

Digital Image Forgery Detection based on Texture Feature and Clustering Technique

Upendra Ujjainiya
Dept. of Information Technology
SATI Vidisha (M.P.)

Shaila Chugh
Dept. of Information Technology
SATI Vidisha(M.P.)

ABSTRACT

The image forgery detection is important tools in digital multi-media analysis. Now a day's digital multi-media faced a problem of copy paste and tampering by different multi-media authoring tools. The tampered and copy paste image change the actual scenario of original image and its illegal process in current scenario of multi-media. For the detection of image forgery various pixel and transform based method are applied. The applied method is better in some detection and estimation, but faced a certain limitation. In this paper proposed texture based image forgery detection. The texture based image forgery detection is very efficient in terms of detection ratio. For the extraction of texture feature used discrete wavelet transform function. For the generation of block used partition clustering technique. the partition clustering technique creates the block of original and forged image. The proposed algorithm is simulated in MATLAB software and used very famous dataset MFIC2000.

Keywords

Image Forgery, DWT, Cluster Segmentation, Texture

1. INTRODUCTION

The image forgery detection process imparts vital role in digital image forensic. For the analysis of image used forgery detection software and tools. The image forgery detection required two image one image is original and other is forged image. Now a day's various image forgery detection technique is used [1,2]. The sampling and processing of image gives two process of domain for image forgery one is pixel based and other is transform based method. For the forgery of image used various technique such as image painting, image slicing, image enhancement and image merging and copy paste. In this paper proposed a novel image forgery method. The proposed method based on wavelet transform function and clustering technique [3]. The wavelet transform function gives the texture feature. The texture feature is important and lower content feature of digital image. The extracted texture feature used for the creation of block and pattern. The generation of block and pattern used clustering technique for the processing of forged and original image. For the processing of clustering used k-means clustering technique. k-means is well known clustering technique and its very simple for the processing of pattern and block [4]. For the matching of different position of block measure similarity difference. For the measurement of similarity difference used person coefficient derivation. The person coefficient measures the similarity and dissimilarity of original and forged image [6]. Texture based image forgery detection have some limitation

related the process of feature selection and region selection of coefficient block. The major problem is measure the similarity of forgery and original image. Optimal feature selection for the purpose of detection. Noise value of image equal to higher intensity value of actual image. Region of forged image are not precise. Most forged image is enhanced. such types of limitation are minimised in proposed algorithm [7,8]. The proposed methods are evaluated on a number of original and forged images. According to our experimental results the proposed methods are quite attractive. The forgery is done with just copy-move, copy-move with rotation, with scaling, and reflection. In this process, an image database that consists of original and forged images is also developed [9,10]. The proposed method achieves 100% accuracy in just copy-move forgery (without any change in the size or characteristics of the object) forgery without post-processing and 97.43%, 66.58%, and 99.12% accuracies in copy-move forgery with rotation, scaling, and reflection, respectively. Also to ensure more efficiency, we have added some random noise on the images, the detection accuracy achieved 98.23%. the above section describes the process of image forgery and proposed method[12]. In section 2 discuss the feature extraction technique. in section 3. Discuss the proposed methodology. In section 4 discuss the experimental result analysis and finally discuss conclusion and future work in section 5.

2. FEATURE EXTRACTION

The image forgery detection method basically based on the lower content feature of digital image. The digital image basically contains three types of features, color feature, texture feature and shape size feature. The texture feature is most important features for the analysis of image forgery detection. For the extraction of texture feature used feature extractor. The texture feature extractor used wavelet transform function. The wavelet transform function is well known texture feature extractor. The wavelet transform function is basically being a combination of lower and high frequency. The process of sampling of original image and forged image are describing here [13,14].

3. PROPOSED METHODOLOGY

The proposed algorithm is combination of two algorithms one is wavelet transform function and other is clustering technique. the wavelet transform function gives the texture feature of original image and forged image. After the extraction of feature of original and forged image generate the pattern of cluster. The formation of cluster required the matching of block for the further process of detection.

