Image Hashing Using Adaptive Local Feature Extraction For Robust Tampering Detection

Chi Man Pun

Outline

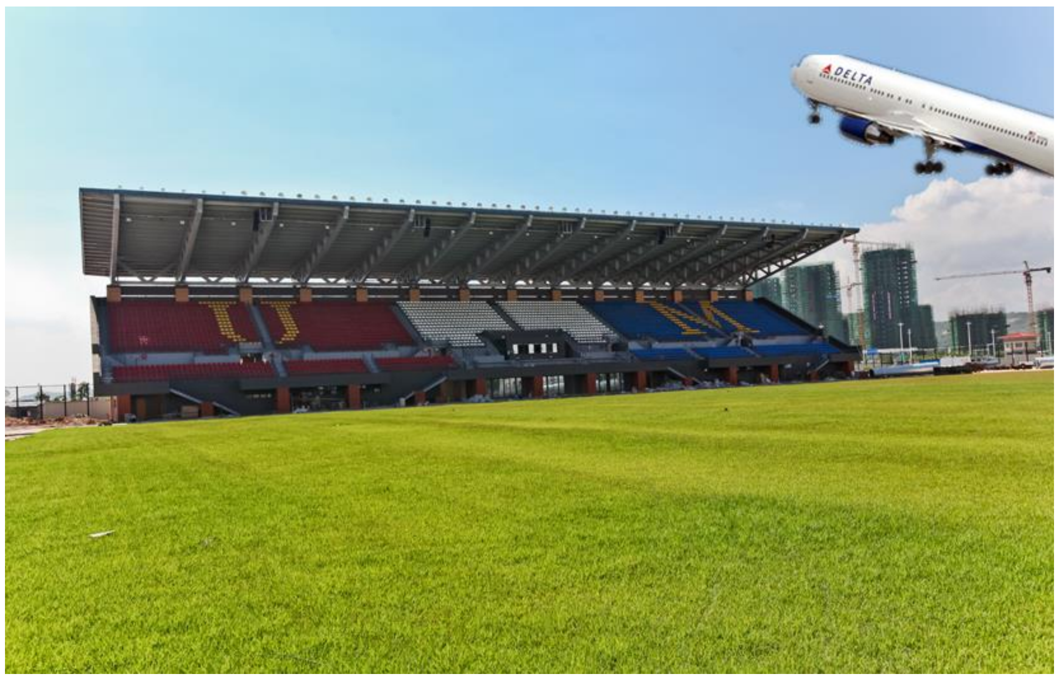
- **1 Introduction & Backgrounds**
- **2 Proposed Tampering Detection Model**
- **3 Experimental Results**
- **4 Conclusions & Future Works**

1 Introduction & Backgrounds

- For a long time, photographs are accepted as proof of evidences in varied fields such as journalism, forensic investigations, military intelligence, scientific research and publications, crime detection and legal proceedings, investigation of insurance claims, medical imaging etc.
- Today, digital images have completely replaced the conventional photographs from every sphere of life but unfortunately, they seldom enjoy the credibility of their conventional counterparts, thanks to the rapid advancements in the field of digital image processing.

1 Introduction & Backgrounds

Seeing is believing … or is it?



1 Introduction & Backgrounds

Easy to be tampered

Source image

Tampered image

1 Introduction & Backgrounds

Problem:

- With the widespread use of image editing software (such as Photoshop, Photoscape, PhotoPlus, etc.), ensuring credibility of the image contents has become an important issue.
- If tampered images are extensively used in the official media, scientific discovery and forensic evidence, will undoubtedly reduce trustworthiness and produce serious impact on various aspects of the society.

1 Introduction & Backgrounds

Image forgery detection :

- Active forgery detection
  - ✓Watermarking [Xie et al. 2001]
  - ✓Signature/hashing [Lv et al. 2012]
- Blind or passive forgery detection
  - ✓Copy-move/cloning [Fridrich et al. 2003]
  - ✓Splicing
    - JPEG compression properties [Hany Farid, 2006]
    - Lighting inconsistency [Johnson et al. 2005]
    - Chromatic aberration [Johnson et al. 2006]
    - Local noise [Gou et al. 2007]
    - ……

1 Introduction & Backgrounds

Hash-based Tampering Detection:

- Tampering detection is a scheme that identifies the integrity and primitivism of the digital multimedia data.
- An image hashing is a distinctive signature which represents the visual content of the image in a compact way. The image hashing should be robust against common operations but is different from the one computed on a different/tampered image.

1 Introduction & Backgrounds

Hash-based Tampering Detection:

1) a robust hashing designed for content-based identification is attached to the host image;
2) the hashing is analyzed at the destination to verify the reliability of the received image.

