Image Forgery Detection sing Clustering Algorithm & Transform Function

Sanjay Gupta

sanjgupta24@gmail.com

Department of computer Science & Engg.

Lecturer, Polytechnic College, Satna (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

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 II discuss the feature extraction technique. in section III. Discuss the proposed methodology. In section IV discuss the experimental result analysis and finally discuss conclusion and future work in section V.

II. 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].

III. 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.

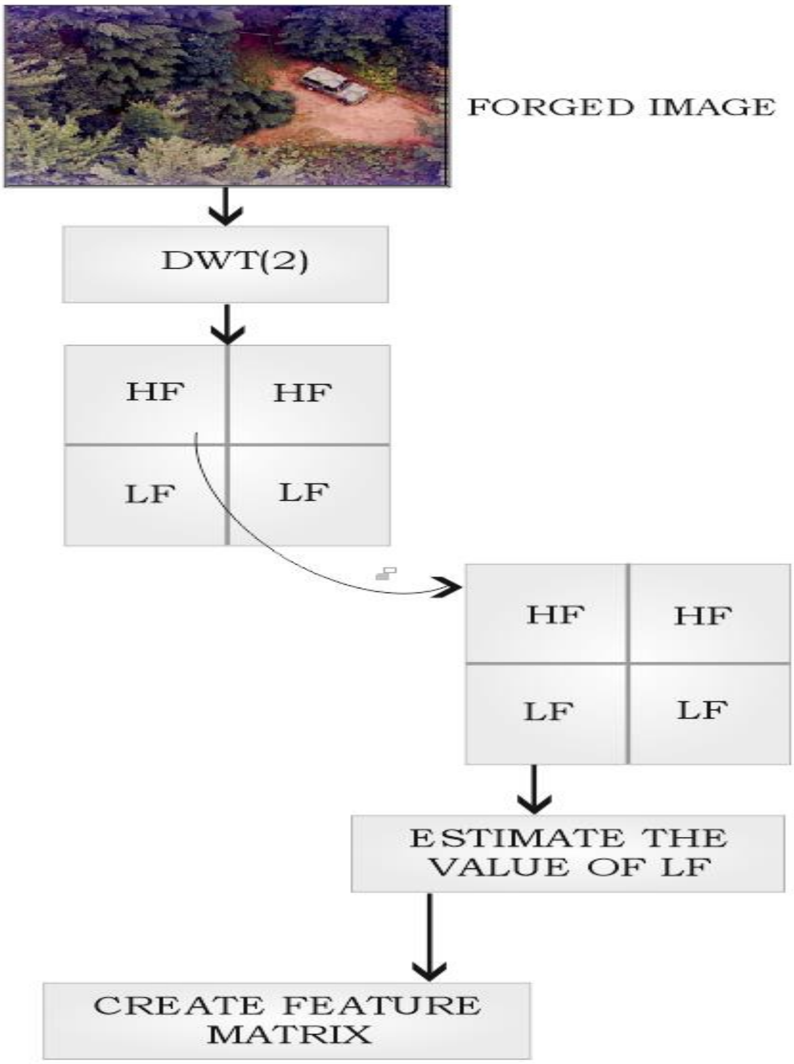

Figure 1 shows that process block diagram of feature extraction for forged image.

Steps 1 sampling 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.

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

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

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

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

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

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

Estimate the common feature block of forged image and original image

$$Q(a) = S_z\, D_z \qquad (4)$$

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):

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

.

(1) Defining $d(z(k), z(h))$ as the absolute distance between two pattern of original and forged image.

$$d(z(k), z(h)) = \sqrt{(z(k) - z(h))\,(z(k) - z(h))} = \sqrt{(z(k) - z(h))^2}$$

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

Step 4 measure the similarity of block pattern

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

Step 5 estimate the area of image as forged.

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

IV. experimental Result

In this section we 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= |{forged images detected as original}|

|{Forged Images}|

F_P= |{Original images detected as forged}|

|{Original Images}|

We 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.

