International Journal of Master of Engineering Research and Technology, 2394-6172-(O)
Volume-5, Issue-7, July 2018

IMAGE FORGERY DETECTION BASED ON LOCAL FEATURE DESCRIPTOR USING HYBRID ALGORITHM

Nupur Agrawal
M. Tech. Scholar
Department of CSE
PIT, Bhopal MP
nupur.agrawal90@gmail.com

Surendra Vishwakarma
Asst. Professor
Department of CSE
PIT, Bhopal MP
s.vish83@gmail.com

ABSTRACT

In current decade, digital images are in use in a wide range of applications and for multiple purposes. They also play an important role in the storage and transfer of visual information, especially the secret ones. With this widespread usage of digital images, in addition to the increasing number of tools and software of digital images editing, it has become easy to manipulate and change the actual information of the image. Therefore, it has become necessary to check the authenticity and the integrity of the image by using modern and digital techniques, which contribute to analysis and understanding of the images' content, and then make sure of their integrity. There are many types of image forgery, the most important and popular type is called copy-move forgery, which uses the same image in the process of forgery. This type of forgery is used for one of two things, first to hide an object or scene by copying the area of the image and pasting it on another area of the same image.

Keywords: - Image Forgery, Forgery Detection, Forgery Detection Technique, Data Provenance, Wavelet Transforms Function, Feature Extraction, Clustering Algorithm.

INTRODUCTION

Forgeries are not new to mankind but are a very old problem. In the past it was limited to art and literature but did not affect the general public. Nowadays, due to the advancement of digital image processing soft-ware and editing tools, an image can be easily manipulated and modified[1]. Digital images in the current era play very important role in various fields. They are used in different applications in the area of military, news, medical diagnosis and media, to mention a few[2-4]. Due to the development in technology of digital image, for example, cameras, software, and computers and the wide spread via the internet, digital image can be considered a major source of information in today's digital world[7]. But to believe what we see, we must make sure that the image is original. Thus, the images are required to pass the test authenticity. It is very difficult for humans to identify visually whether the image is original or manipulated. There is rapid increase in digitally manipulated forgeries in mainstream media and on the Internet. This trend indicates serious vulnerabilities and decreases the credibility of digital images. Therefore, developing techniques to verify the integrity and authenticity of the digital images is very important, especially considering that the images are presented as evidence in a court of law, as news items, as a part of medical records, or as financial documents. In this sense, image forgery detection is one of the primary goals of image forensics[5-6].

In the rest part of this research work, section II – wavelet transform function, Section-III proposed algorithm, Section-IV experimental work and performance and finally discussed the conclusion and future work in section V.

II. WAVELET TRANSFORMS FUNCTION

Wavelet transform is widely used in machine vision as an image processing technique for object detection and classification. Wavelets have been applied in the past to analyze images and are used in many applications in remote sensing, such as removing speckle noise from radar images merging high spectral resolution images with high spatial resolution images and texture analysis and classification[8, 11]. Wavelet transform has been used to classify EEG signal with integration of expert model. The concept of wavelet is closely related to multi-scale and multi- resolution application and it has been used in to image fusion

technique. Implementation of Discrete Wavelet Transform (DWT) as an image processing technique produces the transformation values called wavelet coefficient. The challenge here is how the coefficient can be interpreted to represent object for classification or detection. A common approach of feature extraction from wavelet transformation is the computation of mother of wavelet. Expert model has been used as a feature extraction tool to analyze sub-band frequency of wavelet transform. The sub-band frequencies were used as an input to the expert model network[9]. The common technique used for feature extraction of DWT coefficient is by using neural network. In this, wavelets will be used in the analysis of narrow and broad weed images since DWT allows decomposition of the image into different levels of resolution. By doing so, we introduce a new feature set that is based on the analysis of wavelet coefficient. This technique helps reduce the size of wavelet coefficient and produce a smaller size of feature vectors[10, 12].

III. PROPOSED ALGORITHM

In this section discuss the proposed algorithm for image forgery detection based on clustering technique. In the process of image forgery k-means clustering technique is applied. The k-means clustering technique is very efficient for the creation of block pattern. After the creation of block pattern used block matching process. For the purpose of clustering used texture feature data for forged and original image. Here discuss some algorithm steps for the process of cluster generation and matching process.

