Multimedia Tools and Applications
https://doi.org/10.1007/s11042-018-6922-4

Copy-move forgery detection using combined features and transitive matching

Cong Lin[1,2] · Wei Lu[1,4] · Xinchao Huang[1] · Ke Liu[3] · Wei Sun[3] · Hanhui Lin[2] · Zhiyuan Tan[5]

Received: 13 May 2018 / Revised: 26 August 2018 / Accepted: 19 November 2018 /
Published online: 28 November 2018

Abstract

Recently, the research of Internet of Things (IoT) and Multimedia Big Data (MBD) has been growing tremendously. Both IoT and MBD have a lot of multimedia data, which can be tampered easily. Therefore, the research of multimedia forensics is necessary. Copy-move is an important branch of multimedia forensics. In this paper, a novel copy-move forgery detection scheme using combined features and transitive matching is proposed. First, SIFT and LIOP are extracted as combined features from the input image. Second, transitive matching is used to improve the matching relationship. Third, a filtering approach using image segmentation is proposed to filter out false matches. Fourth, affine transformations are estimated between these image patches. Finally, duplicated regions are located based on those affine transformations. The experimental results demonstrate that the proposed scheme can achieve much better detection results on the public database under various attacks.

Keywords Multimedia big data · Internet of things · Multimedia forensics · Region duplication detection · Copy-move forgery · Image segmentation · LIOP

✉ Wei Lu
luwei3@mail.sysu.edu.cn

Cong Lin
lincong0310@gmail.com

Zhiyuan Tan
z.tan@napier.ac.uk

[1] School of Data and Computer Science, Guangdong Key Laboratory of Information Security Technology, Sun Yat-sen University, Guangzhou 510006, China

[2] Center for Faculty Development and Educational Technology, Guangdong University of Finance and Economics, Guangzhou 510320, China

[3] School of Electronics and Information Technology, Key Laboratory of Information Technology (Ministry of Education), Sun Yat-sen University, Guangzhou 510006, China

[4] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

[5] School of Computing, Edinburgh Napier University, Edinburgh, EH10 5DT, UK

1 Introduction

In recent years, Internet of Things (IoT) [7] and Multimedia Big Data (MBD) [32, 84] represent two appealing fields for many researchers [48, 50, 76, 82]. Internet of Things (IoT) impart networked connectivity to everyday objects in the physical world [7]. Various electronic devices in IoT have generated huge multimedia data. Multimedia has become the “biggest big data”, which is MBD. There are many information security problems of IoT and MBD, i.e., the multimedia of IoT or MBD is tampered. The related research is multimedia forensics, which is a science of acquiring, analyzing, extracting, interpreting and producing an evidence from a multimedia source in civil, criminal or corporate cases of administrative nature [51].

Multimedia forensics [38, 61, 78, 80, 81] is an important domain of information security [9, 10, 12, 13, 19–24, 39]. Both IoT and MBD [17, 18, 28, 30, 42, 46, 47, 58, 62, 65–71, 75, 77, 79, 83, 85] have a lot of multimedia data. Therefore, the research of the multimedia forensics is very meaningful to IoT and MBD. The multimedia forensics can be divided into many branches, i.e., copy-move and splicing.

In a copy-move attack, one or more parts of an image are copied and pasted into another part of the same image [27]. The object of study of copy-move is multimedia data, many multimedia data make up MBD. Therefore, copy-move is an analysis and treatment of MBD. Many image Copy-Move Forgery Detection (CMFD) schemes [4, 5, 16, 25, 27, 29, 33, 34, 44, 49, 64, 72] have been proposed in recent years. According to Christlein et al. [15], commonly known copy-move detection schemes can be divided into two branches. The first one is the block-based schemes, an image is divided into fixed-size overlapping blocks, the each block is represented by a block descriptor, then those descriptors are sorted and matched. The main difference of the block-based schemes is their block features. Fridrich et al. [27] use the Discrete Cosine Transform (DCT) as block features. Popescu and Farid [53] use the Principal Component Analysis (PCA) as block features. Bashar et al. [5] propose a CMFD method using the Discrete Wavelet Transform (DWT) or the Kernel Principal Component Analysis (KPCA). An improved DCT-based method is proposed by Huang et al. [34]. Bravo-Solorio and Nandi [8] propose a CMFD scheme based on the Fourier Transform. Li et al. [41] use the Polar Cosine Transform (PCT) as block features. Ryu et al. [55, 56] propose a CMFD scheme using Zernike moment, and Locality Sensitive Hashing (LSH) matching is adopted in [55]. A histogram of orientated gradients is applied to each block in [36]. A fast Walsh-Hadamard Transform (FWHT) is adopted in [73].

The block-based schemes are not robust to scale, rotation, JPEG compression and additive noise. So keyponint-based schemes are proposed. Feature exaction methods such as the Scale-Invariant Feature Transform (SIFT) [45] and the Speeded Up Robust Features (SURF) [6] are most widely used in keypoint-based schemes. Pan and Lyu [52] propose a framework of the keypoint-based schemes, and their feature was also SIFT. Amerini et al. [3] propose a method using SIFT feature, the g2NN matching and the Agglomerative Hierarchical Clustering (AHC). Shivakumar and Baboo [57] propose a scheme based on SURF and KD-Tree. Silva et al. [59] construct a multi-scale image representation and a voting process among all detection maps. A rotation invariance scheme is proposed by Christlein et al. [14]. The Harris corner points [31] in an image are detected in [11], and their description is based on step sector statistics. Li et al. [40] propose a scheme using the Maximally Stable Color Region (MSCR). Yang et al. [74] propose a scheme using KAZE [2] and SIFT [45]. The image segmentation is adopted by Li et al. [37] and Pun et al. [54]. The image is segmented by Simple Linear Iterative Clustering (SLIC) algorithm [1] before feature extraction. Lin et al. [43] propose a Keypoint Contexts (KC) scheme to deal with duplicated regions with few keypoints. Jin and Wang [35] use OpponentSIFT and optimized J-Linkage to detect duplicated regions.

The block-based scheme is not robust and the keypoint-based scheme cannot detect duplicated regions with few keypoints. To overcome this issue, in this paper, a novel copy-move forgery detection scheme using combined features and transitive matching is proposed.

The remainder of this paper is organized into three sections. Section 2 shows the framework of the proposed scheme and then explains each step in detail. To validate the effectiveness of the proposed scheme, the experimental results are given in Section 3. Finally, Section 4 draws conclusions.

