

# Pixel Patrol

Louis Jean

Master 1 IMAGINE  
Faculté des Sciences, Université de Montpellier

23 avril 2024

Détection de falsifications dans des images



# Sommaire

- 1 Contexte et enjeux
- 2 État de l'art
  - Les méthodes de falsification
  - Méthodes de détection actuelles
  - Bases de données disponibles
- 3 Pixel Patrol
  - Méthodes de détection implémentées
    - Première méthode : détection de copy-move
    - Deuxième méthode : détection de splicing et removal
    - Troisième méthode : classification des images
  - Résultats
    - Définition des métriques d'évaluation
    - Résultats de la première méthode sur le dataset CoMoFoD
    - Résultats de la deuxième méthode sur le dataset In the Wild
    - Interface graphique utilisateur
  - Démonstration
- 4 Conclusion
- 5 Références

# Vue d'ensemble

## 1 Contexte et enjeux

## 2 État de l'art

- Les méthodes de falsification
- Méthodes de détection actuelles
- Bases de données disponibles

## 3 Pixel Patrol

### • Méthodes de détection implémentées

- Première méthode : détection de copy-move
- Deuxième méthode : détection de splicing et removal
- Troisième méthode : classification des images

### • Résultats

- Définition des métriques d'évaluation
- Résultats de la première méthode sur le dataset CoMoFoD
- Résultats de la deuxième méthode sur le dataset In the Wild
- Interface graphique utilisateur

### • Démonstration

## 4 Conclusion

## 5 Références

# Contexte et enjeux

- On estime à 760 milliards le nombre d'images en circulation sur internet
- L'authenticité visuelle est une monnaie de confiance
- Les images sont très puissantes pour façonner l'opinion publique
- L'évolution de la technologie a grandement simplifié la création de contenus falsifiés convaincants
- Ces manipulations posent des risques importants : propagation de fausses informations, atteintes à la réputation, conséquences sécuritaires
- Être capable de démeler le vrai du faux dans les images est donc primordial pour maintenir l'intégrité informationnelle

# Vue d'ensemble

## 1 Contexte et enjeux

## 2 État de l'art

- Les méthodes de falsification
- Méthodes de détection actuelles
- Bases de données disponibles

## 3 Pixel Patrol

- Méthodes de détection implémentées
  - Première méthode : détection de copy-move
  - Deuxième méthode : détection de splicing et removal
  - Troisième méthode : classification des images
- Résultats
  - Définition des métriques d'évaluation
  - Résultats de la première méthode sur le dataset CoMoFoD
  - Résultats de la deuxième méthode sur le dataset In the Wild
  - Interface graphique utilisateur
- Démonstration

## 4 Conclusion

## 5 Références

# Vue d'ensemble

## 1 Contexte et enjeux

## 2 État de l'art

- Les méthodes de falsification

- Méthodes de détection actuelles
- Bases de données disponibles

## 3 Pixel Patrol

- Méthodes de détection implémentées

- Première méthode : détection de copy-move
- Deuxième méthode : détection de splicing et removal
- Troisième méthode : classification des images

- Résultats

- Définition des métriques d'évaluation
- Résultats de la première méthode sur le dataset CoMoFoD
- Résultats de la deuxième méthode sur le dataset In the Wild
- Interface graphique utilisateur

- Démonstration

## 4 Conclusion

## 5 Références

# Les méthodes de falsification

- **Copy-move (C-M)** : duplication d'une partie de l'image pour masquer ou cloner des objets
- **Splicing** : combinaison de morceaux de différentes images pour créer nouvelle image
- **Removal** : suppression d'un élément d'une image
- **Deepfake** : utilisation de l'intelligence artificielle pour remplacer les visages ou simuler des vidéos
- **Quelques exemples parmi tant d'autres :**
  - Photos retouchées de célébrités influençant les normes esthétiques
  - Falsifications d'images de surveillance utilisées pour incriminer des innocents
  - Désinformation appuyée sur des images falsifiées
  - ...

