'aide de la CDL^{XYZ} afin d'éliminer un maximum de faux positifs. Nous montrons que la CDL^{XYZ} permet de diminuer le taux de faux positifs pour un taux de vrais positifs équivalent à plusieurs méthodes de l'état de l'art.

Ces travaux sont soutenu par le projet ANR DEFACTO ANR-16-DEFA-0002 et par la direction générale de l'armement.

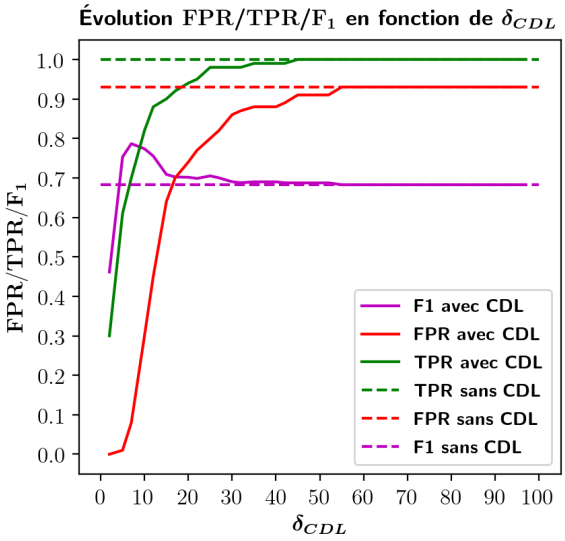


FIGURE 3 – Évolution du taux de faux positifs (FPR), vrai positifs (TPR) et du score F_1 en fonction de δ_{CDL}

Références

[1] Étienne Baudrier, Frédéric Nicolier, Gilles Millon, and Su Ruan. Binary-image comparison with local-dissimilarity quantification. *Pattern Recognition*, 41(5) :1461 – 1478, 2008.

[2] Lilei Zheng, Ying Zhang, and Vrizlynn L.L. Thing. A survey on image tampering and its detection in real-world photos. *Journal of Visual Communication and Image Representation*, 58 :380 – 399, 2019.

[3] J. Li, X. Li, B. Yang, and X. Sun. Segmentation-based image copy-move forgery detection scheme. *IEEE Transactions on Information Forensics and Security*, 10(3) :507–518, March 2015.

[4] D. Cozzolino, G. Poggi, and L. Verdoliva. Efficient dense-field copy–move forgery detection. *IEEE Transactions on Information Forensics and Security*, 10(11) :2284–2297, Nov 2015.

[5] 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*, 6(3) :1099–1110, Sep. 2011.

[6] 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*, 14(5) :1307–1322, May 2019.

[7] XiuLi Bi, Chi-Man Pun, and Xiao-Chen Yuan. Multi-scale feature extraction and adaptive matching for copy-move forgery detection. *Multimedia Tools and Applications*, 77(1) :363–385, Jan 2018.

[8] B. Wen, Y. Zhu, R. Subramanian, T. Ng, X. Shen, and S. Winkler. Coverage — a novel database for copy-move forgery detection. In *2016 IEEE International Conference on Image Processing (ICIP)*, pages 161–165, Sep. 2016.

[9] David G. Lowe. Distinctive image features from scale-invariant keypoints. *International Journal of Computer Vision*, 60(2) :91–110, Nov 2004.

[10] Bernard A. Galler and Michael J. Fisher. An improved equivalence algorithm. *Commun. ACM*, 7(5) :301–303, May 1964.

[11] Youssef Ech-Choudany, Frédéric Morain-Nicolier, Jérôme Landré, Benaïssa Bellach, Mustapha Assarar, and Daniel Scida. Méthodes de reconnaissance de formes basées sur la carte de dissimilarité locale pour la classification des images. *GRETSI*, 2017.

[12] 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*, 7(6) :1841–1854, Dec 2012.