1 Introduction & Backgrounds

Hash-based Tampering Detection:

Received image

+ Image hashing

Source image

Tamper detection result

1 Introduction & Backgrounds

limitations:

- The comprehensiveness of tamper detection
  - for arbitrary size of the tampered region
  - for any position of the tampered regions in the image
- The accuracy of tamper localization
  - under various content-preserved attacks

2 Proposed Tampering Detection Model

Two procedures employed by our method:

2.1 Image hashing construction

- Adaptive feature point detection
- Local feature generation
- Multi-scale image hashing construction

2.2 Robust tampering detection scheme

- Image restoration
- Image authentication
- Tampering localization

2 Proposed Tampering Detection Model

Two procedures employed by our method:

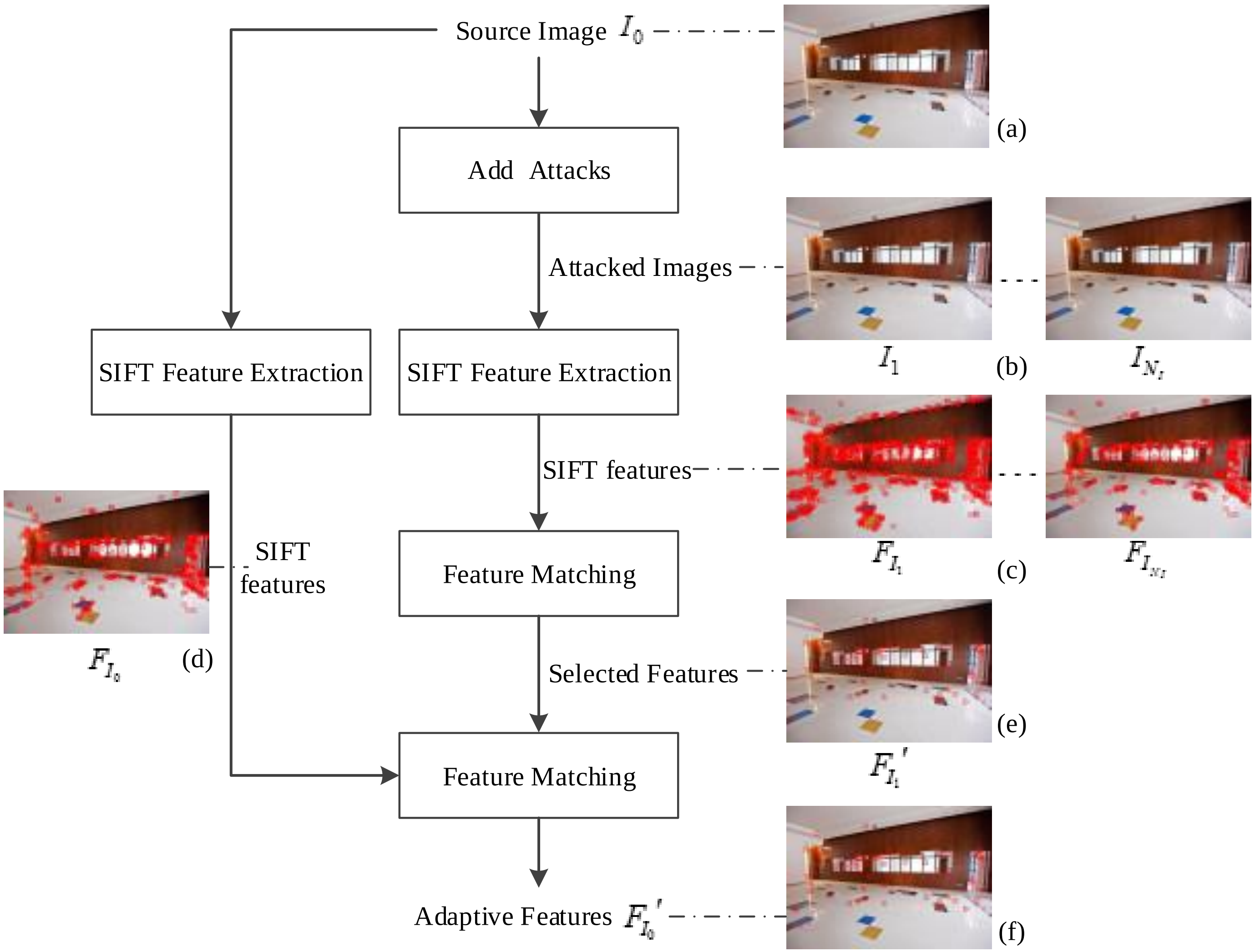
2.1 Image hashing construction

- Adaptive feature point detection (SIFT)
- Local feature generation
- Multi-scale image hashing construction