2 The proposed scheme

2.1 Combined features extraction

A block-based scheme is good at plain copy-move, but it cannot deal with significant geometrical transformations. A keypoint-based scheme is more robust than a block-based scheme, but it cannot deal with duplicated regions with few keypoints. Therefore, a strategy of combined features is proposed by our scheme, where both the Local Intensity Order Pattern (LIOP) [63] and the Scale Invariant Feature Transform (SIFT) [45] are adopted as our combined features. The outline of the proposed scheme is shown in Fig. 1.

Now we describe the reason why we choose LIOP and SIFT as the combined features. First, SIFT is invariant to image scale, rotation, addition of noise, etc. Meanwhile, SIFT has been widely used in many CMFD schemes [3, 4, 52] and obtained good results. Second, both local and overall intensity ordinal information of the local patch are captured by the LIOP descriptor [63]. Therefore, LIOP is invariant to image scale, rotation, viewpoint change, image blur and JEPG compression. We choose combined features to deal with duplicated regions with few keypoints.

We are familiar with SIFT. So let's introduce LIOP [63]. The main idea of LIOP is that when the intensity monotonous changes, the relative order of pixel intensities remains unchanged. The steps of LIOP are as follows. First, the local patch is divided into ordinal bins using the overall intensity order. Second, for a point x, the LIOP of which is defined as follows [63]:

$$LIOP(x) = \Phi(\gamma(P(x))) \tag{1}$$

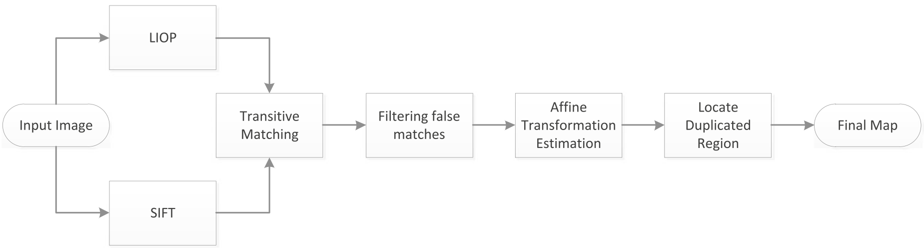


Fig. 1 The framework of the copy-move forgery detection scheme

where $P(x) = (I(x_1), I(x_2), \cdots, I(x_N)) \in P^N$ and $I(x_i)$ represent the intensity of the i-th neighboring sample point x_i. Third, for a local patch, to accumulate the LIOPs of points in each ordinal bin, we obtained the LIOP descriptor [63]:

$$\begin{aligned} D_{LIOP} &= (des_1, des_2, \cdots, des_B) \\ des_i &= \Sigma_{x \in bin_i} \omega(x) LIOP(x) \end{aligned} \tag{2}$$

where $\omega(x)$ is a weighting function and B is the number of the ordinal bins.

In some cases, the results of LIOP are better than that of SIFT. But in other cases, the results of SIFT are better than that of LIOP. Therefore, both LIOP and SIFT are integrated as our combined features, and the results of combined features are better than that of LIOP or SIFT, as shown in Fig. 2.

2.2 Transitive matching

The detected keypoints are tentatively matched using their feature vectors. There are two common matching methods. The first one is the 2NN matching proposed by Pan and Lyu [52]. Given a keypoint, its distance d_1 to the nearest neighbor and the distance d_2 to the next-nearest-neighbour are compared, if d_1/d_2 is less than a threshold (often fixed to 0.5 or 0.6), a pair of keypoints is obtained. To deal with multiple keypoint matching, Amerini et al. [3] proposed the generalized 2NN (g2NN) matching.

Some duplicated regions which are copied and pasted more than once still cannot be detected by the g2NN matching, because some matched keypoints cannot be detected. Therefore, the transitive matching is proposed to improve the matching relationship. We obtain a list of matched keypoints after the g2NN matching, as shown in Fig. 3, there are three duplicated regions, which are labeled as Ω_1, Ω_2 and Ω_3. The duplicated regions Ω_1 and Ω_3 are easy to be detected for there are enough matched keypoints between them. Neither the matched keypoints between Ω_1 and Ω_2, nor the matched keypoints between Ω_2 and Ω_3 are sufficient. So the duplicated region Ω_2 cannot be detected.

In fact, keypoints are sufficient, only their matching relationship is not detected. Now the transitive matching is used to obtain the new matching relationship. We obtain the matched keypoints (a_1, c_1) between Ω_1 and Ω_3, the matched keypoints (a_1, b_1) between Ω_1 and Ω_2, which are connected by a solid line in Fig. 3. Keypoints a_1 is matched with c_1, and the same keypoints is matched with b_1, then we draw a conclusion that keypoints b_1 is matched with

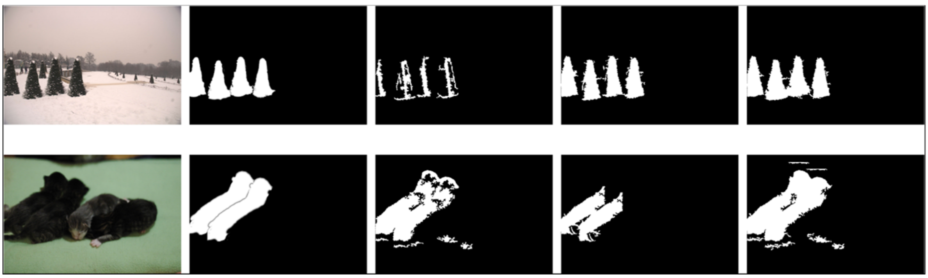


Fig. 2 Copy-move forgery detection results of the proposed scheme. Column 1: the forged images; column 2: the ground truth; column 3: the detection results only using SIFT; column 4: the detection results only using LIOP; column 5: the detection results using the proposed scheme(SIFT+LIOP)