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

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

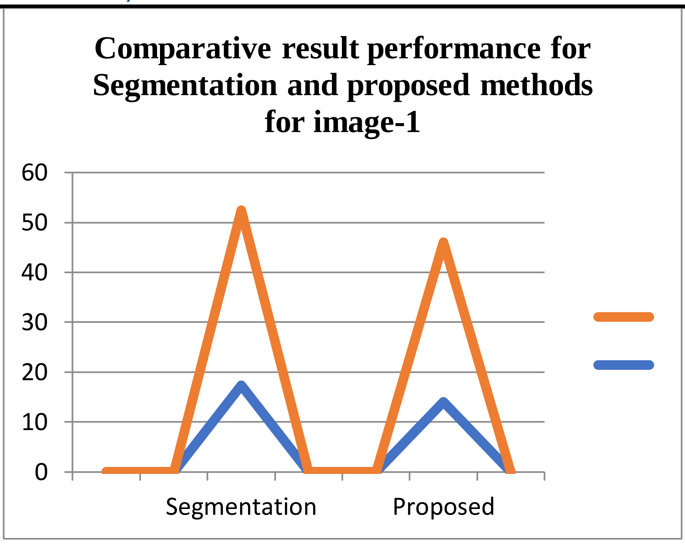

Figure 2: Shows that the comparative performance evaluation graphs for FN and FP with using Segmentation and Proposed methods with using image-1.

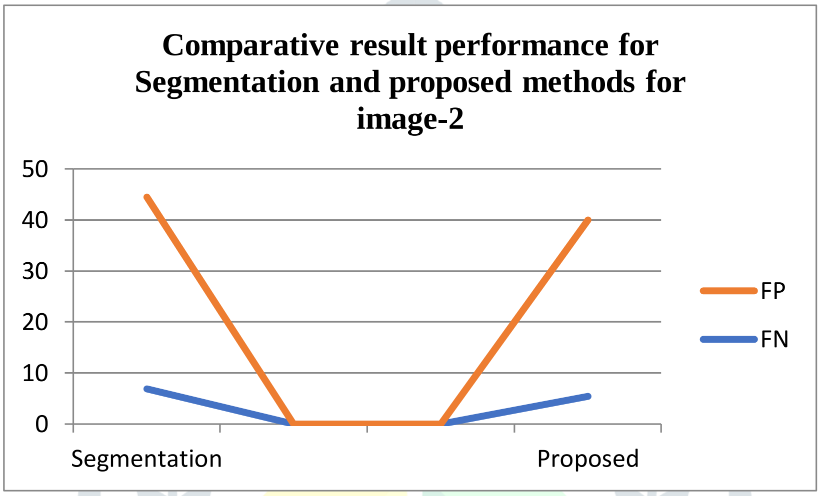

Figure 3: Shows that the comparative performance evaluation graphs for FN and FP with using Segmentation and Proposed methods with using image-2.

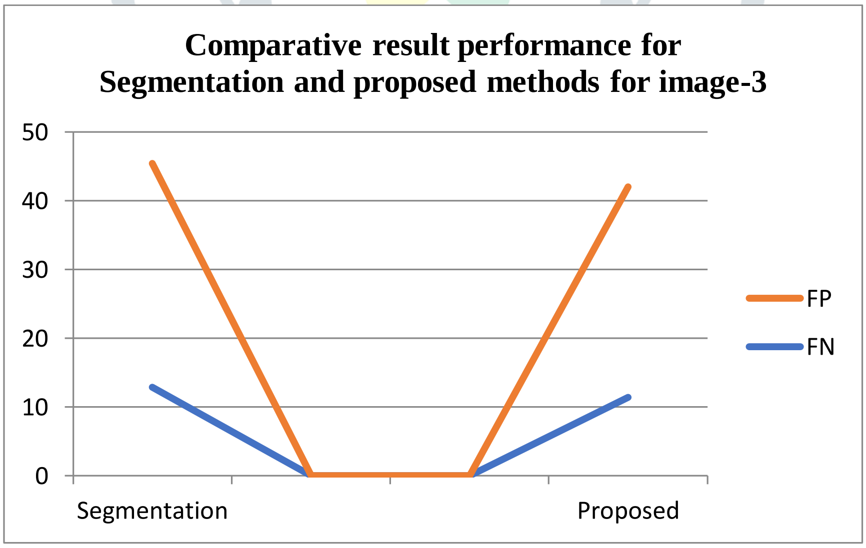

Figure 4: Shows that the comparative performance evaluation graphs for FN and FP with using Segmentation and Proposed methods with using image-3.