# Les méthodes de falsification : exemples



Figure 1 – Falsification par copy-move



Figure 3 – Falsification par removal



Figure 2 – Falsification par splicing



Figure 4 – Falsification par deepfake

# Vue d'ensemble

## 1 Contexte et enjeux

## 2 État de l'art

- Les méthodes de falsification
- Méthodes de détection actuelles
- Bases de données disponibles

## 3 Pixel Patrol

- Méthodes de détection implémentées
  - Première méthode : détection de copy-move
  - Deuxième méthode : détection de splicing et removal
  - Troisième méthode : classification des images
- Résultats
  - Définition des métriques d'évaluation
  - Résultats de la première méthode sur le dataset CoMoFoD
  - Résultats de la deuxième méthode sur le dataset In the Wild
  - Interface graphique utilisateur
- Démonstration

## 4 Conclusion

## 5 Références

# Méthodes de détection actuelles

Pour détecter les falsifications, plusieurs approches ont été développées :

- Cohérence des pixels : couleur, bruit, motifs, et estimation de la source de lumière.
- Analyse en fréquence : utilisation de la FFT, filtres passe-haut, et amplification des artefacts.
- Examen des métadonnées et techniques de tatouage numérique (watermarking).

Les méthodes contemporaines s'appuient de plus en plus sur l'intelligence artificielle :

- Réseaux de neurones (CNN) pour la reconnaissance de motifs
- Machines à vecteurs de support (SVM) pour la classification

Ces méthodes plus récentes montrent une efficacité accrue par rapport aux techniques traditionnelles.

# Vue d'ensemble

## 1 Contexte et enjeux

## 2 État de l'art

- Les méthodes de falsification
- Méthodes de détection actuelles
- **Bases de données disponibles**

## 3 Pixel Patrol

- Méthodes de détection implémentées
  - Première méthode : détection de copy-move
  - Deuxième méthode : détection de splicing et removal
  - Troisième méthode : classification des images
- Résultats
  - Définition des métriques d'évaluation
  - Résultats de la première méthode sur le dataset CoMoFoD
  - Résultats de la deuxième méthode sur le dataset In the Wild
  - Interface graphique utilisateur
- Démonstration

## 4 Conclusion

## 5 Références

# Bases de données disponibles

Il existe des bases de données spécialement conçues pour la détection de falsifications des images. En voici une liste non-exhaustive :

- **Splicing, copy-move, removal** : CASIA 1.0, CASIA 2.0, NIST, ...
- **Splicing** : Wild Web, MISD, VIIPP, ...
- **Copy-move** : CoMoFoD, COVERAGE, ...

# Vue d'ensemble

## 1 Contexte et enjeux

## 2 État de l'art

- Les méthodes de falsification
- Méthodes de détection actuelles
- Bases de données disponibles

## 3 Pixel Patrol

### • Méthodes de détection implémentées

- Première méthode : détection de copy-move
- Deuxième méthode : détection de splicing et removal
- Troisième méthode : classification des images

### • Résultats

- Définition des métriques d'évaluation
- Résultats de la première méthode sur le dataset CoMoFoD
- Résultats de la deuxième méthode sur le dataset In the Wild
- Interface graphique utilisateur

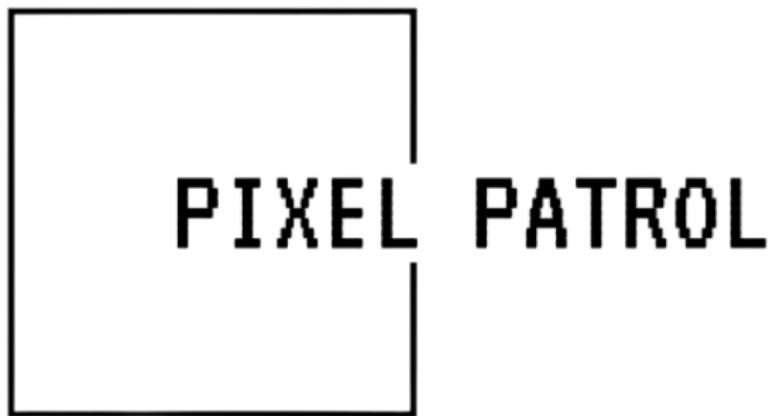
### • Démonstration

## 4 Conclusion

## 5 Références

# Pixel Patrol

Pixel Patrol est une application visant à détecter et analyser les falsifications d'images. Elle offre aux utilisateurs un moyen efficace de vérifier l'authenticité des images et de localiser les modifications potentielles. L'application est écrite en Python, tout comme son interface graphique qui utilise CustomTkinter.