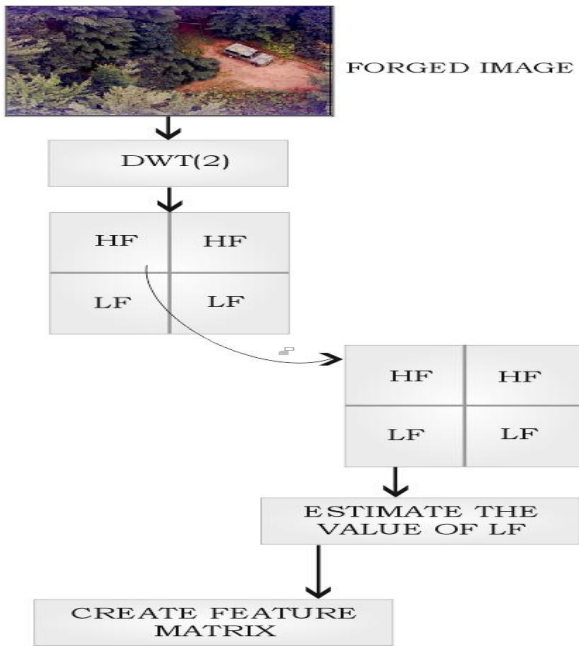


Figure 1: shows that process block diagram of feature extraction for forged image.

Steps 1sampling of texture feature

The texture feature distributes for the process of cluster mapping using equation (1) and (2)

For the processing of texture feature mapping of data.

$$x(i, j) = \frac{(x^*(i, j) - x_{\min}(j))}{(x_{\max}(j) - x_{\min}(j))} \quad (1)$$

Creates blocks for the matching of point in forged and original image:

$$x(i, j) = \frac{(x_{\max}(j) - x^*(i, j))}{(x_{\max}(j) - x_{\min}(j))} \quad (2)$$

Step 2 estimates the value of block of forged image $Q(a)$.

$\{x(i, j) | j = 1, 2, \dots, p\}$ is block point for the pattern $a = [a(1), a(2), \dots, a(p)]$ as:

$$z(i) = \sum_{j=1}^p a(j)x(i, j), \quad i = 1, 2, \dots, n \quad (3)$$

Estimate the common feature block of forged image and original image

$$Q(a) = S_z D_z \quad (4)$$

Where S_z is the similar block of original image $z(i)$; D_z is the forged image block S_z and mapping D_z are defined in formula (5):

$$\begin{cases} S_z = \sqrt{\frac{\sum_{i=1}^n (z(i) - E(z))^2}{(n-1)}} \\ D_z = \sum_{i=1}^n \sum_{j=1}^n (R - r(i, j))u(R - r(i, j)) \end{cases} \quad (5)$$

(1) Defining $d(z(k), z(h))$ as the absolute distance between two pattern of original and forged image $d(z(k), z(h)) = \sqrt{(z(k) - z(h))(z(k) - z(h))} = \sqrt{(z(k) - z(h))^2}$

$k = 1, 2, \dots, N; h = 1, 2, \dots, N$

Step 3 measure the similarity of block pattern

$$\begin{cases} \text{s. t. } \sum_{j=1}^p a^2(j) = 1 \\ 1 \geq a(j) \geq 0 \end{cases} \quad (7)$$

Step 4 estimate the area of image as forged.

The validation of cluster of both image used equation (3)

4. EXPERIMENTAL RESULT

In this section define the experimental results analysis with existing and proposed methods, the simulation environment is matlab, and all software the performance parameters are calculated with this software using existing as well as proposed method methods. Here the the detection error at the image level is measured by the ratio of the missing detection to the forged images (i.e. false negative rate, FN), and the ratio of the false alarm to the original images (i.e. false positive rate, FP). Mathematically [15,16],

$$F_N = \frac{\{\text{forged images detected as original}\}}{\{\text{Forged Images}\}}$$

$$F_P = \frac{\{\text{Original images detected as forged}\}}{\{\text{Original Images}\}}$$

$$F_P = \frac{\{\text{Original images detected as forged}\}}{\{\text{Original Images}\}}$$

$$F_P = \frac{\{\text{Original images detected as forged}\}}{\{\text{Original Images}\}}$$

In this paper, also used some dataset for the result analysis the MICC-600 this dataset is composed by 600 high resolution images containing realistic and challenging copy-move attacks; 160 are tampered images and 440 are originals.