2.2 Robust tampering detection scheme

- Image restoration
- Image authentication
- Tampering localization

Adaptive feature point detection (SIFT)



2 Proposed Tampering Detection Model

Two procedures employed by our method:

2.1 Image hashing construction

- Adaptive feature point detection
- Local feature generation (SWT)
- Multi-scale image hashing construction

2.2 Robust tampering detection scheme

- Image restoration
- Image authentication
- Tampering localization

Local feature generation (SWT)

2 Proposed Tampering Detection Model

Two procedures employed by our method:

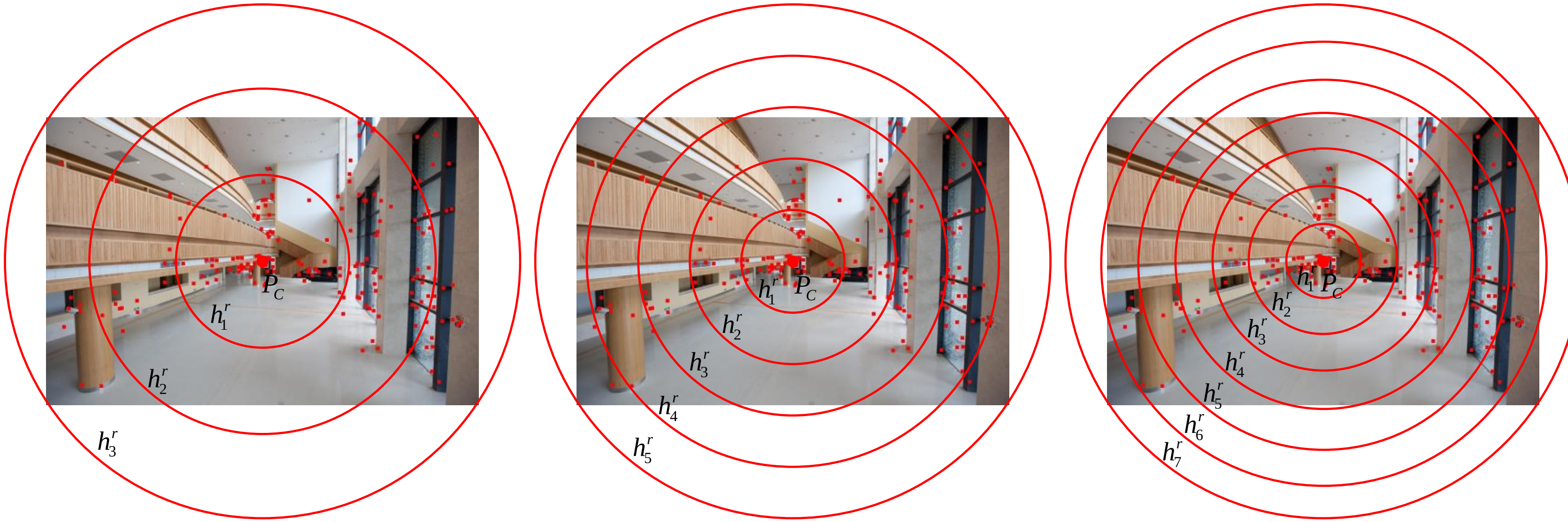
2.1 Image hashing construction

- Adaptive feature point detection
- Local feature generation
- Multi-scale image hashing construction