# Vue d'ensemble

## 1 Contexte et enjeux

## 2 État de l'art

- Les méthodes de falsification
- Méthodes de détection actuelles
- Bases de données disponibles

## 3 Pixel Patrol

### • Méthodes de détection implémentées

- Première méthode : détection de copy-move
- Deuxième méthode : détection de splicing et removal
- Troisième méthode : classification des images

### • Résultats

- Définition des métriques d'évaluation
- Résultats de la première méthode sur le dataset CoMoFoD
- Résultats de la deuxième méthode sur le dataset In the Wild
- Interface graphique utilisateur

### • Démonstration

## 4 Conclusion

## 5 Références

# Méthodes de détection implémentées

Pixel Patrol inclut trois méthodes différentes dans leurs implantations et leurs objectifs.

- **Première méthode** : excellant dans la détection de falsification par copy-move, elle utilise les algorithmes SIFT et RANSAC.
- **Deuxième méthode** : spécialisée dans la détection de falsification par splicing et removal, elle fait appel à la DCT.
- **Troisième méthode** : ayant pour unique but de classifier les images authentiques ou falsifiées, elle utilise le LBP, la DCT et un SVM.

# Première méthode : détection de copy-move

Cette méthode est tirée de l'article [1], qui propose une approche robuste utilisant SIFT et RANSAC.

- **Qu'est-ce que SIFT (Scale-Invariant Feature Transform) ?**

- Algorithme mis au point en 1999 par David Lowe
- Déetecte et décrit les points d'intérêt locaux dans les images
- Les caractéristiques sont invariantes à l'échelle, la rotation et partiellement au changement de perspective

- **Qu'est-ce que RANSAC (RAnDom SAmple Consensus) ?**

- Algorithme publié par Fischler et Bolles en 1981
- Estime les paramètres d'un modèle mathématique à partir d'un ensemble de données observées
- Sélectionne un sous-ensemble aléatoire des points, construit un modèle de transformation possible, puis vérifie le nombre de points s'adaptant à ce modèle
- Répète le processus pour trouver le modèle le plus robuste

- Pourquoi SIFT ?

- **Robustesse** : SIFT détecte des points d'intérêt qui sont invariants à l'échelle, la rotation, et partiellement à la translation, le rendant idéal pour identifier des régions similaires dans différentes parties de l'image
- **Précision** : les descripteurs obtenus fournissent une représentation détaillée des points-clés, permettant une comparaison précise entre les régions copiées et déplacées

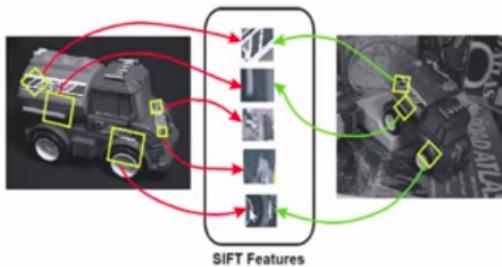


Figure 5 – Exemple de capture de caractéristiques SIFT

- Pourquoi RANSAC ?

- **Fiabilité** : RANSAC est robuste aux données aberrantes et peut donc trouver les transformations appliquées aux zones copiées même si certains points d'appariement sont incorrects
- **Sélectivité** : le processus itératif garantit le meilleur modèle qui explique le plus grand nombre de points entre les régions suspectées d'être copiées, minimisant ainsi l'impact des erreurs de détection.



Figure 6 – Jeu de données avec valeurs aberrantes

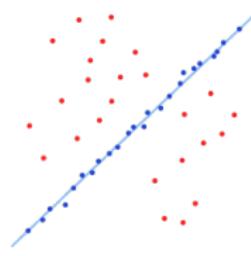


Figure 7 – Modèle trouvé par RANSAC

# La première méthode en quelques mots

Pour résumer la première méthode en quelques mots :

- D'abord, l'image est chargée et convertie en niveaux de gris pour simplifier l'analyse
- SIFT est utilisé pour identifier les points d'intérêt robustes et leurs descripteurs
- Les points clés sont comparés à l'aide du cosinus de l'angle entre leurs descripteurs pour trouver des correspondances potentielles, indiquant des régions dupliquées
- RANSAC est utilisé pour affiner les correspondances et exclure les fausses correspondances
- Enfin, un masque est créé pour visualiser les régions de l'image où la duplication a été détectée