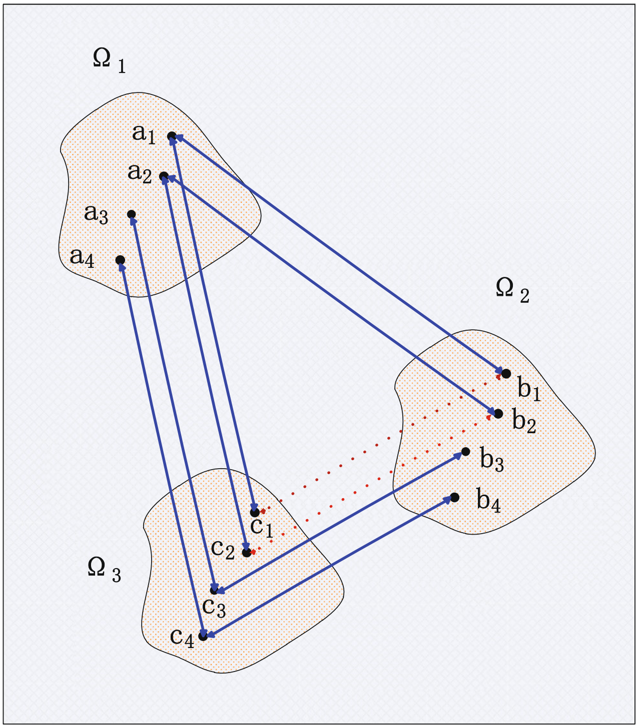


Fig. 3 The transitive matching. There are three duplicated regions, such as Ω_1, Ω_2 and Ω_3. The initial matching are connected by a solid line, for instance, (a_1, b_1) and (a_1, c_1). The transitive matching are connected by a dotted line, for instance, (b_1, c_1)

c_1, which is the transitive matching. Therefore, the transitive matching can be described as follows:

$$(K_1, K_2), (K_1, K_3) \Rightarrow (K_2, K_3) \tag{3}$$

where (K_1, K_2) indicates the matched keypoints K_1 and K_2. Then the new matched keypoints such as (b_1, c_1) and (b_2, c_2) is obtained, which are connected by a dotted line in Fig. 3. Thus, we can estimate the affine transformation between Ω_2 and Ω_3 after the transitive matching. The transitive matching try to detect a region which is copied and pasted more than once. The matching relation is improved by the transitive matching. To decrease mismatches, the transitive matching is limited to some regions which have matching relation. As shown in Fig. 3, there are matched keypoints between the three regions, which are connected by a solid line, then the transitive matching is carried out in the three regions.

2.3 Filtering false matches

In the section, the filtering algorithm to discard false matches is described. To improve the accuracy of affine transformations, those mismatched keypoints should be discarded after the transitive matching. Therefore, the Random Sample Consensus (RANSAC) algorithm [26] is adopted by Pan and Lyu [52]. The RANSAC algorithm returns with the affine transformations that lead to the largest number of matched keypoints and the smallest error.

Some mismatched keypoints can be discarded by RANSAC. But when there are lots of mismatched keypoints, the inaccurate affine transformation will be obtained by RANSAC. To overcome this issue, some false matches should be filtered, and the corresponding affine transformation will not be estimated. Considering the duplicated regions are usually meaningful regions, the input image is divided into non-overlapping image patches. It should be noted that the images are segmented by the Simple Linear Iterative Clustering (SLIC) algorithm [1]. Then N_m is adopted to represent the number of matched keypoints between the two image patches. If N_m is larger than a threshold, an affine transformation between the two image patches is estimated. Otherwise, those mismatched keypoints will be discarded. Thus some false matches can be discarded by our filtering algorithm.

2.4 Estimation of affine transformation

After the matched keypoints and the image patches are obtained, an affine transformation is estimated between the two image patches, one denotes as the source region and the other denotes as the forged region, if there are more than three matched keypoint between the two image patches. Two matched keypoints $\hat{x}_i = (x_i, y_i, 1)^T$ and $\hat{x}_i' = (x_i', y_i', 1)^T$ are from the source region and the forged region, respectively. Formally, their transformation can be expressed in matrix form as:

$$\hat{x}_i' = H\hat{x}_i = \begin{pmatrix} h_{11} & h_{12} & t_x \\ h_{21} & h_{22} & t_y \\ 0 & 0 & 1 \end{pmatrix} \hat{x}_i \tag{4}$$

where t_x and t_y are denoted as the translation factors, while h_{11}, h_{12}, h_{21} and h_{22} are denoted as rotation and scaling directions deformation. An affine transformation has six degrees of freedom, corresponding to the six matrix elements, then the transformation can be computed from three pairs of matched keypoints that are not collinear. Using RANSAC, the transformation matrix which returns the the largest number matched keypoints is obtained. Meanwhile, their total error of the affine transformation is minimized. Thus, an affine transformation between the two image patches is estimated. Then the duplicated regions are located according to the affine transformation [52].

3 Experiments and discussions

3.1 Dataset and error measures

To evaluate the efficiency of the proposed scheme, the Image Manipulation Dataset (IMD) [15] is adopted as the image dataset. The average size of an image is about 3000×2300 pixels. There are 1488 images on IMD. The details of the utilized image dataset are shown in Table 1.

Table 1 Setting of the attacks on IMD

Attacks	Criteria	Parameters
Scaling	Ratio	0.91:0.02:1.09
Rotation	Angle	2°:2°:10°
AWGN	Stand Deviation	0.02:0.02:0.1
JPEG	Quality Factor	20:10:100

In fact, the forgery is more difficult to be detected when the duplicated regions are small. Many images on the Internet are usually small, they are not as big as the images on IMD. Therefore, all the images on IMD are resized, just as Li et al. [37] did. The maximum of the width and the height of the images are set to 800 pixels. The proposed scheme is rather challenging for the duplicated regions are difficult to be detected after the images are resized.

It should be noted that the images on IMD are segmented by the SLIC algorithm [1], which is implemented by vlFeat library [60], where all the images on IMD are empirically divided into 100 image patches.

To assess the proposed scheme, we should test the detection error at two different levels, namely the image level and the pixel level. The detection error are measured by the *recall*, the *precision*, and the F_1 score [15], which are calculated as follows:

$$precision = \frac{|\{Forged\ pixels\} \bigcap \{Detected\ pixels\}|}{|\{Detected\ pixels\}|} \tag{5}$$

$$recall = \frac{|\{Forged\ pixels\} \bigcap \{Detected\ pixels\}|}{|\{Forged\ pixels\}|} \tag{6}$$

$$F_1 = \frac{2 * precision * recall}{precision + recall} \tag{7}$$

3.2 Comparisons with other relevant methods

In the section, the proposed scheme is compared with several state-of-the-art existing schemes, for instance, SIFT [3, 52], SURF [57], JLinkage [4] and Zernike [56]. The results of SIFT, SURF and Zernike are different with Christlein et al. [15] because of the image resizing. The process of resizing will make the duplicated regions smaller than before. Therefore, it will difficult to be detected for all the CMFD schemes. The proposed scheme combines both LIOP and SIFT. Some detection results of the proposed scheme in comparison with only SIFT or LIOP are shown in Fig. 2. Obviously, the most duplicated regions can be detected by the the proposed scheme.

