Copy-move Forgery Detection Based on YIQ and ORB for Color Images

Zheng Jiming [1, 2, a], Hu Mengqi[1, b]

[1]*School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*
[2]*Key Lab of Intelligent Analysis and Decision on Complex Systems, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*
[a]*zhengjm@cqupt.edu.cn*, [b]*1431280070@qq.com*

Keywords: digital image forensics; copy-move detection; YIQ color space; mismatch elimination

Abstract: In order to solve the problem of the false matching in detecting copy-move forgeries, an improved method based on Oriented FAST and Rotated BRIEF (ORB) and YIQ color space is proposed. First, to detect the key points of the original image and extract ORB features. Secondly, for each key point, the YIQ color feature is extracted. Finally, the ORB feature descriptor and the YIQ color feature vector between every two different key points are matched to determine the copy-move regions. The experimental results show that the proposed algorithm can not only guarantee the high efficiency of the detection algorithm, but also can effectively reduce the false matching rate comparing with the ORB algorithm. What's more, the proposed algorithm has better robustness even when an image is distorted by Gaussian blur, white noise and JPEG compression.

1. Introduction

With the increasing popularity of digital image acquisition devices, digital images become inseparable parts of human life. However, there are also a lot of powerful editing software like PhotoShop that make image tampering become easier. If these tampered images appear in news reports, academic research and court evidence, they will reduce people's trust in images and bring serious negative effects to the society.

There are various means of image tampering, copy-move forgery is the most common way of tampering. Copy-move forgery detection (CMFD) technique are traditionally categorized into two classes: block-based and keypoint-based methods [1]. In 2003, Fridrich et al. first proposed the block-based matching method and proposed a CMFD algorithm based on Discrete Cosine Transform (DCT) [2]. However, the disadvantage is that the feature dimension of this algorithm is high. In 2004, Popescu and Farid used the Principal Component Analysis (PCA) to characterize the image blocks [3], which reduced the dimension of the feature descriptor. This algorithm is robust to noise-adding and

JPEG compression. In 2012, Muhammad et al. proposed a detection algorithm based on Dyadic Wavelet Transform (DyWT), combining LL1 channel and HH1 channel [4], which improved the accuracy of block-based CMFD algorithm. Block-based algorithm is difficult to determine the block size, and has high computational complexity, in addition, it has weak robustness to rotation, scaling, noise, blur and other operations [5].

In 2008, Huang et al. proposed a keypoint-based CMFD algorithm--Scale-Invariant Feature Transform (SIFT) [6] to detect the tampered area, which can effectively deal with light, rotation and scale changes. In the same year, Shivakumar et al. proposed a tampering detection algorithm based on Speeded Up Robust Features (SURF) [7]. The performance of the SURF algorithm is similar to that of the SIFT algorithm, but the computational complexity is greatly reduced. Besides, in order to solve the high dimension feature descriptor and high matching time complexity of the SIFT and the SURF algorithm, In 2013, Ethan et al. proposed Oriented FAST and Rotated BRIEF(ORB) feature extraction algorithm[8]. ORB is a method based on high speed binary descriptor BRIEF, at the same time, this method also has invariance over rotation, and is robust to the noise.

Most of the current CMFD algorithms only use the gray information of the image, and significant color information is ignored. However, color plays an important role in identifying objects. To solve this problem, this paper proposes a CMFD algorithm based on ORB and YIQ color space. On the basis of the ORB algorithm, the color feature of the key points is extracted to increase the detecting accuracy for color images. Experiments show that the algorithm can eliminate the mismatch problem of ORB algorithm and improve the accuracy of identification.

The rest of this paper is organized as follows. Section 2, describes the general workflow. The propose algorithm is introduced in section 3 and section 4; section 5 illustrates the experimental results and gives the comparative analysis of the proposed algorithm with some classical detection methods. Finally, section 6 concludes the paper and discusses some possible future work.

2. Proposed Method

As discussed in section 1, a majority of existing work ignore the color information of images. Thus, this paper present a YIQ space-based strategy for CMFD, as shown in Fig.1.First extract the keypoints; next the ORB features of the image is extracted; then color invariant of every key-point is computed; Finally, the intersection of the matching keypoint pairs of the two sets is the result of CMFD detection.