# Résultats visuels de la première méthode

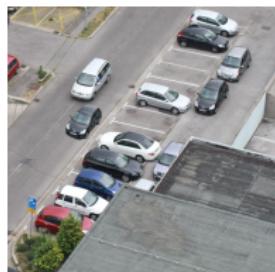


Figure 8 – Image falsifiée par C-M



Figure 10 – Masque de prédiction



Figure 9 – Extraction des points d'intérêt



Figure 11 – Masque de vérité

# Résultats visuels de la première méthode



Figure 12 – Image falsifiée par C-M

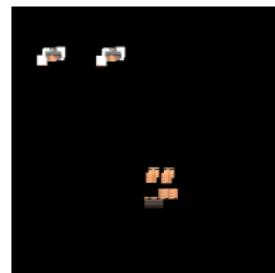


Figure 14 – Masque de prédiction



Figure 13 – Extraction des points d'intérêt

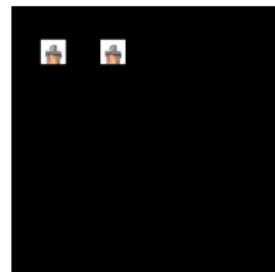


Figure 15 – Masque de vérité

# Résultats visuels de la première méthode

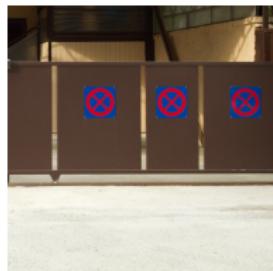


Figure 16 – Image falsifiée par C-M

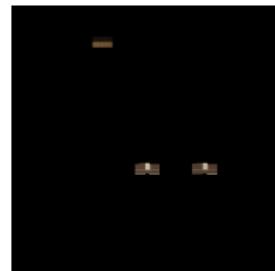


Figure 18 – Masque de prédiction

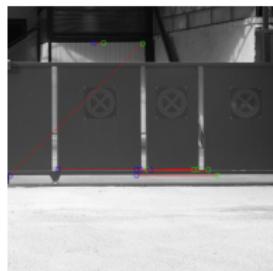


Figure 17 – Extraction des points d'intérêt

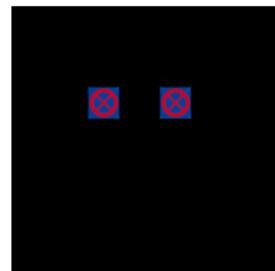


Figure 19 – Masque de vérité

## Deuxième méthode : détection de splicing et removal

Cette méthode s'inspire de l'article [2], qui établit une méthode de détection de falsifications basée sur l'analyse des coefficients DCT. Elle repose sur le principe que les manipulations d'image affectent principalement les hautes fréquences.

- **Qu'est-ce que la DCT (Discrete Cosinus Transform) ?**
  - La DCT est un outil mathématique utilisé pour convertir les données spatiales en données fréquentielles
- **Pourquoi la DCT ?**
  - Pour la détection de falsification, la DCT peut révéler des incohérences dans les fréquences qui pourraient ne pas être visibles dans le domaine spatial

## La deuxième méthode en quelques mots

Pour résumer la deuxième méthode en quelques mots :

- D'abord, l'image est chargée et convertie dans l'espace YCrCb pour utiliser le canal Y (luminance)
- L'image est découpée en blocs (de taille identique mais configurable)
- Sur chaque bloc, la DCT est appliquée, puis seules les hautes fréquences sont conservées (la partie inférieure droite du bloc DCT)
- Un seuil est déterminé grâce à la moyenne et à l'écart-type des hautes fréquences
- Chaque fréquence supérieure à ce seuil est marquée en rouge sur l'image de base
- Une ouverture puis une fermeture sont appliquées sur cette nouvelle image pour minimiser les erreurs
- Enfin, un masque est créé pour visualiser les régions suspectées de falsification

# Résultats visuels de la deuxième méthode



Figure 20 – Image falsifiée par slicing



Figure 22 – Masque de prédiction



Figure 21 – Détection (blocs 8x8)



Figure 23 – Masque de vérité

# Résultats visuels de la première méthode



Figure 24 – Image falsifiée par removal



Figure 25 – Détection (blocs 8x8)