3.2.1 Detection results under plain copy-move

In this section, we evaluate the proposed scheme under ideal conditions. There are 48 original images and 48 forgery images, in which a one-to-one copy-move is implemented. The experimental results under plain copy-move at the image level and the pixel level are shown in Tables 2 and 3, respectively. It should be noted that all the images on IMD are resized and the experimental results are different with Christlein et al. [15]. From Tables 2 and 3, it can be observed easily that the *recall* of the proposed scheme is the best among all the test schemes. The *precision* of the proposed scheme is better than that of SIFT, SURF

Table 2 Detection results for plain copy-move at the image level

Methods	Recall (%)	Precision (%)	F_1 (%)
SIFT [3, 52]	47.92	74.19	58.23
SURF [57]	43.75	72.41	54.55
JLinkage [4]	62.50	78.95	69.77
Zernike [56]	79.17	88.37	83.52
Proposed	93.75	81.82	87.38

Table 3 Detection results for plain copy-move at the pixel level

Methods	Recall (%)	Precision (%)	F_1 (%)
SIFT [3, 52]	37.93	36.79	37.35
SURF [57]	25.81	31.44	28.35
JLinkage [4]	47.47	48.12	47.79
Zernike [56]	53.92	87.37	66.68
Proposed	75.41	73.44	74.42

and JLinkage, all of which are keypoint-based schemes. Meanwhile, the F_1 score of the proposed scheme is much better than that of the existing state-of-the-art schemes. As a comprehensive evaluation, the F_1 score combines both the $recall$ and the $precision$ into a single value. Therefore, the proposed scheme is the best among the existing state-of-the-art schemes.

3.2.2 Detection results under other attackers

This section presents the comparison of the proposed method with other schemes under various attacks. The proposed scheme is evaluated by the $recall$, the $precision$ and the F_1

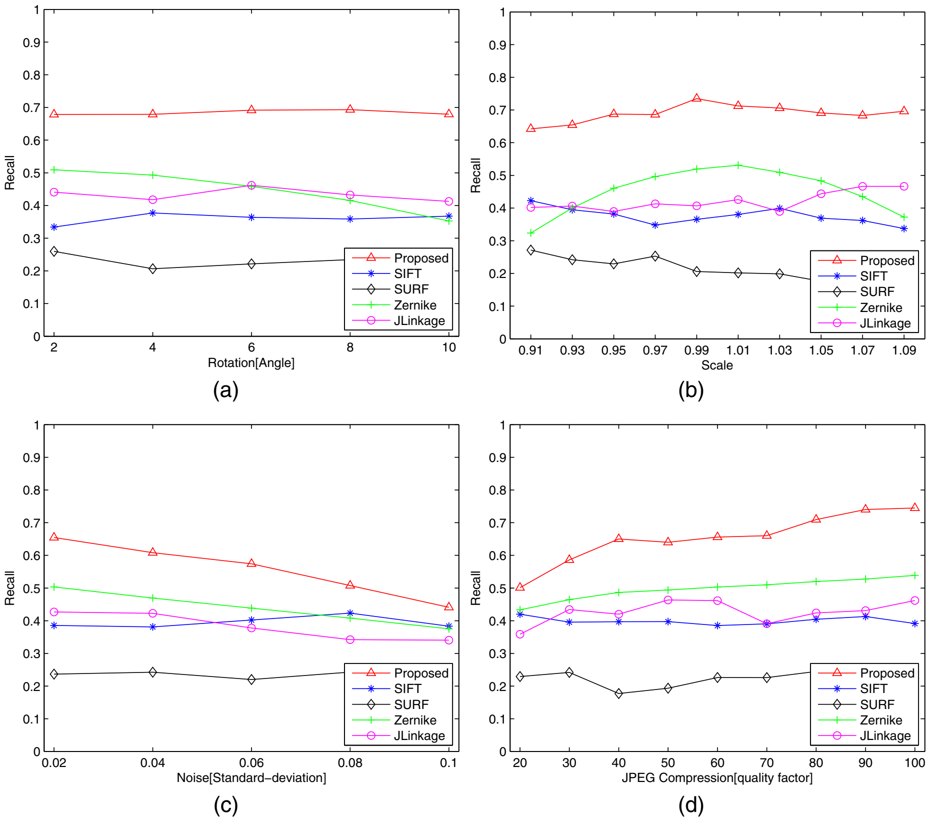


Fig. 4 *Recall* results at the pixel level. **a** Rotation, **b** Scale, **c** Adding noise, **d** JPEG compression

at the pixel level. It should be noted that the results of SIFT, SURF and Zernike are different with Christlein et al. [15] because of the image resizing. In the experiments, all the images are resized to no more than 800 pixels, just as Li et al. [37] did.

Figure 4 shows the *recall* results of the proposed scheme compared with the test schemes. It can be observed easily that the *recall* of the proposed scheme is the best among all the test schemes, which means that more number of duplicated regions can be obtained by the proposed scheme.

Figure 5 shows the *precision* results of the proposed scheme compared with the test schemes. The *precision* results of the proposed scheme is better than that of SIFT, SURF and JLinkage, all of which are keypoint-based schemes. As a block-based scheme, the *precision* results of Zernike is the best among all the test schemes. Therefore, the *precision* results of the proposed scheme is the best among all the keypoint-based schemes.

Figure 6 shows the F_1 results of the proposed scheme compared with the test schemes. Obviously, the proposed scheme outperforms the prior arts in terms of F_1 criterion. The F_1 score combines both the *precision* and the *recall* into a single value, it is a comprehensive evaluation. Therefore, the proposed scheme is better than the existing state-of-the-art schemes under various attacks.