Table 1. Shows that the performance evaluation using Segmentation and proposed methods

Types of Image	Method Name	FN	FP
Image-1	Segmentation	17.4059	35.0606
	Proposed	14.0278	32.0606
Image-2	Segmentation	6.8661	37.6000
	Proposed	5.4049	34.6000
Image-3	Segmentation	12.7531	32.5431
	Proposed	11.6547	30.7576

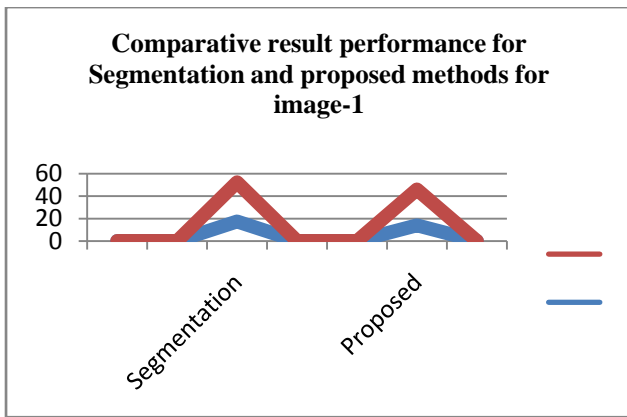


Figure 2: Shows that the comparative performance evaluation graphs for FN and FP with using Segmentation and Proposed methods with using image-1.

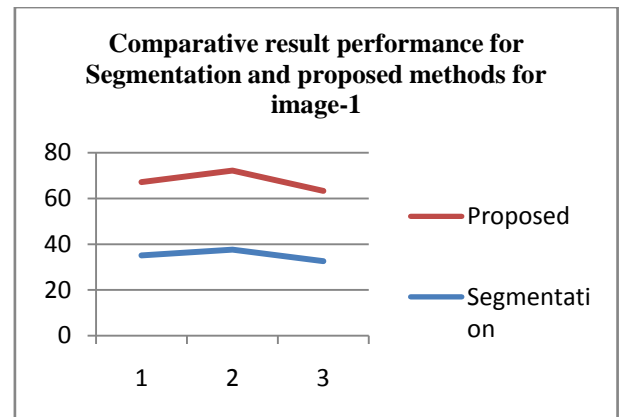


Figure 5: Shows that the comparative performance evaluation graphs for FN and FP with using Segmentation and Proposed methods with using image-1.

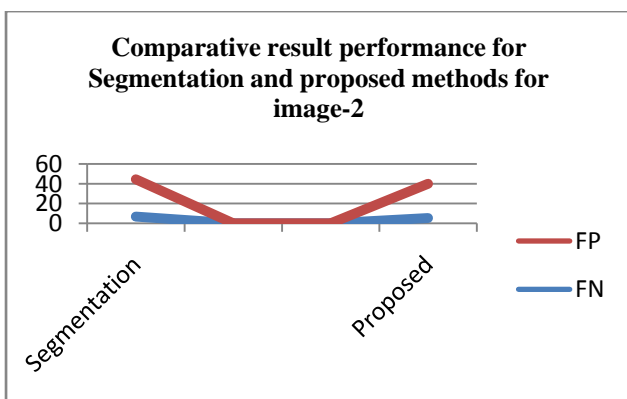


Figure 3: Shows that the comparative performance evaluation graphs for FN and FP with using Segmentation and Proposed methods with using image-2.

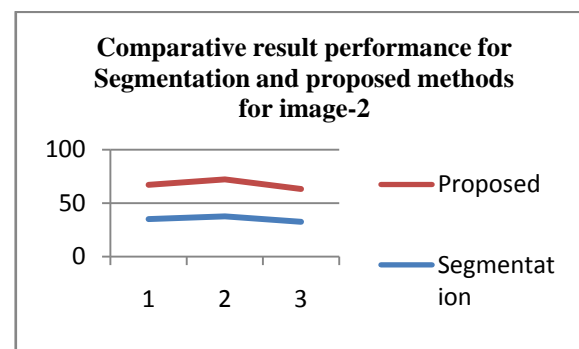


Figure 6: Shows that the comparative performance evaluation graphs for FN and FP with using Segmentation and Proposed methods with using image-2.

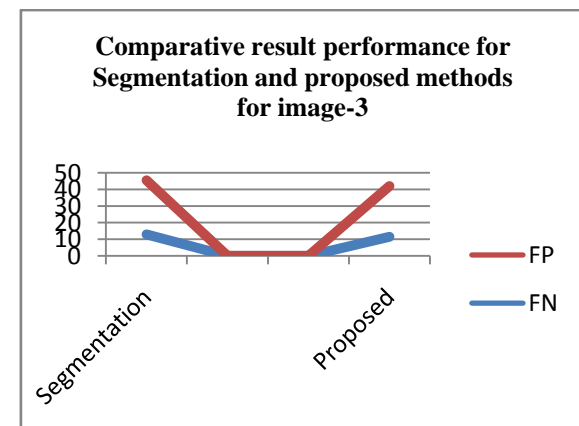


Figure 4: Shows that the comparative performance evaluation graphs for FN and FP with using Segmentation and Proposed methods with using image-3.