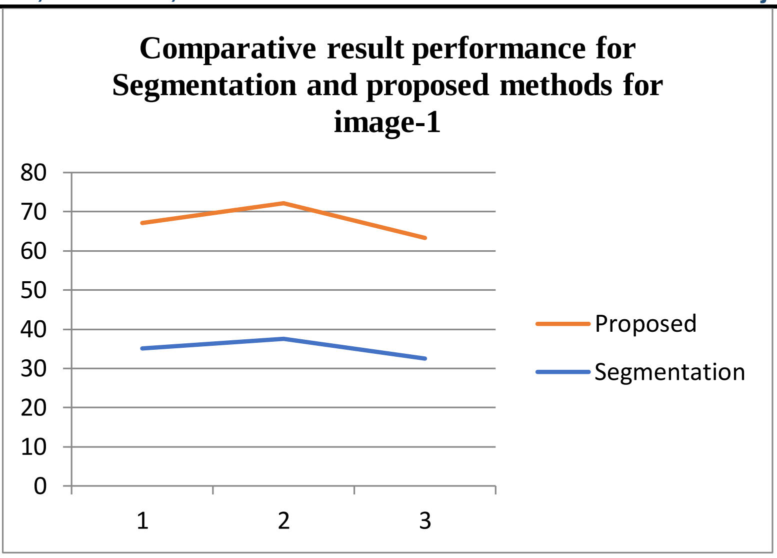

Figure 5: Shows that the comparative performance evaluation graphs for FN and FP with using Segmentation and Proposed methods with using image-1.

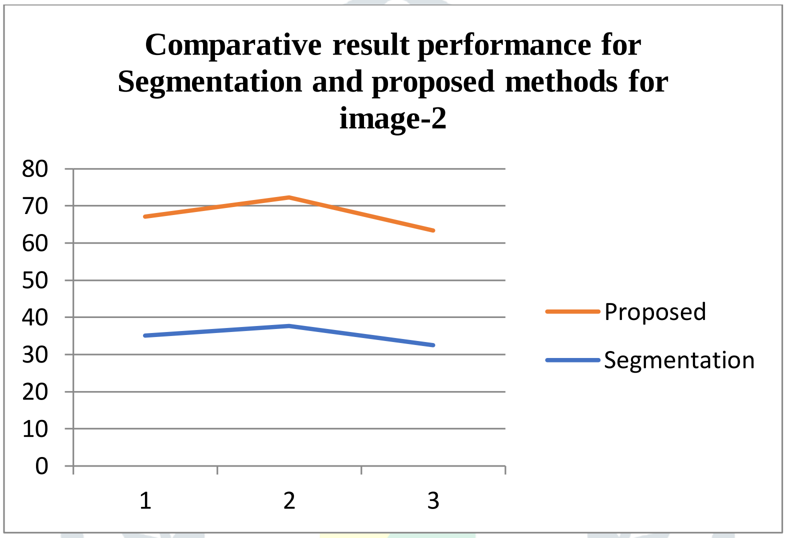

Figure 6: Shows that the comparative performance evaluation graphs for FN and FP with using Segmentation and Proposed methods with using image-2.

V. Conclusion & Future Work

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.

References

[1]. Emam, Mahmoud, Qi Han, and Xiamu Niu. "PCET based copy-move forgery detection in images under geometric transforms." Multimedia Tools and Applications 75, no. 18 (2016): 11513-11527.

[2]. Isaac, Meera Mary, and M. Wilscy. "Image forgery detection based on Gabor wavelets and local phase quantization." Procedia Computer Science 58 (2015): 76-83.

[3]. Qureshi, Muhammad Ali, and Mohamed Deriche. "A bibliography of pixel-based blind image forgery detection techniques." Signal Processing: Image Communication 39 (2015): 46-74.

[4]. Alhussein, Musaed. "Image tampering detection based on local texture descriptor and extreme learning machine." In 2016 UKSim-AMSS 18th International Conference on Computer Modelling and Simulation (UKSim), pp. 196-199. IEEE, 2016.