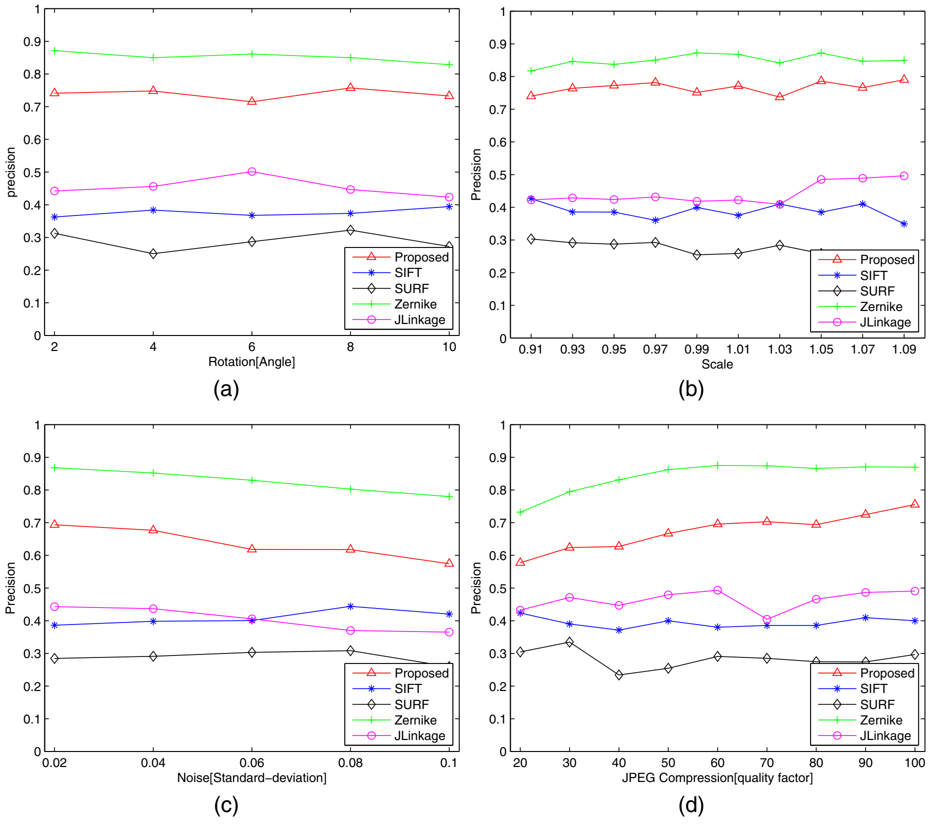


Fig. 5 *Precision* results at the pixel level. **a** Rotation, **b** Scale, **c** Adding noise, **d** JPEG compression

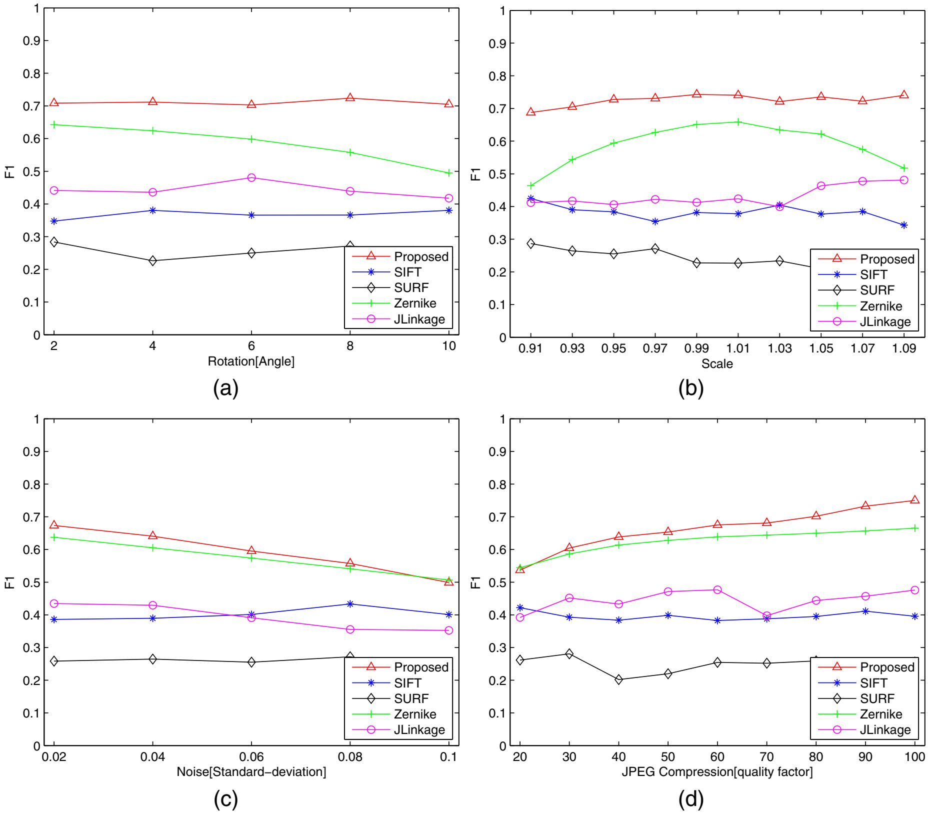


Fig. 6 F_1 results at the pixel level. **a** Rotation, **b** Scale, **c** Adding noise, **d** JPEG compression

4 Conclusions

In this paper, a novel copy-move forgery detection scheme using combined features and transitive matching is proposed. The specific contributions are summarized as follows. First, combined features which are composed of LIOP and SIFT are proposed. Thus, some duplicated regions with few keypoints can be detected. Second, transitive matching is used after the g2NN matching, then the matching relationship is improved. Third, to discard the false matches, a new filtering approach based on image segmentation is proposed. Experimental results show that the proposed scheme can achieve the best *recall* and the best F_1 score under challenging conditions.

Acknowledgments This work is supported by the National Natural Science Foundation of China (No. U1736118), the Natural Science Foundation of Guangdong (No. 2016A030313350), the Special Funds for Science and Technology Development of Guangdong (No. 2016KZ010103), the Key Project of Scientific Research Plan of Guangzhou (No. 201804020068), the Fundamental Research Funds for the Central Universities (No. 16lgjc83 and No. 17lgjc45), the Science and Technology Planning Project of Guangdong Province (Grant No.2017A040405051).