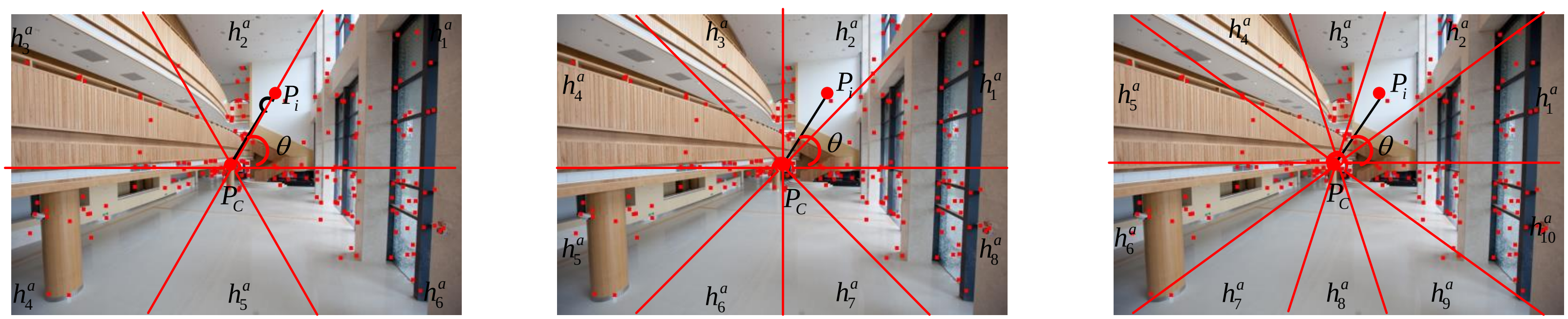
2.2 Robust tampering detection scheme

- Image restoration
- Image authentication
- Tampering localization

Multi-scale image hashing construction

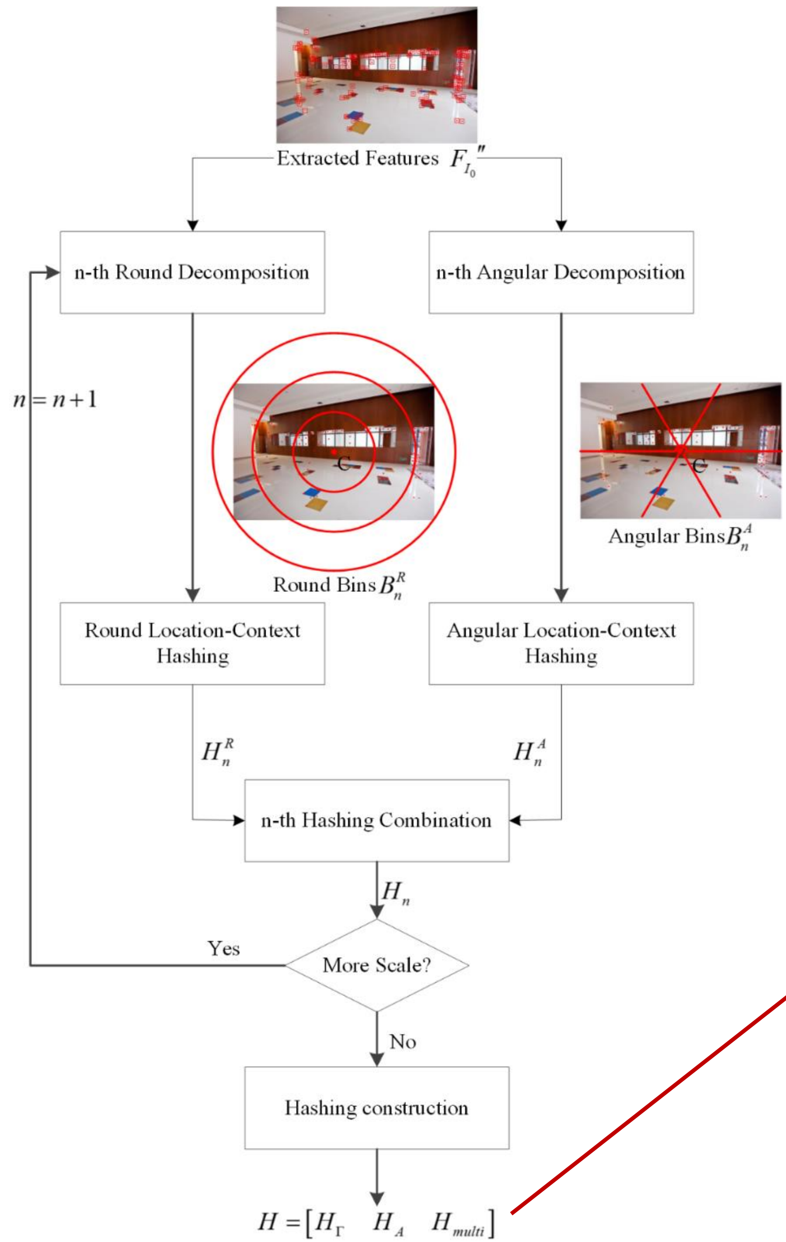


(a) $L_1^R = 3$ (b) $L_2^R = 5$ (c) $L_3^R = 7$



(d) $L_1^A = 6$ (e) $L_2^A = 8$ (f) $L_3^A = 10$

Multi-scale image hashing construction



H_Γ : the most robust feature points

H_A : the global hash for image authentication

H_{multi} : the multi-scale image hash for tamper localization

2 Proposed Tampering Detection Model

Two procedures employed by our method:

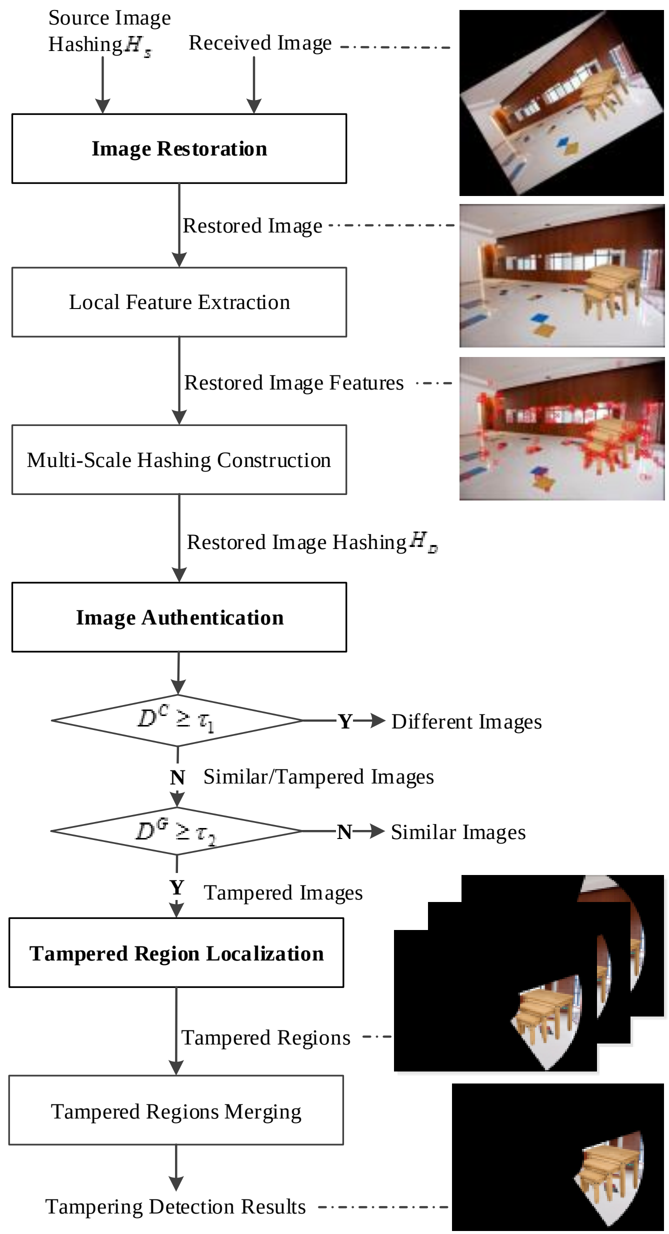
2.1 Image hashing construction

- Adaptive feature point detection
- Local feature generation
- Multi-scale image hashing construction

2.2 Robust tampering detection scheme

- Image restoration
- Image authentication
- Tampering localization

Robust tampering detection scheme



2 Proposed Tampering Detection Model

Two procedures employed by our method:

2.1 Image hashing construction

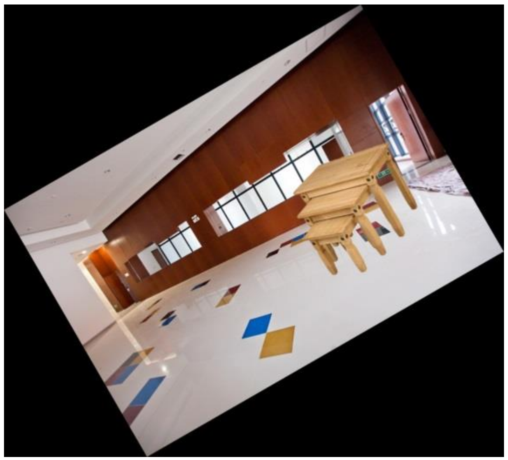
- Adaptive feature point detection
- Local feature generation
- Multi-scale image hashing construction

2.2 Robust tampering detection scheme

- Image restoration
- Image authentication
- Tampering localization

Image restoration

Source image



Received image

Restored image

+ Image hashing P_Γ

P_Γ : Γ most robust SIFT feature points, which is composed by the id lable, the dominant direction θ, and the coordinates (x, y) for each selected SIFT as in [10].

[10] S. Battiato, G. M. Farinella, E. Messina, and G. Puglisi, "Robust Image Alignment for Tampering Detection," *IEEE Transactions on Information Forensics and Security,* vol. 7, pp. 1105-1117, 2012.