# Résultats visuels de la deuxième méthode



Figure 26 – Image falsifiée par slicing



Figure 28 – Masque de prédiction



Figure 27 – Détection (blocs 8x8)

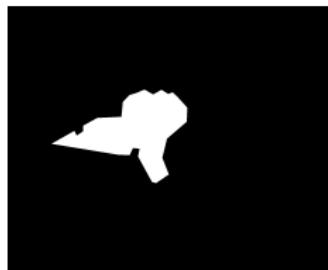


Figure 29 – Masque de vérité

# Troisième méthode : classification des images

Cette méthode reprend la technique présentée dans l'article [3]. Elle s'appuie sur le calcul de caractéristiques dans l'image grâce au LBP et à la DCT, puis procède à l'entraînement d'une machine à vecteurs de support (SVM).

- **Qu'est-ce que le LBP (Local Binary Pattern) ?**

- Le LBP est un descripteur de texture simple et efficace qui résume les motifs locaux de pixels en comparant chaque pixel avec ses voisins directs et en encodant le résultat en binaire

- **Qu'est-ce qu'un SVM ?**

- Un SVM est un modèle d'apprentissage supervisé qui analyse les données, utilisé pour la classification en trouvant l'hyperplan qui maximise la marge entre les classes de données

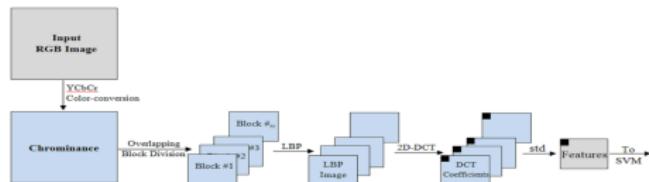


Figure 30 – Pipeline de la troisième méthode

## La troisième méthode en quelques mots

Pour résumer la troisième méthode en quelques mots :

- D'abord, l'image est convertie en espace colorimétrique YCrCb, et les canaux Cr et Cb sont extraits pour l'analyse
- L'image est découpée en petits blocs carrés qui sont traités individuellement, ce qui permet de capter des caractéristiques locales
- Sur chaque bloc, le LBP est calculé pour capturer la texture locale, suivi d'une transformation DCT pour quantifier les fréquences de ces textures
- L'écart-type des coefficients DCT de chaque bloc est calculé comme caractéristique représentative
- Les caractéristiques extraites de tous les blocs sont normalisées
- Enfin, les caractéristiques normalisées sont utilisées pour entraîner un SVM, qui apprend à distinguer entre les images authentiques et celles qui ont été falsifiées

# Vue d'ensemble

## 1 Contexte et enjeux

## 2 État de l'art

- Les méthodes de falsification
- Méthodes de détection actuelles
- Bases de données disponibles

## 3 Pixel Patrol

- Méthodes de détection implémentées
  - Première méthode : détection de copy-move
  - Deuxième méthode : détection de splicing et removal
  - Troisième méthode : classification des images

## • Résultats

- Définition des métriques d'évaluation
- Résultats de la première méthode sur le dataset CoMoFoD
- Résultats de la deuxième méthode sur le dataset In the Wild
- Interface graphique utilisateur

## • Démonstration

## 4 Conclusion

## 5 Références

# Définition des métriques d'évaluation

- **Précision** : rapport entre le nombre de vrais positifs et le nombre total de cas classés positifs, mesure la précision des prédictions positives
- **Rappel** : rapport entre le nombre de vrais positifs et le nombre total de cas positifs réels, mesure la capacité du modèle à détecter tous les cas positifs
- **F1-score** : moyenne harmonique de la précision et du rappel, donne un seul score qui équilibre les deux métriques
- **Indice de Jaccard** : rapport entre l'intersection et l'union des deux ensembles prédits et réels

# Résultats de la première méthode sur le dataset CoMoFoD

Le dataset CoMoFoD comporte 200 images, toutes falsifiées par copy-move, ainsi que leurs masques de vérité.

Précision	Rappel	F1-score	Indice de Jaccard
52,1%	96,9%	55,7%	44,2%

Table 1 – Performances de la première méthode sur le dataset CoMoFoD

## Résultats de la deuxième méthode sur le dataset In the Wild

Le dataset In the Wild contient 201 images, toutes falsifiées par splicing, ainsi que leurs masques de vérité.