References

1. Achanta R, Shaji A, Smith K, Lucchi A, Fua P, Süsstrunk S. (2012) Slic superpixels compared to state-of-the-art superpixel methods. IEEE Trans Pattern Anal Mach Intell 34(11):2274–2282
2. Alcantarilla PF, Bartoli A, Davison AJ (2012) Kaze features. In: European conference on computer vision(ECCV), Florence, Italy, pp 214–227
3. Amerini I, Ballan L, Caldelli R, Bimbo AD, Serra G (2011) A SIFT-based forensic method for copy-move attack detection and transformation recovery. IEEE Trans Inf Forensic Secur 6(3):1099–1110
4. Amerini I, Ballan L, Caldelli R, Bimbo AD, Tongo LD, Serra G (2013) Copy-move forgery detection and localization by means of robust clustering with J-Linkage. Signal Process Image Commun 28(6):659–669
5. Bashar M, Noda K, Ohnishi N, Mori K (2010) Exploring duplicated regions in natural images. IEEE Trans Image Process PP(99):1–1
6. Bay H, Ess A, Tuytelaars T, Gool LV (2008) SURF: speeded up robust features. Comput Vis Image Underst 110(3):346–359
7. Bedi G, Venayagamoorthy GK, Singh R, Brooks R, Wang KC (2018) Review of internet of things (iot) in electric power and energy systems. IEEE Int Things J PP(99):1–1
8. Bravo-Solorio S, Nandi AK (2011) Exposing duplicated regions affected by reflection, rotation and scaling. In: IEEE International conference on acoustics, speech and signal processing(ICASSP), Prague, Czech Republic, pp 1880–1883
9. Chen J, Lu W, Fang Y, Liu X, Yeung Y, Yingjie X (2018) Binary image steganalysis based on local texture pattern. J Vis Commun Image Represent 55:149–156
10. Chen J, Lu W, Yeung Y, Xue Y, Liu X, Lin C, Zhang Y (2018) Binary image steganalysis based on distortion level co-occurrence matrix. Comput Mater Continua 55(2):201–211
11. Chen L, Lu W, Ni J, Sun W, Huang J (2013) Region duplication detection based on harris corner points and step sector statistics. J Vis Commun Image Represent 24(3):244–254
12. Chen X, Weng J, Lu W, Xu J (2018) Multi-gait recognition based on attribute discovery. IEEE Trans Pattern Anal Mach Intell PP(99):1–1
13. Chen X, Weng J, Lu W, Xu J, Weng J (2017) Deep manifold learning combined with convolutional neural networks for action recognition. IEEE Trans Neural Netw Learn Syst PP(99):1–15
14. Christlein V, Riess C, Angelopoulou E (2010) On rotation invariance in copy-move forgery detection. In: EEE International workshop on information forensics and security (WIFS), Seattle, WA, USA, pp 1–6
15. Christlein V, Riess C, Jordan J, Riess C (2012) Angelopoulou, e.: an evaluation of popular copy-move forgery detection approaches. IEEE Trans Inf Forensic Secur 7(6):1841–1854
16. Cozzolino D, Poggi G, Verdoliva L (2015) Efficient dense-field copy-move forgery detection. IEEE Trans Inf Forensic Secur 10(11):2284–2297
17. Fang W, Li Y, Zhang H, Xiong N, Lai J, Vasilakos AV (2014) On the throughput-energy tradeoff for data transmission between cloud and mobile devices. Inf Sci 283(283):79–93
18. Fang Y, Fang Z, Yuan F, Yang Y, Yang S, Xiong NN (2017) Optimized multioperator image retargeting based on perceptual similarity measure. IEEE Trans Syst Man Cybern Syst 47(11):2956–2966
19. Feng B, Lu W, Sun W (2014) Secure binary image steganography based on minimizing the distortion on the texture. IEEE Trans Inf Forensic Secur 10(2):243–255
20. Feng B, Lu W, Sun W (2015) Binary image steganalysis based on pixel mesh markov transition matrix. J Vis Commun Image Represent 26:284–295
21. Feng B, Lu W, Sun W (2015) Novel steganographic method based on generalized k-distance n-dimensional pixel matching. Multimed Tools Appl 74(21):9623–9646
22. Feng B, Lu W, Sun W, Huang J, Shi YQ (2016) Robust image watermarking based on tucker decomposition and adaptive-lattice quantization index modulation. Signal Process Image Commun 41(C):1–14
23. Feng B, Weng J, Lu W, Pei B (2017) Steganalysis of content-adaptive binary image data hiding. J Vis Commun Image Represent 46:119–127. https://www.sciencedirect.com/science/article/pii/S1047320317300081
24. Feng B, Weng J, Lu W, Pei B (2017) Multiple watermarking using multilevel quantization index modulation. In: International workshop on digital watermarking, Beijing, China, pp 312–326
25. Ferreira A, Felipussi SC, Alfaro C, Fonseca P, Vargasmunoz JE, Dos Santos JA, Rocha A (2016) Behavior knowledge space-based fusion for copy-move forgery detection. IEEE Trans Image Process 25(10):4729–4742
26. Fischler MA, Bolles RC (1981) Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography. Commun ACM 24(6):381–395