[5]. Marra, Francesco, Giovanni Poggi, Fabio Roli, Carlo Sansone, and Luisa Verdoliva. "Counter-forensics in machine learning based forgery detection." In Media Watermarking, Security, and Forensics 2015, vol. 9409, pp. 181-191. SPIE, 2015.

[6]. Shahroudnejad, Atefeh, and Mohammad Rahmati. "Copy-move forgery detection in digital images using affine-SIFT." In 2016 2nd International Conference of Signal Processing and Intelligent Systems (ICSPIS), pp. 1-5. IEEE, 2016.

[7]. Kaur, Navneet, and Nitish Mahajan. "Image forgery detection using SIFT and PCA classifiers for panchromatic images." Indian journal of Science and Technology 9, no. 35 (2016): 1-6.

[8]. Uliyan, Diaa M., Hamid A. Jalab, and Ainuddin W. Abdul Wahab. "Copy move image forgery detection using Hessian and center symmetric local binary pattern." In 2015 IEEE conference on open systems (ICOS), pp. 7-11. IEEE, 2015.

[9]. Malathi, J., T. Satya Nagamani, and KNVSK Vijaya Lakshmi. "Survey: Image forgery and its detection techniques." In Journal of Physics: Conference Series, vol. 1228, no. 1, p. 012036. IOP Publishing, 2019.

[10]. Zhang, Yujin, Chenglin Zhao, Yiming Pi, Shenghong Li, and Shilin Wang. "Image-splicing forgery detection based on local binary patterns of DCT coefficients." Security and Communication Networks 8, no. 14 (2015): 2386-2395.

[11]. Hashmi, Mohammad Farukh, and Avinash G. Keskar. "Block and fuzzy techniques based forensic tool for detection and classification of image forgery." Journal of Electrical Engineering and Technology 10, no. 4 (2015): 1886-1898.

[12]. Reshma, P. D., and C. Arunvinodh. "Image forgery detection using SVM classifier." In 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), pp. 1-5. IEEE, 2015.

[13]. Abd Warif, Nor Bakiah, Ainuddin Wahid Abdul Wahab, Mohd Yamani Idna Idris, Roziana Ramli, Rosli Salleh, Shahaboddin Shamshirband, and Kim-Kwang Raymond Choo. "Copy-move forgery detection: survey, challenges and future directions." Journal of Network and Computer Applications 75 (2016): 259-278.

[14]. Tuba, Ira, Eva Tuba, and Marko Beko. "Digital image forgery detection based on shadow texture features." In 2016 24th Telecommunications Forum (TELFOR), pp. 1-4. IEEE, 2016.

[15]. Zhu, Ye, Tian-Tsong Ng, Xuanjing Shen, and Bihan Wen. "Revisiting copy-move forgery detection by considering realistic image with similar but genuine objects." arXiv preprint arXiv:1601.07262 (2016).

[16]. Gong, Jiachang, and Jichang Guo. "Image copy-move forgery detection using SURF in opponent color space." Transactions of Tianjin University 22, no. 2 (2016): 151-157.

[17]. Shih, Frank Y., and Jason K. Jackson. "Copy-cover image forgery detection in parallel processing." International Journal of Pattern Recognition and Artificial Intelligence 29, no. 08 (2015): 1554004.

[18]. Kaushik, Rajeev, Rakesh Kumar Bajaj, and Jimson Mathew. "On image forgery detection using two dimensional discrete cosine transform and statistical moments." Procedia Computer Science 70 (2015): 130-136.

[19]. Barani, Milad Jafari, Peyman Ayubi, Fooad Jalili, Milad Yousefi Valandar, and Ehsan Azariyun. "Image forgery detection in contourlet transform domain based on new chaotic cellular automata." Security and Communication Networks 8, no. 18 (2015): 4343-4361.

[20]. Zheng, Jiangbin, Yanan Liu, Jinchang Ren, Tingge Zhu, Yijun Yan, and Heng Yang. "Fusion of block and keypoints based approaches for effective copy-move image forgery detection." Multidimensional Systems and Signal Processing 27, no. 4 (2016): 989-1005.