1: For image = (X,C) ←empty
2: C_list ← K-means (Ci_list, K_{auto})
3: Input C_list X , the clustering number pn , texture scale XN , probability For image P stop conditions cS ;
4: Code the data in real number and initialize texture matrix S(i),i = 0 at random;
5: Evaluate the all individual in the current instant D(s);
6: CR clustering requires number of cluster center, which way thrashing of data of waiting cluster. Hence the fitness function of algorithm is determined by f(x).
7: $$G(s)=\frac{N(s)}{D(s)}=\frac{\sum_{i=0}^{n-1}A_i s^i}{\sum_{i=0}^{n}a_i s^i}$$
Umpire the termination conditions. If the termination situation are satisfied, then turn to step 9, if not, turn to step 10;
8: Crack to find and compute the number clustering centers.
9: find final block of forged image
10: Take the CR matching on population P (i) and generate the next generation A (i +1). Then turn to step

11: for h ∈ A(i+1) do
12: h.nn ← CR (A(i+1)- {h})
13: h.sc ← Compute-SC (h, h.nn)
14: FORIMAGE←FORIMAGE ∪ {h}
15: FORIMAGE←FORIMAGE ∪ {h.nn}

16: if h.sc < th_{sc} then
17: E←E ∪ {(h,h.nn)}
18: End if
19: end for
20: count ← Matrix
for each pair of components (g1, g2) ∈ G do

21: μ_1←mean-dist (g1), μ_2←mean-dist (g2)
22: if $\frac{\mu_1+\mu_2}{2*centroid\_dist(g1,g2)}$ > 1 then g1←Merge (g1, g2)
23: end for
24: N_type ← empty
25: for x ∈ N list do

26: h←Pseudo point of (x)
27: estimate detection rate
28: FRR
29: end for

PROPOSED MODEL

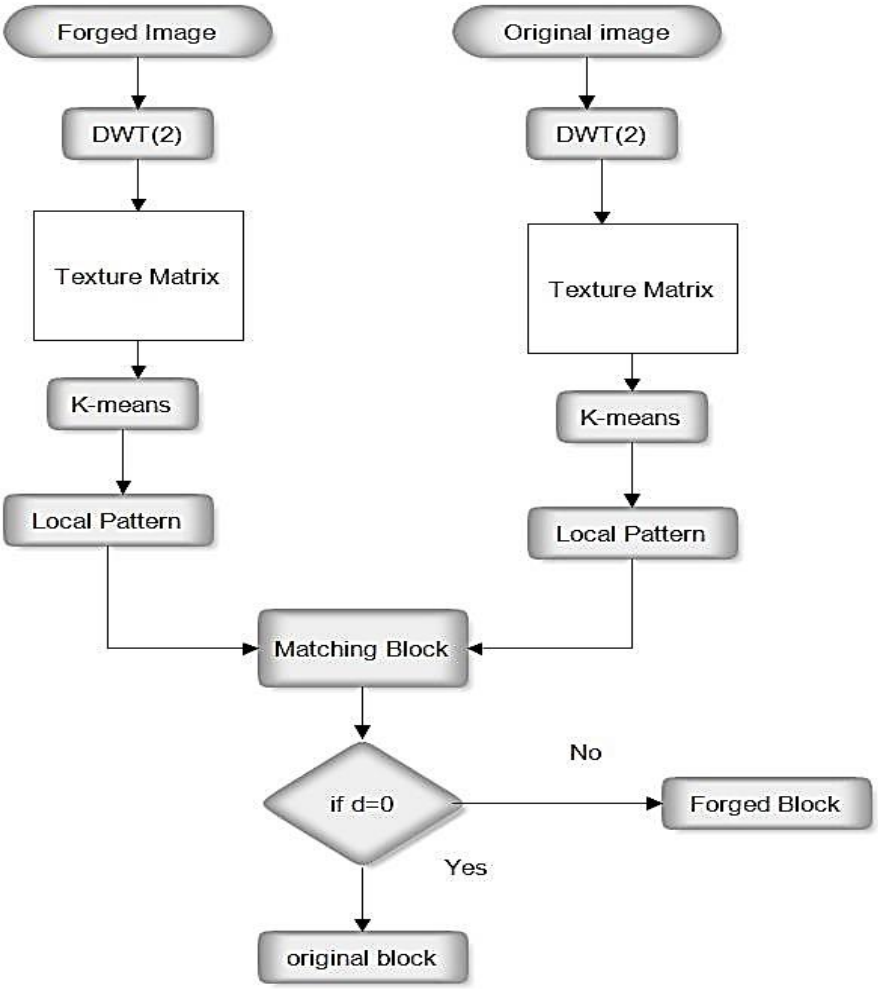

Figure 1: proposed model for image forged image.