27. Fridrich J, Soukal D, Lukáš J (2003) Detection of copy-move forgery in digital images. In: Proceeding of digital forensic research workshop, Cleveland, OH, USA, pp 19–23
28. Gao L, Yu F, Chen Q, Xiong N (2016) Consistency maintenance of do and undo/redo operations in real-time collaborative bitmap editing systems. Clust Comput 19(1):255–267
29. Ghorbani M, Firouzmand M, Faraahi A (2011) DWT-DCT (QCD) based copy-move image forgery detection. In: International conference on systems, signals and image processing, pp 1–4. Sarajevo
30. Gui J, Hui L, Xiong N (2017) A game-based localized multi-objective topology control scheme in heterogeneous wireless networks. IEEE Access 5(99):2396–2416
31. Harris CG, Stephens MJ (1988) A combined corner and edge detector. In: Alvey vision conference, pp 147–151
32. Hu C, Xu Z, Liu Y, Mei L, Chen L, Luo X (2014) Semantic link network-based model for organizing multimedia big data. IEEE Trans Emerg Topics Comput 2(3):376–387
33. Huang H, Guo W, Zhang Y (2008) Detection of copy-move forgery in digital images using SIFT algorithm. In: IEEE Pacific-Asia workshop on computational intelligence and industrial application, pp 272–276
34. Huang Y, Lu W, Sun W, Long D (2011) Improved DCT-based detection of copy-move forgery in images. Forensic Sci Int 206(1-3):178–184
35. Jin G, Wan X (2017) An improved method for SIFT-based copy-move forgery detection using non-maximum value suppression and optimized J-Linkage. Signal Process Image Commun 57:113–125
36. Lee JC, Chang CP, Chen WK (2015) Detection of copy-move image forgery using histogram of orientated gradients. Inf Sci 321(C):250–262
37. Li J, Li X, Yang B, Sun X (2015) Segmentation-based image copy-move forgery detection scheme. IEEE Trans Inf Forensic Secur 10(3):507–518
38. Li J, Lu W (2016) Blind image motion deblurring with L0-regularized priors. J Vis Commun Image Represent 40:14–23
39. Li J, Lu W, Weng J, Mao Y, Li G (2018) Double jpeg compression detection based on block statistics. Multimed Tools Appl 77(24):1–16
40. Li J, Yang F, Lu W, Sun W (2016) Keypoint-based copy-move detection scheme by adopting mscrs and improved feature matching. Multimed Tools Appl 76(20):1–15
41. Li Y (2013) Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching. Forensic Sci Int 224(1-3):59
42. Lin B, Guo W, Xiong N, Chen G, Vasilakos AV, Zhang H (2016) A pretreatment workflow scheduling approach for big data applications in multicloud environments. IEEE Trans Netw Serv Manag 13(3):581–594
43. Lin C, Lu W, Sun W, Zeng J, Xu T, Lai JH (2017) Region duplication detection based on image segmentation and keypoint contexts. Multimed Tools Appl 77(11):1–18
44. Liu G, Wang J, Lian S, Wang Z (2011) A passive image authentication scheme for detecting region-duplication forgery with rotation. J Netw Comput Appl 34(5):1557–1565
45. Lowe DG (2004) Distinctive image features from scale-invariant keypoints. Int J Comput Vis 60(2):91–110
46. Lu X, Tu L, Zhou X, Xiong N, Sun L (2017) Vimedianet: an emulation system for interactive multimedia based telepresence services. J Supercomput 73(8):3562–3578
47. Lu Z, Lin YR, Huang X, Xiong N, Fang Z (2017) Visual topic discovering, tracking and summarization from social media streams. Multimed Tools Appl 76(8):1–25
48. Ma Y, Luo X, Li X, Bao Z, Zhang Y (2018) Selection of rich model steganalysis features based on decision rough set α-positive region reduction. IEEE Trans Circ Syst Video Technol PP(99): 1–1
49. Mahdian B, Saic S (2007) Detection of copy-move forgery using a method based on blur moment invariants. Forensic Sci Int 171:180–189
50. Melro LS, Jensen LR (2017) Influence of functionalization on the structural and mechanical properties of graphene. Comput Mater Continua 53(2):111–131
51. Nelson B, Phillips A, Steuart C (2015) Guide to computer forensics and investigations delmar learning
52. Pan X, Lyu S (2010) Region duplication detection using image feature matching. IEEE Trans Inf Forensic Secur 5(4):857–867
53. Popescu AC, Farid H (2004) Exposing digital forgeries by detecting duplicated image regions. Tech. Rep. TR2004-515, Department of Computer Science Dartmouth College
54. Pun CM, Yuan XC, Bi XL (2015) Image forgery detection using adaptive over-segmentation and feature points matching. IEEE Trans Inf Forensic Secur 10(8):1705–1716

55. Ryu SJ, Kirchner M, Lee MJ, Lee HK (2013) Rotation invariant localization of duplicated image regions based on Zernike moments. IEEE Trans Inf Forensic Secur 8(8):1355–1370
56. Ryu SJ, Lee MJ, Lee HK (2010) Detection of copy-rotate-move forgery using Zernike moments. In: IEEE International workshop on information hiding(IH). Springer, Berlin, pp 51–65
57. Shivakumar BL, Baboo S (2011) Detection of region duplication forgery in digital images using SURF. Int J Comput Sci Issues 8(4):199–205
58. Shu L, Fang Y, Fang Z, Yang Y, Fei F, Xiong N (2016) A novel objective quality assessment for super-resolution images. Int J Sig Process 9(5):297–308
59. Silva E, Carvalho T, Ferreira A, Rocha A (2015) Going deeper into copy-move forgery detection: exploring image telltales via multi-scale analysis and voting processes. J Vis Commun Image Represent 29(C):16–32
60. Vedaldi A, Fulkerson B (2010) Vlfeat: an open and portable library of computer vision algorithms. In: International conference on multimedea, Firenze, Italy, pp 1469–1472
61. Wang J, Li T, Shi YQ, Lian S, Ye J (2016) Forensics feature analysis in quaternion wavelet domain for distinguishing photographic images and computer graphics. Multimed Tools Appl 76(22):1–17
62. Wang Y, Chen K, Yu J, Xiong N, Leung H, Zhou H, Zhu L (2017) Dynamic propagation characteristics estimation and tracking based on an em-ekf algorithm in time-variant mimo channel. Inf Sci 408(C):70–83
63. Wang Z, Fan B, Wu F (2011) Local intensity order pattern for feature description. In: IEEE International conference on computer vision (ICCV), pp 603–610
64. Warif NBA, Wahab AWA, Idris MYI, Salleh R, Othman F (2017) SIFT-symmetry: a robust detection method for copy-move forgery with reflection attack. J Vis Commun Image Represent 46:219–232
65. Wu P, Xiao F, Sha C, Huang H, Wang R, Xiong N (2017) Node scheduling strategies for achieving full-view area coverage in camera sensor networks. Sensors 17(6):1303
66. Xia Z, Wang X, Sun X, Liu Q, Xiong N (2016) Steganalysis of lsb matching using differences between nonadjacent pixels. Multimed Tools Appl 75(4):1947–1962
67. Xia Z, Xiong NN, Vasilakos AV, Sun X (2017) Epcbir: an efficient and privacy-preserving content-based image retrieval scheme in cloud computing. Inf Sci 387:195–204
68. Xiong N, Jia X, Yang LT, Vasilakos AV, Li Y, Pan Y (2010) A distributed efficient flow control scheme for multirate multicast networks. IEEE Trans Parallel Distrib Syst 21(9):1254–1266
69. Xiong N, Liu RW, Liang M, Wu D, Liu Z, Wu H (2017) Effective alternating direction optimization methods for sparsity-constrained blind image deblurring. Sensors 17(1):1–27
70. Xiong N, Vasilakos AV, Yang LT, Song L, Pan Y, Kannan R, Li Y (2009) Comparative analysis of quality of service and memory usage for adaptive failure detectors in healthcare systems. IEEE J Sel Areas Commun 27(4):495–509
71. Xiong N, Vasilakos AV, Yang LT, Wang CX, Kannan R, Chang CC, Pan Y (2009) A novel self-tuning feedback controller for active queue management supporting tcp flows. Inf Sci 180(11):2249–2263
72. Xu B, Wang J, Liu G, Dai Y (2010) Image copy-move forgery detection based on SURF. In: International conference on multimedia information networking and security (MINES), Nanjing, China, pp 889–892
73. Yang B, Sun X, Chen X, Zhang J, Li X (2013) An efficient forensic method for copy-move forgery detection based on dwt-fwht. Radioengineering 22(4):1098–1105
74. Yang F, Li J, Lu W, Weng J (2017) Copy-move forgery detection based on hybrid features. Eng Appl Artif Intell 59:73–83
75. Yang Y, Tong S, Huang S, Lin P (2014) Dual-tree complex wavelet transform and image block residual-based multi-focus image fusion in visual sensor networks. Sensors 14(12):22,408–22,430
76. Yang Z, Ma L, Ma Q, Cui J, Nie Y, Dong H, An X (2017) Multiscale nonlinear thermo-mechanical coupling analysis of composite structures with quasi-periodic properties. Comput Mater Continua 53(3):219–248
77. Zhang C, Wu D, Liu RW, Xiong N (2015) Non-local regularized variational model for image deblurring under mixed gaussian-impulse noise. J Int Technol 16(7):1301–1319
78. Zhang F, Lu W, Liu H, Xue F (2018) Natural image deblurring based on l0-regularization and kernel shape optimization. Multimed Tools Appl 77(20):1–19
79. Zhang H, Liu RW, Wu D, Liu Y, Xiong NN (2016) Non-convex total generalized variation with spatially adaptive regularization parameters for edge-preserving image restoration. J Int Technol 17(7):1391–1403
80. Zhang Q, Lu W, Wang R, Li G (2018) Digital image splicing detection based on markov features in block dwt domain. Multimed Tools Appl 77(23):1–22