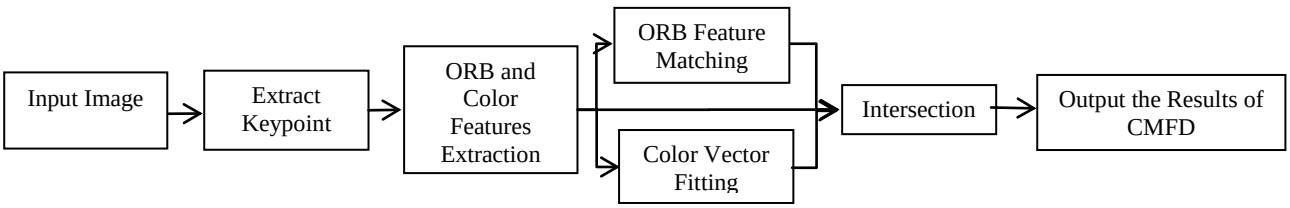

Fig.1 Framework of proposed method

3. Keypoint Extraction

For image $I(x, y)$, draw a circle with a radius of 3 pixels centered on the point (x, y). Take the points on the circumference as the surrounding points, if there are continuous 12 surrounding points, whose gray value is larger than that of the center point (x, y) plus the threshold value or less than the gray value of the center point (x, y) minus the threshold, then the circle pixel is regarded as the keypoint.

3.1 ORB Feature Extraction

After the feature points determined, first define the $p+q$ moments of a feature-centric image block m_{pq}, shown in Equation (1).

$$m_{pq} = \sum_{x,y} x^p y^q I(x,y) \tag{1}$$

The centroid position $C = (\frac{m_{10}}{m_{00}}, \frac{m_{01}}{m_{00}})$,and the direction of the keypoint is $\theta = \arctan \frac{m_{01}}{m_{10}}$. In the neighborhood of one keypoint, n pairs of point p_i, q_i $(i = 1,2,\cdots,n)$ are selected. Then compare the pixel values for each point pair. If $I(p_i) > I(q_i)$, then generate 1 for binary string, otherwise 0. All point pairs are compared to generate a binary string of length n. For any feature set of n binary tests at location (x_i, y_i), define the $2 \times n$ matrix $S = \begin{pmatrix} x_1,\ldots,x_n \\ y_1,\ldots,y_n \end{pmatrix}$, using the patch orientation θ and the corresponding rotation matrix $R_\theta = \begin{pmatrix} \cos\theta, -\sin\theta \\ \sin\theta, \cos\theta \end{pmatrix}$ to construct S_θ, $S_\theta = R_\theta S$,. Then at this point from the order of the new binary test, we define the ORB descriptor as Equation (2).

$$g_n(p,\theta) := f_n(p) \mid (x_i, y_i) \in S_\theta \tag{2}$$

The BRIEF descriptor thus obtained has rotational invariance. Finally the ORB feature set $F^{(1)}$ is formed, shown in Equation (3).

$$F^{(1)} = \left\{ f_1^{(1)}, f_2^{(1)}, \ldots, f_n^{(1)} \right\} \tag{3}$$

3.2 Color Feature Extraction

Considering the real-time character of the feature point detection algorithm, this paper uses color components extracted from the color space as color features. Compared with other color space, YIQ color space not only considers the color information of image, but also the relationship between YIQ color space and RGB color space is linear transformation, which can be effectively used in color image processing[14]. The corresponding relationship between RGB and YIQ is shown in Equation (4).

$$\begin{bmatrix} Y \\ I \\ Q \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0.596 & -0.274 & -0.322 \\ 0.211 & -0.523 & 0.312 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix}, \quad \begin{cases} R,G,B,Y \in [0,1] \\ I \in [-0.5957, 0.5957] \\ Q \in [-0.5226, 0.5226] \end{cases} \tag{4}$$

In Equation (4), Y refers to the brightness of the color, I refers to the color, Q refers to saturation. According to the coordinates of the feature points, the color space is transformed from the original image by Equation (4), and its YIQ color features are extracted. According to the extracted color features, a set of color feature vectors $F^{(2)}$ is obtained, shown in Equation (5).

$$F^{(2)} = \left\{ f_1^{(2)}, f_2^{(2)}, \ldots, f_n^{(2)} \right\} \tag{5}$$

4. Keypoint Matching

In the feature matching phase, we search for feature descriptions within $F^{(1)}$ and $F^{(2)}$,

respectively. Take $F^{(1)}$ as an example. For each feature pair $f_i^{(1)}$, $f_j^{(1)}$ (i ,j= 1, 2, ..., n) , calculate their Hamming distance $d^{(1)}$. $f_i^{(1)}$, $f_j^{(1)}$ is a qualified match if $d^{(1)} \geq T_{h1}$ (T_{h1} represent the threshold that predefined), then all the matched pairs are preserved while others are discarded. An identical procedure is then applied to the feature set $F^{(2)}$, calculate the vector product $d^{(2)}$, only when $d^{(2)} \geq T_{h2}$ (T_{h2} represent the threshold that predefined) $f_i^{(2)}$, $f_j^{(2)}$ can be regarded as the correct match. A keypoint pair that meets the appeal conditions at the same time will be counted as a pair of effective match. Finally, connect all the matching feature points, and the two areas that are connected to the line are judged to be the areas of copy-move forgery.