IV. EXPERIMENTAL WORK AND PERFORMANCE

Figure 2: Image Forgery Detection based on the proposed technique

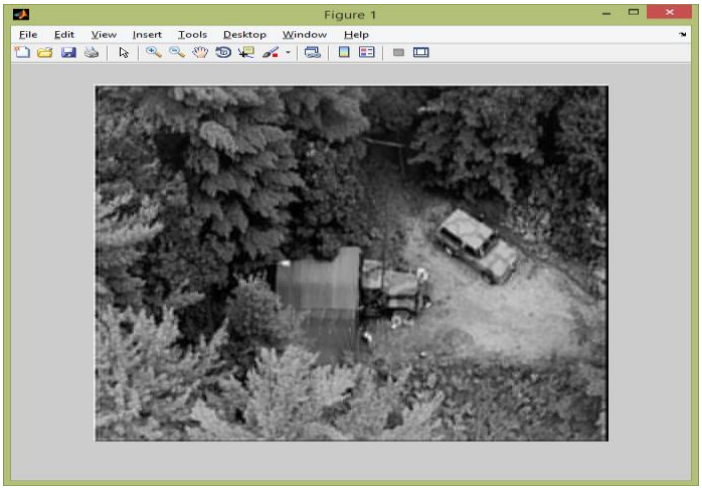

Figure 3: Shows that the Forest image loads initially from the dataset.

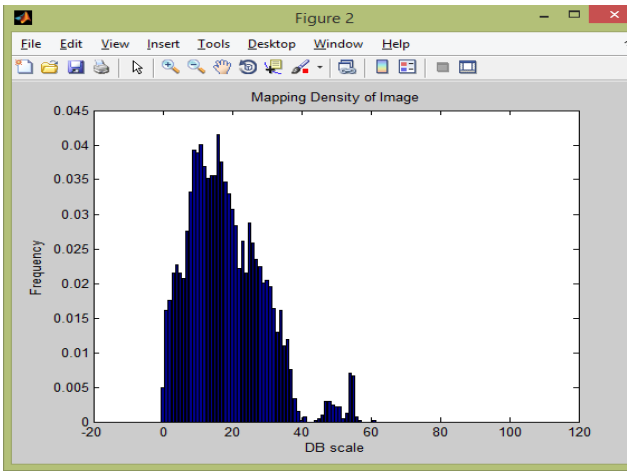

Figure 4: Mapping density of Forest image for proposed technique.

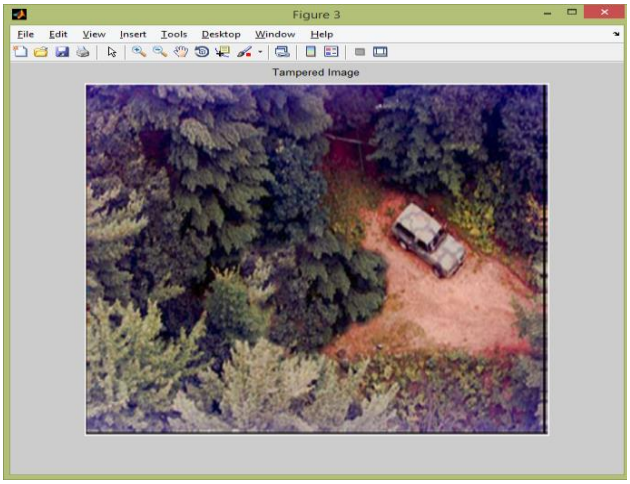

Figure 5: Tampered image of Forest image for the proposed technique.

Image name	Method	Detection Rate %	FRR %
Couple	LDBM	87.79	2.10
	PROPOSED	93.82	.420
Forest	LDBM	88.12	1.93
	PROPOSED	94.12	.268
Historical	LDBM	86.24	3.18
	PROPOSED	92.67	1.48
Water Fall	LDBM	89.27	3.820
	PROPOSED	95.48	.987

Table 1: Shows that the Detection Rate and FRR with using LDBM and Proposed method for the same and different number of images.

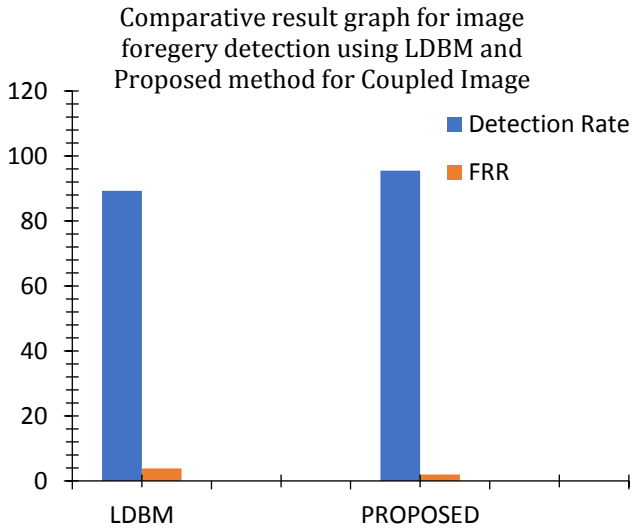

Figure 6: Shows that comparative result of Image "Coupled", with using LDBM and Proposed method and here our proposed method shows that the better result in the form of higher Detection Rate and low FRR than the existing method.