2 Proposed Tampering Detection Model

Two procedures employed by our method:

2.1 Image hashing construction

- Adaptive feature point detection
- Local feature generation
- Multi-scale image hashing construction

2.2 Robust tampering detection scheme

- Image restoration
- Image authentication
- Tampering localization

Image authentication

Color distance: $D^{C} = \frac{Dist\left(H^{C\_S}, H^{C\_D}\right)}{\sum H^{C\_S}}$

Global distance: $D^{G} = \frac{\left|H^{G\_D} - H^{G\_S}\right|}{H^{G\_S}}$

Hash component of source image: $H_{\mathrm{A}\_S} = \left[H^{G\_S}, H^{C\_S}\right]$

Hash component of received image: $H_{\mathrm{A}\_D} = \left[H^{G\_D}, H^{C\_D}\right]$

H^{G} is calculated by summing all the local features of the feature points extracted with the proposed Adaptive Feature Point Detection algorithm.

H^{C} is average color values of the regions under one of image decomposition method.

2 Proposed Tampering Detection Model

Two procedures employed by our method:

2.1 Image hashing construction

- Adaptive feature point detection
- Local feature generation
- Multi-scale image hashing construction

2.2 Robust tampering detection scheme

- Image restoration
- Image authentication
- Tampering localization

Tampering localization

$$T_n^R = \left\{ b_\lambda^R(\lambda) : \frac{Del_\lambda^R}{\sum_{\lambda=1}^{L_n^R} Del_\lambda^R} \geq \delta_n \right\}, \quad Del_\lambda^R = \left| h_\lambda^R(I_S) - h_\lambda^R(I_D) \right|$$

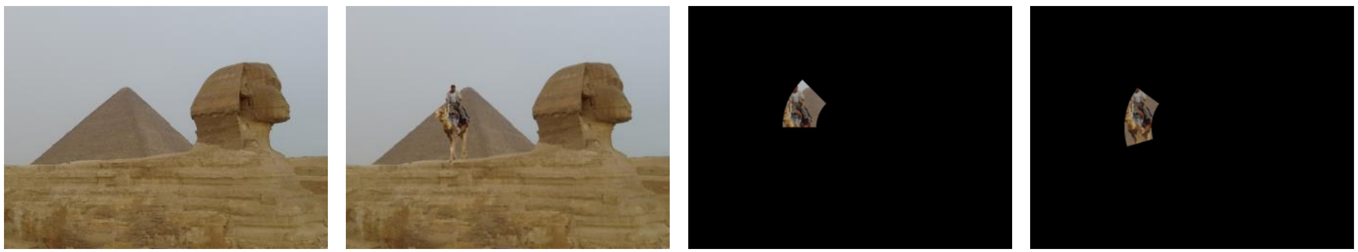
$$T_n^A = \left\{ b_\lambda^A(\lambda) : \frac{Del_\lambda^A}{\sum_{\lambda=1}^{L_n^A} Del_\lambda^A} \geq \delta_n \right\}, \quad Del_\lambda^A = \left| h_\lambda^A(I_S) - h_\lambda^A(I_D) \right|$$

$$T_n = T_n^R \cap T_n^A$$

$$T = T_1 \cap T_2 \cap \cdots \cap T_N$$

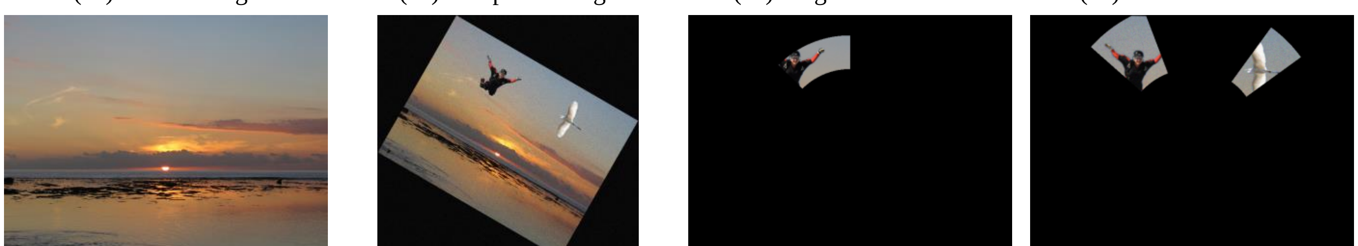
3 Experimental Results

(a1) Source image (a2) Tampered image (a3) Single-scale result (a4) Multi-scale result



(b1) Source image (b2) Tampered image (b3) Single-scale result (b4) Multi-scale result

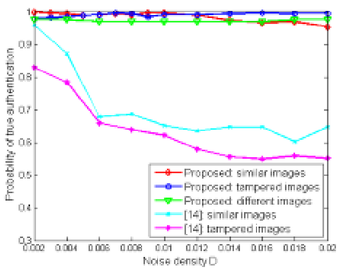
(c1) Source image (c2) Tampered image (c3) Single-scale result (c4) Multi-scale result