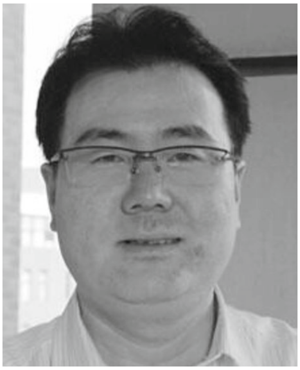
81. Zhang Q, Lu W, Weng J (2016) Joint image splicing detection in dct and contourlet transform domain. J Vis Commun Image Represent 40:449–458
82. Zhang Y, Qin C, Zhang W, Liu F, Luo X (2018) On the fault-tolerant performance for a class of robust image steganography. Sig Process 146:1–1
83. Zheng H, Guo W, Xiong N (2017) A kernel-based compressive sensing approach for mobile data gathering in wireless sensor network systems. IEEE Trans Syst Man Cybern Syst PP(99):1–13
84. Zhou P, Zhou Y, Wu D, Jin H (2016) Differentially private online learning for cloud-based video recommendation with multimedia big data in social networks. IEEE Trans Multimed 18(6):1217–1229
85. Zhou Y, Zhang D, Xiong N (2017) Post-cloud computing paradigms: a survey and comparison. Tsinghua Sci Technol 22(6):714–732

Cong Lin received the B.S. degree in computer science from Tsinghua University, Beijing, China in 2005, the M.S. degree in computer science from Sun Yat-sen University, Guangzhou, China in 2009. He is currently working toward the Ph.D. degree in computer science at the Sun Yat-sen University, Guangzhou, China. His research interests include multimedia forensics and security.

Wei Lu received the B.S. degree in Automation from Northeast University, China in 2002, the M.S. degree and the Ph.D. degree in Computer Science from Shanghai Jiao Tong University, China in 2005 and 2007 respectively. He was a research assistant at Hong Kong Polytechnic University from 2006 to 2007. He is currently an Associate Professor with the School of Data and Computer Science, Sun Yat-sen University, Guangzhou, China. His research interests include multimedia forensics and security, multimedia signal processing, image/video intelligent analysis.

Xinchao Huang received the B.S. degree from the Software College, Northeastern University, China in 2015. He is currently a Master Candidate in the School of Data and Computer Science, Sun Yat-sen University, Guangzhou, China. His research interests include multimedia forensics and security.

Ke Liu received the B.S. degree from the school of Communication engineering, Ludong University, China in 2017. She is currently a master Candidate in the school of Information and Communication Engineering, Sun Yat-sen University, Guangzhou, China. Her research interests include multimedia forensics and security.



Wei Sun received the Ph.D. degree in computer science from Sun Yat-sen University, Guangzhou, China in 2004, where he is currently a Professor with the School of Electronics and Information Engineering. His current research interests include information security and computer graphics.

Hanhui Lin received the B.S. degree from Guangdong University of Finance and Economics, Guangzhou, China; the M.S. degree from South China University of Technology, Guangzhou, China, in 2004 and 2008 respectively, all in software engineering. He is currently a senior engineer with the Center for Faculty Development and Educational Technology, Guangdong University of Finance and Economics. His current research interests include information security and educational technology.

Zhiyuan Tan is a Lecturer in Cybersecurity at the School of Computing, Edinburgh Napier University (ENU), United Kingdom. He is a Member of IEEE and EAI. His research interests include cybersecurity, machine learning, pattern recognition, data analytics, virtualisation and cyber-physical system.

Prior to joining ENU in 2016, Dr Tan held different research positions at three research-intensive universities, respectively. He was a Postdoctoral Researcher in Cybersecurity at the University of Twente (UT), the Netherlands from 2014 to 2016; a Research Associate at the University of Technology, Sydney (UTS), Australia in 2014; and a Senior Research Assistant at La Trobe University, Australia in 2013.

His research findings have been published in world-leading journals such as IEEE Transactions on Computers, IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Cloud Computing, Future Generation Computer Systems (FGCS), Computer Networks (CN). He has also played various chair roles in International workshops and conferences, such as SECSOC, SITN, EAI Future 5V and EAI BD:TA 2018. He serves on the editorial board of International Journal of Computer Sciences and its Applications. He is Associate Editor of IEEE Access and has organised Special Issues for Ad Hoc & Sensor Wireless Networks Journal, International Journal of Distributed Sensor Networks, Computers & Electrical Engineering, IEEE Access, etc.