Table 2. Table captions should be placed above the table

Graphics	Top	In-between	Bottom
Tables	End	Last	First
Figures	Good	Similar	Very well

5. CONCLUSION

In this paper proposed image forgery detection algorithm based on wavelet transform function and clustering algorithm. the proposed algorithm used data distribution technique using cluster selection technique. the proposed algorithm used two image one image is original and other is forged image. The distribution of data using the partition clustering technique creates block of pattern. The process of standard deviation measures the bock of difference of original and forged image. The proposed algorithm simulated in MATLAB software and used standard forgery image dataset MFICC2000. The proposed algorithm reduces the value of false negative and improve the value of detection. In future used feature optimization technique for better generation of pattern during the process of matching.

6. REFERENCES

- [1] Jian Li, Xiaolong Li, Bin Yang, Xingming Sun "Segmentation-Based Image Copy-Move Forgery Detection Scheme" IEEE 2015 PP 507-518.
- [2] Edoardo Ardizzone, Alessandro Bruno, Giuseppe Mazzola "Copy-Move Forgery Detection by Matching Triangles of Keypoints" IEEE 2015 PP 2084- 2093.

- [3] Davide Cozzolino, Giovanni Poggi, Luisa Verdoliva “Efficient Dense-Field Copy–Move Forgery Detection” IEEE 2015 PP 2284-2296
- [4] B.L.Shivakumar, Lt. Dr. S.Santhosh Baboo “Detecting Copy-Move Forgery in Digital Images: A Survey and Analysis of Current Methods” Global Journal of Computer Science and Technology 2010 PP 660-664.
- [5] Raymond B. Wolfgang and Edward J. Delp “A Watermark For Digital Images”.
- [6] Tanzeela Qazi, Khizar Hayat, Samee U. Khan, Sajjad A. Madani, Imran A. Khan, Joanna Kołodziej, Hongxiang Li, Weiyao Lin, Kin Choong Yow, Cheng-Zhong Xu “Survey on blind image forgery detection IET Image Processing” IET 2013 PP 660-669.
- [7] Gajanan K. Birajdar , Vijay H. Mankar “Digital image forgery detection using passive techniques: A survey” ELESEVIER Digital Investigation 2013 PP 226–245.
- [8] Archana V. Mire, Dr S. B. Dhok, Dr N. J. Mistry ,Dr P. D. Porey “Catalogue of Digital Image Forgery Detection Techniques, an Overview” Elsevier, 2013 502-508.
- [9] Gung Polatkan, Sina Jafarpour, Andrei Brasoveanu, Shannon Hughes, Ingrid Daubechies “Detection Of Forgery In Paintings Using Supervised Learning”
- [10] Yu-Feng Hsu ,Shih-Fu Chang “Detecting Image Splicing Using Geometry Invariants And camera Characteristics Consistency”
- [11] Gang Cao, Yao Zhao and Rongrong Ni “Edge-based Blur Metric for Tamper Detection” Journal of Information Hiding and Multimedia Signal Processing 2010 .PP 20-27.
- [12] Chih-Chung Hsu , Tzu-Yi Hung, Chia-Wen Lin , Chiou-Ting Hsu “Video Forgery Detection Using Correlation of Noise Residue”
- [13] Ghulam Muhammad , Munner H, Al-Hammadi , Muhammad Hussain, George Bebis, “Image Forgery Detection using Steerable Pyramid Transform and Local Binary Pattern” Springer-Verlag Berlin Heidelberg ,2013.
- [14] Tiziano Bianchi, Alessia De Rosa, Alessandro Piva, “Improved DCT Coefficient Analysis for Forgery Localization In JPEG Images” IEEE, 2011. Pp 2444-2447.
- [15] H. Farid, "Image Forgery Detection" Signal Processing Magazine, IEEE, March 2009, Vol. 26, No. 2, Pp 16-25.
- [16] G. Cao, Y. Zhao, R. Ni and X. Li, “Contrast Enhancement-Based Forensics in Digital Images” IEEE Transactions on Information Forensics and Security, 2014, Vol 9, No. 3, Pp 515-525.
- [17] G. Chierchia, G. Poggi, C. Sansone and L. Verdoliva, “A Bayesian-MRF Approach for PRNU-Based Image Forgery Detection” Information Forensics and Security, IEEE Transactions, 2014, Vol. 9, No. 4, Pp 554-567.