5. Experimental Results and Analysis

In this section, a series of simulation experiments are conducted to evaluate the effectiveness and robustness of the proposed CMFD approach. All experiments are launched on a desktop computer, running Python 2.7. In this paper, we have used 200 original and tampered images from two public available datasets CASIA and FAU for evaluating and comparing the proposed CMFD approach with the ones from Reference [6,7,8]. Fig.2 represents the CMFD results of proposed method and other CMFD different with different attacks.

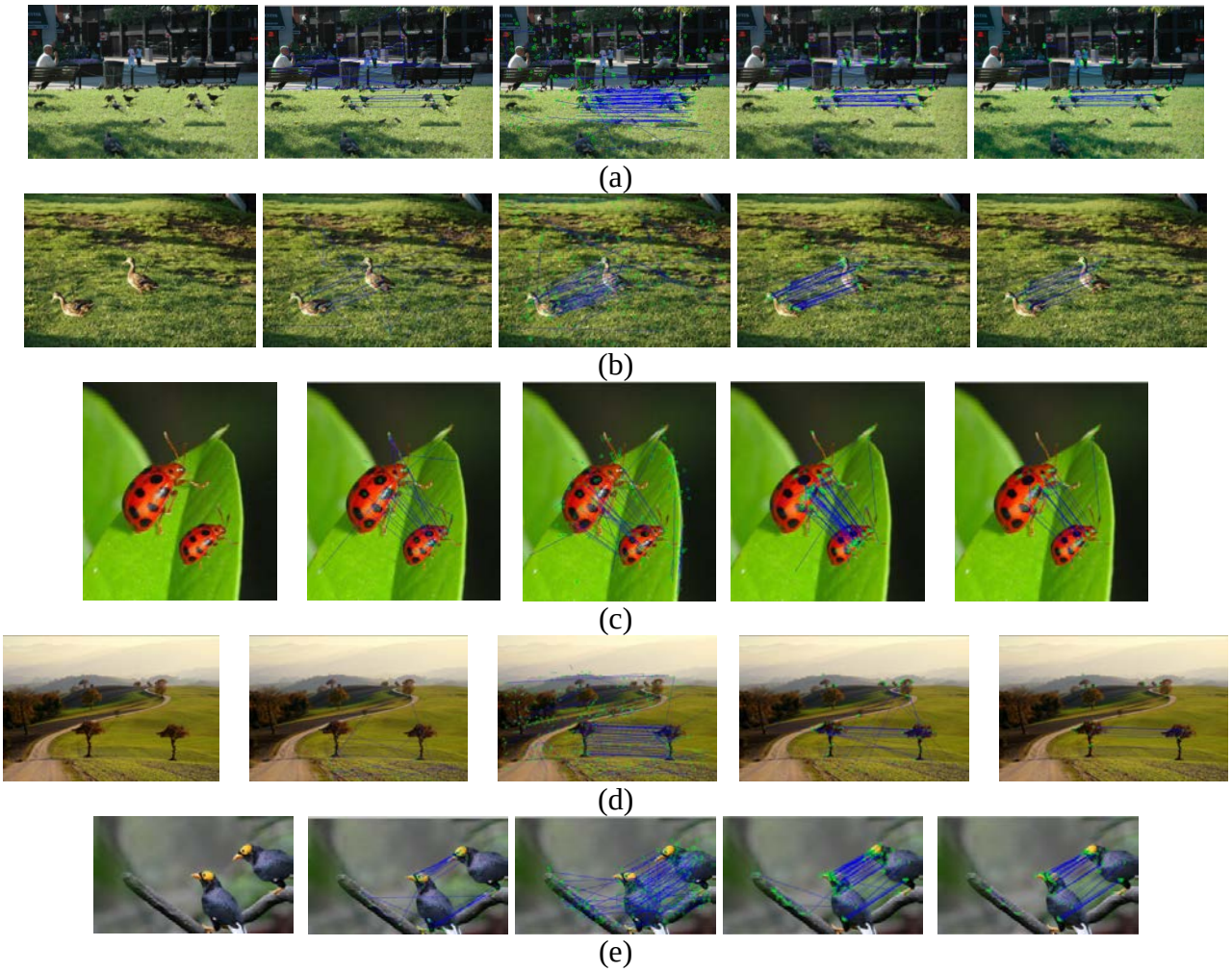

Fig.2 CMFD results of different methods with different attack. From left: copy-move forgery image, CMFD results of SIFT,SURF,ORB and proposed methods :(a) plain copy-move, (b) rotation, (c)scaling, (d)addictive White Gaussian noise, (e)JPEG compression

Suppose the total number of matched feature points is P, the number of correct matching feature points is R and the number of false matching feature points is $P-R$, the false detection rate η is shown in Equation (6).

$$\eta = \frac{P-R}{P} \tag{6}$$

Table 1 Contrast Experiment Results

Algorithm	***Average Detection Time(s)***	***Average False Detection Rate***
SIFT	0.41	0.15
SURF	0.39	0.27
ORB	0.28	0.19
Proposed	0.32	0.11

6. Conclusions

In this paper, an efficient forensic method based on the YIQ and ORB for detecting copy-move forgery in color images was proposed. We have evaluated the proposed CMFD approach on two public available datasets CASIA and FAU, and extensive experimental results have proved that the proposed approach can detect and localize color image copy-moves with good accuracy even in adverse conditions. What's more, the time complexity of the algorithm proposed is not significantly increased on the basis of the ORB algorithm. In our future work, we will focus on improve the robustness of this algorithm to copy-move forgery in smooth regions.

References

[1] Asghar K, Habib Z, Hussain M. Copy-move and splicing image forgery detection and localization techniques: a review [J]. Australian Journal of Forensic Sciences, 2016, 49(3):281-307.