Taille de bloc	Précision	Rappel	F1-score	Indice de Jaccard
4	75,2%	27,3%	20,6%	12,8%
8	79,6%	17,5%	14,6%	10,1%
16	72,9%	31,3%	21,9%	13,7%
32	71,2%	47,5%	26,2%	15,8%

Table 2 – Performances de la deuxième méthode sur le dataset In the Wild pour différentes tailles de blocs

## Résultats de la troisième méthode

Le SVM a été entraîné sur la base de données CASIA 2.0. Les données ont été remaniées pour contenir exactement 5123 images authentiques et 5123 images falsifiées.

Classe	Précision	Rappel	F1-score	Support
Authentique	72%	68%	70%	1043
Falsifiée	69%	73%	71%	1007
Moyenne pondérée	<b>70%</b>	<b>70%</b>	<b>70%</b>	<b>2050</b>

Table 3 – Résultats de classification du modèle

Taux de bonnes réponses sur le dataset CoMoFoD : 98% (196/200)

Taux de bonnes réponses sur le dataset In the Wild : 85% (170/201)

Taux de bonnes réponses sur le dataset CASIA 1.0 : 43% (741/1721)

# Interface graphique utilisateur

Pour rassembler toutes ces méthodes au sein d'une application et permettre à l'utilisateur une utilisation intuitive et simple, Pixel Patrol propose une interface graphique. On peut y choisir la méthode de détection, visualiser les images originales et résultantes, et obtenir des métriques sur la détection.

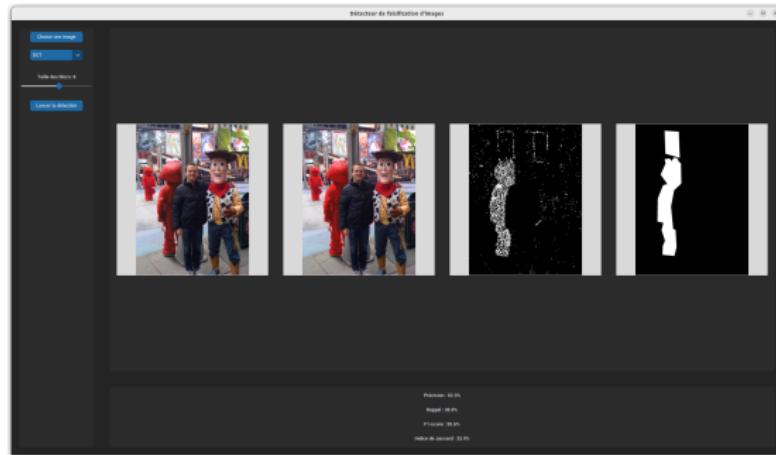


Figure 31 – Interface graphique utilisateur

# Vue d'ensemble

## 1 Contexte et enjeux

## 2 État de l'art

- Les méthodes de falsification
- Méthodes de détection actuelles
- Bases de données disponibles

## 3 Pixel Patrol

### • Méthodes de détection implémentées

- Première méthode : détection de copy-move
- Deuxième méthode : détection de splicing et removal
- Troisième méthode : classification des images

### • Résultats

- Définition des métriques d'évaluation
- Résultats de la première méthode sur le dataset CoMoFoD
- Résultats de la deuxième méthode sur le dataset In the Wild
- Interface graphique utilisateur

### • Démonstration

## 4 Conclusion

## 5 Références

# Démonstration

Veuillez apprécier cette vidéo de présentation de Pixel Patrol

# Vue d'ensemble

- 1 Contexte et enjeux
- 2 État de l'art
  - Les méthodes de falsification
  - Méthodes de détection actuelles
  - Bases de données disponibles
- 3 Pixel Patrol
  - Méthodes de détection implémentées
    - Première méthode : détection de copy-move
    - Deuxième méthode : détection de splicing et removal
    - Troisième méthode : classification des images
  - Résultats
    - Définition des métriques d'évaluation
    - Résultats de la première méthode sur le dataset CoMoFoD
    - Résultats de la deuxième méthode sur le dataset In the Wild
    - Interface graphique utilisateur
  - Démonstration
- 4 Conclusion
- 5 Références

- **Importance des détecteurs de falsifications** : enjeux importants, besoin extrêmement croissant
- **Contribution de Pixel Patrol** : un outil pour détecter et analyser les falsifications d'images, pas excellent mais a des perspectives d'amélioration
- **Tests sur diverses bases de données** : mesures de l'efficacité de l'outil
- **Améliorations futures** : perspectives d'amélioration de toutes les méthodes, notamment de l'apprentissage, et de l'interface utilisateur pour une expérience plus intuitive

Merci pour votre attention !