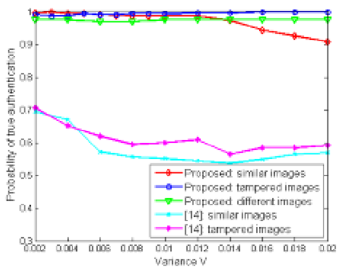
(d1) Source image (d2) Tampered image (d3) Single-scale result (d4) Multi-scale result

3 Experimental Results

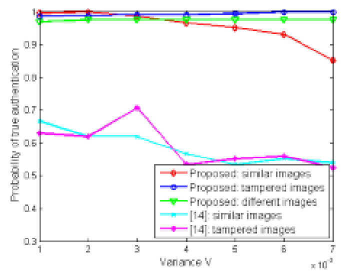
Comparison of image authentication performances under different attacks:



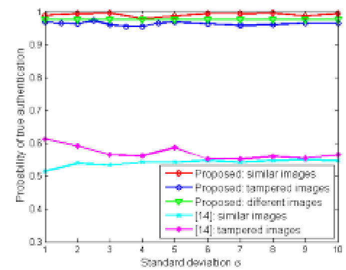
(a) Salt & Pepper Noise



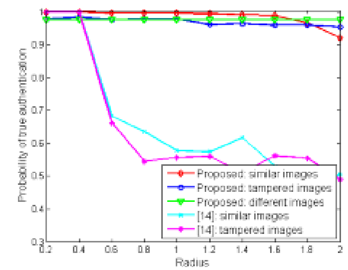
(b) Speckle Noise



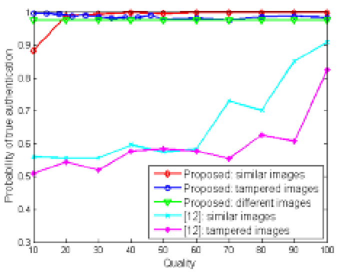
(c) Gaussian Noise



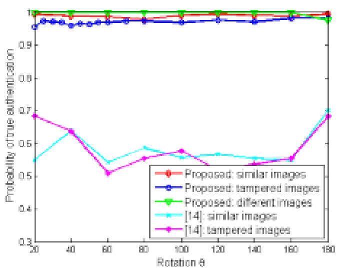
(d) Gaussian Blurring



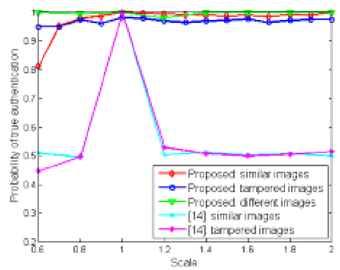
(e) Circular Blurring



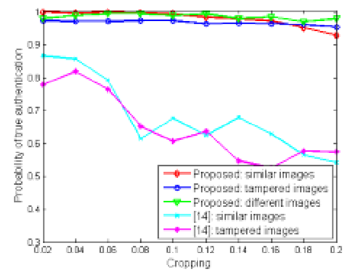
(f) JPEG Compression



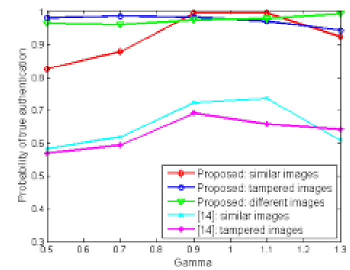
(g) Rotation



(h) Scaling



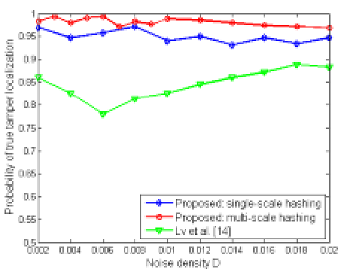
(i) Cropping



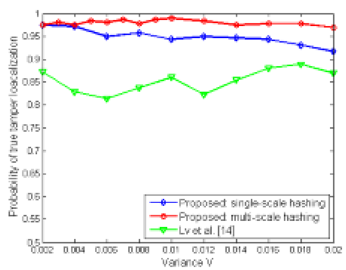
(j) Gamma Correction

3 Experimental Results

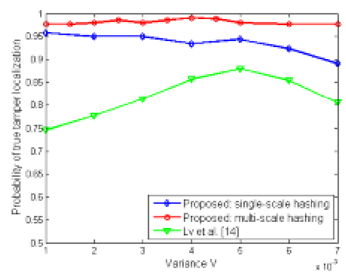
Comparison of tampering localization performances under different attacks