[2] Fridrich J, Soukal D, Lukas J. Detection of copy-move forgery in digital images [J]. Proceedings of Digital Forensic Research Workshop, 2003.

[3] Popescu A C, Farid H. Exposing digital forgeries by detecting duplicated image regions [J]. Comput.sci.dartmouth College Private Ivy League Res.univ, 2004, 646.

[4] Muhammad G, Hussain M, Bebis G. Passive copy move image forgery detection using undecimated dyadic wavelet transform [J]. Digital Investigation, 2012, 9(1):49-57.

[5] Zandi M, Mahmoudi-Aznaveh A, Talebpour A. Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector [J]. IEEE Transactions on Information Forensics & Security, 2016, 11(11):2499-2512.

[6] Huang H, Guo W, Zhang Y. Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm[C]// Computational Intelligence and Industrial Application, 2008. PACIIA '08. Pacific-Asia Workshop on. IEEE, 2009:272-276.

[7] Bay H, Tuytelaars T, Gool L V. SURF: Speeded Up Robust Features[C]. Computer Vision & Image Understanding, 2006:110(3):404-417.

[8] Rublee E, Rabaud V, Konolige K, et al. ORB: An efficient alternative to SIFT or SURF[C]// IEEE International Conference on Computer Vision. IEEE, 2012:2564-2571.

[9] Shen X J, Ye Z, Ying-Da L, et al. Coloured image copy-move forgery detection based on SIFT and HSI[J]. Journal of Jilin University, 2014, 44(1):171-176.

[10] Zhou H, Shen Y, Zhu X, et al. Digital image modification detection using color information and its histograms [J]. Forensic Science International, 2016, 266:379-388.

[11] Vinayak V, Jindal S. CBIR System using Color Moment and Color Auto-Correlogram with Block Truncation Coding [J]. International Journal of Computer Applications, 2017, 161(9):1-7.

[12] Malviya A V, Ladhake S A. Pixel Based Image Forensic Technique for Copy-move Forgery Detection Using Auto Color Correlogram ☆[J]. Procedia Computer Science, 2016, 79:383-390.

[13] Gong Jiachang, Guo Jichang. Image Copy-Move Forgeries Detection Using CSURF [J]. Journal of Tianjin University, 2014, 47(9):759-764.
[14] Lumb M, Sethi P. Texture Feature Extraction of RGB, HSV, YIQ and Dithered Images using GLCM, Wavelet Decomposition Techniques [J]. International Journal of Computer Applications, 2013, 73(10):41-49.