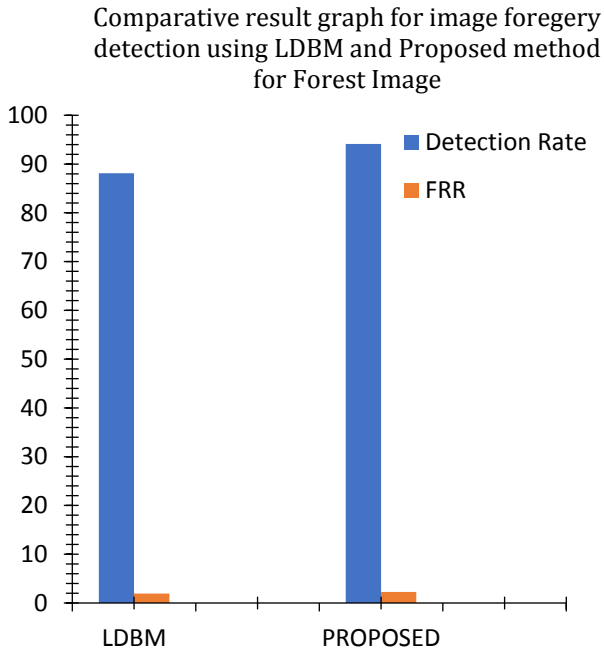

Figure 7: Shows that comparative result of Image "Forest", with using LDBM and Proposed method and here our proposed method shows that the better result in the form of higher Detection Rate and low FRR than the existing method.

V. CONCLUSIONS

In this dissertation proposed an image forgery detection technique based on clustering technique. The proposed image forgery used wavelet transform function for the extraction of feature of original and forged image. The extracted feature passes through clustering technique for the generation of local pattern. The local pattern passes though matching block and measure distance of two similar and dissimilar blocks. The proposed image forged detection technique is very efficient in compression of local pattern and transform function-based technique. 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.

REFERENCE

[1] Giovanni Chierchia, Giovanni Poggi, Carlo Sansone, Luisa Verdoliva "A Bayesian-MRF Approach for PRNU-Based Image Forgery Detection" Ieee Transactions on Information Forensics and Security, Vol-9, 2014. Pp 554-567.
[2] Andrea Costanzo, Irene Amerini, Roberto Caldelli, Mauro Barni "Forensic Analysis of SIFT Keypoint Removal and Injection" Ieee Transactions on Information Forensics and Security, Vol-9, 2014. Pp 1450-1464.
[3] Neenu H.U., Jini Cheriyan "Image Forgery Detection based on Illumination Inconsistencies & Intrinsic Resampling Properties" International Conference on Magnetics, Machines & Drives, IEEE 2014. Pp 1-6.
[4] Ghulam Muhammad, M. Solaiman Dewan, M. Moniruzzaman, Muhammad Hussain, M. Nurul Huda "image forgery detection using gabor filters and DCT" International Conference on Electrical Engineering and Information & Communication Technology, IEEE, 2014. Pp 254-259.
[5] Davide Cozzolino, Diego Gragnaniello, Luisa Verdoliva "Mage Forgery Detection Through Residual-Based Local Descriptors and Block-Matching" IEEE, 2014. Pp 5297-5302.
[6] Abhishek Kashyap, Shiv Dutt Joshi, "Detection of Copy-Move Forgery Using Wavelet Decomposition" IEEE, 2013, Pp 396-400.
[7] Saba Mushtaq and Ajaz Hussain Mir, "Digital Image Forgeries and Passive Image Authentication Techniques: A Survey" International Journal of Advanced Science and Technology (IJAST), 2014, Vol.73, Pp 15-32.
[8] Ketan S Bacchuwar, Aakashdeep, K.R Ramakrishnan, "A Jump Patch-Block Match Algorithm for Multiple Forgery Detection" IEEE, 2013, Pp 723-726.
[9] Ghulam Muhammada, Muhammad Hussain, George Bebis , "Passive Copy Move Image Forgery Detection using Undecimated Dyadic Wavelet Transform" Digital Investigation, 2012,Vol. 9,Pp 49-57.
[10] Sondos M. Fadl , Noura A. Semary, Mohiy M. Hadhoud, "Copy-Rotate-Move Forgery Detection Based on Spatial Domain" IEEE,2014,Pp 136-141.
[11] Cheng-Shian Lin and Jyh-Jong Tsay "Passive Forgery Detection for JPEG Compressed Image based on Block Size Estimation and Consistency Analysis" Natural Science Publishing Cor.,2015, Pp 1015-1028.
[12] Michael Zimba,Sun Xingming, "DWT-PCA (EVD) Based Copy-move Image Forgery Detection" IJDCTA, Vol.5, 2011, Pp 251-258 .