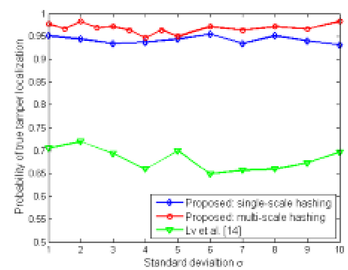
(a) Salt & Pepper Noise



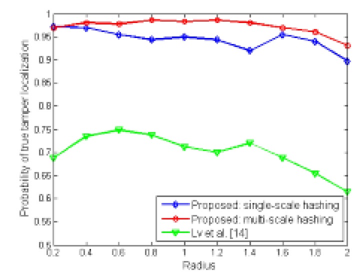
(b) Speckle Noise



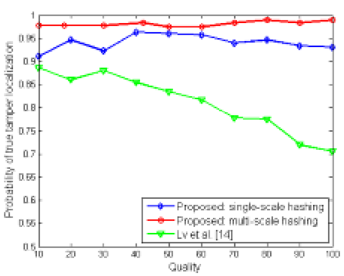
(c) Gaussian Noise



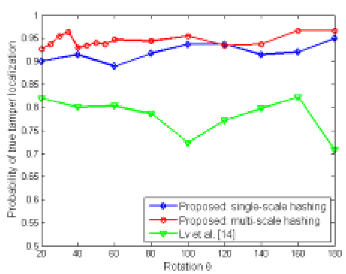
(d) Gaussian Blurring



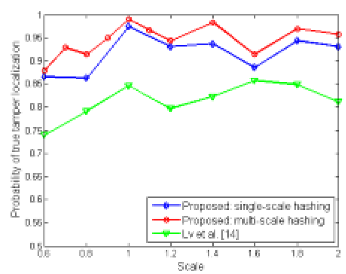
(e) Circular Blurring



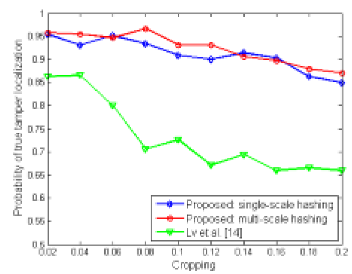
(f) JPEG Compression



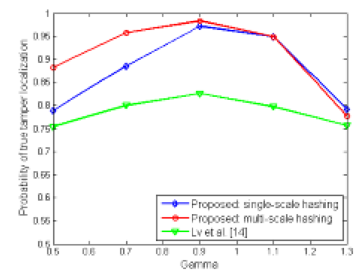
(g) Rotation



(h) Scaling



(i) Cropping



(j) Gamma Correction

3 Experimental Results

	Monga et al. 2007	Tang et al. 2008	Zhao et al. 2013	Lv et al. 2012	Wang et al. 2015	Proposed
Features used	Local	Global	Global & Local	Local	Local	**Global & Local**
Hashing length	64 digits	320 bits	560 bits	30 digits	Thousands of digits	**302 digits**
Robust against noise addition	Yes	Yes	Yes	Yes	Yes	**Yes**
Robust against blurring	Yes	Yes	Yes	Yes	Yes	**Yes**
Robust against cropping with boundary 20%	Yes	No	No	Yes	Yes	**Yes**
Robust against any-angle rotation	No	No	No	Yes	Yes	**Yes**
Robust against scaling	Yes	Yes	Yes	Yes	Yes	**Yes**
Ability to complete image authentication	Yes	Yes	Yes	Yes	Yes	**Yes**
Ability to locate tampered regions anywhere	No	No	No	No	Yes	**Yes**

4 Conclusions & Future Works

- **Advantages of proposed algorithm:**
  - ➢An adaptive local feature extraction method
  - ➢A multi-scale image hashing method

- **Future works:**
  - ➢More reliable feature generation
  - ➢More compact hash
  - ➢More accurate localization

Publication:

- C.-P. Yan, C.-M. Pun, and X.-C. Yuan, "Multi-scale image hashing using adaptive local feature extraction for robust tampering detection," *Signal Processing,* vol. 121, pp. 1-16, 2016.
- C.-P. Yan and C.-M. Pun, "Multi-Scale Difference Map Fusion for Tamper Localization Using Binary Ranking Hashing," *IEEE Transactions on Information Forensics and Security (TIFS)*, 12(9), pp. 2144 - 2158, 2017.
- C.-M. Pun, C.-P. Yan and X.-C. Yuan, "Image Alignment based Multi-Region Matching for Object-level Tampering Detection," *IEEE Transactions on Information Forensics and Security (TIFS)*, 12(2), pp. 377-391 2017.
- C.-P. Yan, C.-M. Pun and X.-C. Yuan, "Quaternion-based Image Hashing for Adaptive Tampering Localization," *IEEE Transactions on Information Forensics and Security (TIFS)*, 11(12), pp.2664-2677, 2016.

Thanks!