*Remerciements à M. Reinders et M. Puech pour  
l'encadrement de ce projet*

# Des questions ?

# Vue d'ensemble

## 1 Contexte et enjeux

## 2 État de l'art

- Les méthodes de falsification
- Méthodes de détection actuelles
- Bases de données disponibles

## 3 Pixel Patrol

- Méthodes de détection implémentées
  - Première méthode : détection de copy-move
  - Deuxième méthode : détection de splicing et removal
  - Troisième méthode : classification des images
- Résultats
  - Définition des métriques d'évaluation
  - Résultats de la première méthode sur le dataset CoMoFoD
  - Résultats de la deuxième méthode sur le dataset In the Wild
  - Interface graphique utilisateur
- Démonstration

## 4 Conclusion

## 5 Références

## Références I

- [1] Gonapalli Ramu et S. B. G. Thilak Babu. "Image forgery detection for high resolution images using SIFT and RANSAC algorithm". In : *2017 2nd International Conference on Communication and Electronics Systems (ICCES)*. 2017, p. 850-854. doi : 10.1109/CESYS.2017.8321205.
- [2] Phuong Nguyen et al. "An Image Forgery Detection Solution based on DCT Coefficient Analysis". In : jan. 2019, p. 487-494. doi : 10.5220/0007412804870494.
- [3] Amani A. Alahmadi et al. "Splicing image forgery detection based on DCT and Local Binary Pattern". In : *2013 IEEE Global Conference on Signal and Information Processing*. 2013, p. 253-256. doi : 10.1109/GlobalsIP.2013.6736863.
- [4] Zihao Zhang. *Image forgery datasets lists*.  
<https://github.com/greatzh/Image-Forgery-Datasets-List>.

## Références II

- [5] Figure 1. *146\_F.png*. CoMoFoD dataset.
- [6] Figure 2. *5492.png*. In the Wild dataset.
- [7] Figure 3. *Image d'origine modifiée par mes soins*.  
<https://www.nostalgie.fr/actus/jackson-five-bee-gees-ces-groupes-qui-ont-ete-crees-en-famille-70243222>.
- [8] Figure 4. *morgan\_freeman\_deepfake.png*.  
<https://www.dailystar.co.uk/tech/news/most-realistic-deepfake-ever-terrifies-28780484>.
- [9] Figure 5. *sift\_example.png*.  
<https://medium.com/@deepanshut041/introduction-to-sift-scale-invariant-feature-transform-65d7f3a72d40>.
- [10] Figure 6. *ransac1.png*. <https://fr.wikipedia.org/wiki/RANSAC>.
- [11] Figure 7. *ransac2.png*. <https://fr.wikipedia.org/wiki/RANSAC>.

## Références III

- [12] Figure 8. *059\_F.png*. CoMoFoD dataset.
- [13] Figure 11. *059\_M.png*. CoMoFoD dataset.
- [14] Figure 12. *003\_F.png*. CoMoFoD dataset.
- [15] Figure 15. *003\_M.png*. CoMoFoD dataset.
- [16] Figure 16. *009\_F.png*. CoMoFoD dataset.
- [17] Figure 19. *009\_M.png*. CoMoFoD dataset.
- [18] Figure 20. *im30\_edit6.jpg*. In the Wild dataset.
- [19] Figure 23. *im30\_edit6.png*. In the Wild dataset.
- [20] Figure 24. *Image d'origine modifiée par mes soins*.  
<https://www.nostalgie.fr/actus/jackson-five-bee-gees-ces-groupes-qui-ont-ete-crees-en-famille-70243222>.
- [21] Figure 26. *im3\_edit1.jpg*. In the Wild dataset.

## Références IV

- [22] Figure 29. *im3\_edit1.png*. In the Wild dataset.
- [23] Figure 30. *pipeline.png*. Image tirée de [3].