Image Forgery Detection Algorithm  
Based on Non-Sampling Wavelet Transform  
and Zernike Moments  

Xiao Jinke

1Public Security Fourteen Bureau Zhuhai City Guangdong Province, Zhuhai Guangdong, 519000

Abstract. The image forgery detection technology based on non sampling wavelet transform coupling with Zernike moments is proposed in this article. Specifically, LL and HH sub-bands are obtained through non sampling wavelet transform to calculate the similarity and the diversity of the image blocks, and then LL similarity and HH diversity are combined for dual judgment. Meanwhile, Zernike moments are introduced therein to construct distance matrix for image feature matching. Finally, the images are selected from CASIA TIDEV1.0 database for algorithm evaluation, and the experimental result shows: the algorithm proposed in the article has the features of good noise immunity, good compression resistance, high algorithm accuracy, low false negative rate and low false positive rate.

Keywords: Non Sampling Wavelet Transform; Zernike Moments; Copy & Paste; Image Forgery Detection; Robustness

1 Introduction

Therefore, an image copying & moving forgery detection algorithm based on non-sampling wavelet transform (UWT) coupling with Zernike moments is proposed in this article. Specifically, Zernike moments are introduced to construct distance matrix for image feature matching and image forgery detection. Finally, the detection performance of the forgery location technology proposed in this article is also verified.

2 Mathematical Model for Copying & moving Forgery

Image copying & moving forgery as a common forgery measure aims at copying a certain part of the original image and then pasting it to the other non-overlapped zones of the same image in order to conceal or add new contents. The forgery model thereof is simplified as follows [7]:

ISSN: 2287-1233 ASTL  
Copyright © 2016 SERSC
\[ I'(x, y) = T[I(x, y)] + n(x, y) \]

In the above formula, \( I(x, y) \) refers to the original image, \( I'(x, y) \) refers to the forged image, \( T \) refers to the operating function for \( I(x, y) \), and \( n(x, y) \) refers to random noise. The implementation process of the image copying & moving forgery is as shown in Fig.1.

Fig. 1. Image Copying & Moving Process

\( f(x, y) \) is the copied zone of \( I(x, y) \), \( f'(x, y) \) is the pasted zone of \( I'(x, y) \), \( f(x, y) \) and \( I(x, y) \) shall meet the connectivity principle and keep a certain distance, without any overlap. \( \Delta x \) and \( \Delta y \) are the movement displacements of the copied zone and the pasted zone, and such displacements are usually not smaller than the forgery zone. The copied zone is sourced from the same image, so the features thereof are much similar to those of the original image, but the copied zone is usually decorated through noise, fuzziness, JPEG lossy compression, etc. during the forgery process to cover the forgery marks, thus weakening the similarity of the copied zone and the pasted zone and bringing significant difficulty to the detection.

The image copying & pasting forgery detection is mainly used to judge whether the image has the sub-blocks with large same or similar area, and mainly includes the following steps: 1. Image preprocessing; 2. Image block division; 3. Image block characteristic quantity extraction; 4. Image block matching; 5. Identification and location based on preset rules.

3 Experimental Result

In order to verify the effectiveness and the superiority of the algorithm proposed in this article, two comparison groups are set: the algorithms proposed in literature [4] and literature [5] are respectively recorded as Algorithm A and Algorithm B. MATLAB8.0 is adopted to test the performance of the algorithm proposed in this article. Additionally, the simulation conditions are as follows: \( DELL \) i5, 2.3GHz, four-core CPU, 500GB hard disk, 4GB memory, Windows7 system. The image with the size of 384×256 is selected from CASIA TID EV1.0 database [11].
In order to evaluate algorithm performance, false negative rate FN, false positive rate FP and accuracy AC are introduced in this article [3].

3.1 Test Under Noise and JPEG Compression Factor

200 images are randomly selected from CASIA TIDEV1.0 database for the test. For each image, a zone is selected to be copied and pasted to a non-overlapped zone, and then Gaussian noise or JPEG compression is implemented in the pasted zone, and finally the above three algorithms are respectively adopted for image test. The test results are as shown in Fig.8, Fig.9 and Fig.10.

![Fig. 2. Detection Accuracy under Different Noises and JPEG Qualities](image1)

![Fig. 3. False Positive Rate under Different Noises and JPEG Qualities](image2)

![Fig. 4. False Negative Rate under Different Noises and JPEG Qualities](image3)
According to Fig.8, Fig.9 and Fig.10, for the same algorithm, if the tampered zone is less post-processed, then the detection accuracy thereof is higher while the false positive rate and the false negative rate thereof are lower; for the same post-processing, the algorithm proposed in the article is superior to Algorithm A and Algorithm B in the aspects of accuracy rate, false positive rate and false negative rate, thus indicating that the algorithm proposed in the article has good robustness, because LL and HH dual constraints are adopted for the algorithm proposed in the article to reduce false detection and missing detection of the image and improve the detection accuracy of the algorithm.

In a word, the image forgery detection algorithm based on the translation invariance of non-sampling wavelet transform and the amplitude rotation invariance of Zernike moments can improve algorithm robustness and has strong noise immunity.

4 Conclusion

In order to solve such problems as poor robustness and low detection accuracy in the present copying & pasting forgery detection algorithm, an image copying & moving forgery detection algorithm based on non-sampling wavelet transform (undecimated wavelet transform, UWT) coupling with Zernike moments is proposed in this article. Firstly, the non-sampling wavelet transform is adopted to decompose the input image into approximation coefficient LL and detail coefficient HH to obtain the similarity and the diversity of the image blocks; secondly, the overlapped blocks are divided to calculate the sub-block interval of the image; thirdly, the sub-blocks are ordered and classified according to LL similarity and HH diversity; fourthly, Zernike moments are introduced to construct the distance matrix for image feature matching and image forgery detection. The experiment shows: the algorithm proposed thereby has good translation invariance and amplitude rotation invariance, good post-processing resistance performance, high detection accuracy, low false negative rate and low false positive rate.

References