IMPLEMENTATION OF COPY MOVE FORGERY DETECTION USING DCT METHOD AND EDGE DETECTION

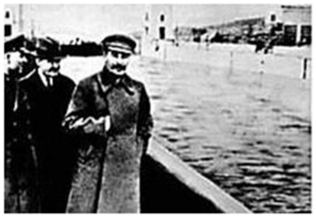
Sahil Mehra, Navdeep Kanwal
Punjabi University Patiala
iamsahil.mehra@gmail.com

***ABSTRACT*:** Security these days is a very important factor in information. The paper deals with image information security. An image is forged so that the desired results are obtained. The most common method is copy-move forgery. There is one technique called copy move forgery, in which a small content of image is moved to other portion. The need of copy move detection should be there to reduce such attacks. The Paper has suggested a new technique that is edge enhancement using Gabor filtering as pre-processing and the DCT transformation for the overlapping blocks has been generated as a feature vector. The features are then used for finding the blocks. The algorithm is evaluated by using standard quality metrics:- Sensitivity, Specificity as well as Accuracy. Experimental results show 98-100% accuracy in forgery detection for the tested images taken from CoMoFoD database.

***Keywords*:** Forgery detection, DCT, edge detection, sobel filter etc.

I. INTRODUCTION

Today there is large amount of data all around the world. How we secure that data these days is a big question. These days a largely modify data available easily at all places. How can we find that the data we have is original or not. Image forgery is common these days as we take example of one image.



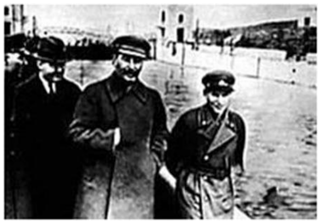
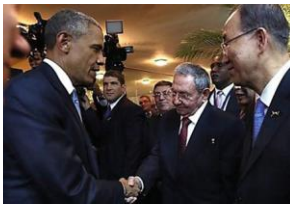


Fig 1(a): Forged Image

Fig 1(b): The original Image

There are two images which one is original, no one can say that. In Fig 1(a), there are 2 people in an image but in fig 1(b) there are three people in another. Both the images are same with little difference. This can be done with image forgery. In digital world fake news, image or data is common as person modified it according to their needs. But the fig 1(b) is the original one which is identified by the copy move forgery detection methods.

Another popular example which was in news in 2015 year is the barack obama handshake with Javad Zarif which was very popular in social media. But later we find that it's a matter of image forgery. Original image is Fig 2(b) in which barack obama handshake with Cavillion Raul.



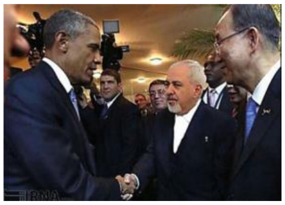


Fig2(a): Forged Image Fig2(b): Original Image

Now question arise that how can we find that the image is original or not. There are two techniques in the image forgery detection method:

- Active forgery Detection
- Passive forgery detection

Active forgery detection method is used for the authentication of the data. This technique is very helpful for finding the authenticity. Active forgery technique used watermark, statically tools and digital signature to protect and detect the data.

Passive forgery detection method is also known as blind forgery technique. In this method we only maintain the integrity of the image. In which we don't use watermark and digital signature to authentication of the image. It is used to remove the inconsistency of the image.

There are researchers who have contributed in various forgery techniques. The researchers have proposed different techniques to detect the forged portion of the image. They have done wonderful contribution in detecting the forged region of the image but the existing techniques have less accuracy in terms of forgery detection.

II. LITERATURE SURVEY

Copy move forgery detection has a lot of concerns in research in which different types of algorithms has been proposed by different scholars. The techniques suggested detecting this type of interfering along with the original image but, numerous questions still persisted either unresolved or there is too much possibility for performance enhancement. In [4], a technique called forgery detection has identified for the first time. Many algorithms are developed in this approach as it's a very sensitive and personal matter. Data is always important from the last so many year but today as world is going to become digital a large scale side-effects come to see. Today there are lots of technique, algorithms, approaches and methods are developed to stop forgery but till now we cannot reach to 100 percent result. Many scientists are doing research on this field to make it better day by day. In [11], a DCT technique is developed in forgery to check the block to block detection. In [13], PCA technique to use in represents the image block. Principal component analysis exploiting various features in it but failed to detect when rotation is there. After then a new technique is formed called DWT which is based on sorted neighborhood. In which we divide the image into four parts and apply singular value decomposition technique on the low part. In [12], a new technique called FMT is proposed with bloom filter to detect image forgery. In [17], an upgraded DCT technique is used for detection of rotated image. Both methods were studied centered on the major constituents relatively to the three-channel colored image. Attained consequences were associated to a mentioned method. During carrying out this method, three basic parameters, namely contrast threshold, block dimension, and similarity threshold were optimized. In [22], a block matching new technique is developed which is called adaptive similarity threshold approach. In [15], a new algorithm is developed by with the help of DCT which is called row-column reduction algorithm, which identified the original image by converting into the matrix. This paper help us to study different techniques for image forgery and also tell us how to reduce complexity. Still there are some copy-move methods that do not gives us the exact results so we have presented a method based on following methodology.

III. METHDOLOGY

First a Red-Green-Blue(RGB) Image is converted to Grayscale. Then we apply gabor filter on edge pixels. In the next step, Sobel filter is applied for dominant edge detection. Then we break the image into overlapped square pattern for which image has been carried out using DCT algorithm and mean value. In matching process; only those blocks are matched whom central pixel is detected as edge pixel by sobel edge detection. This reduces computation time and gives effective results in less time. After that forged pixels has been calculated and the forgery is detected. The algorithm is described using given flowchart below:

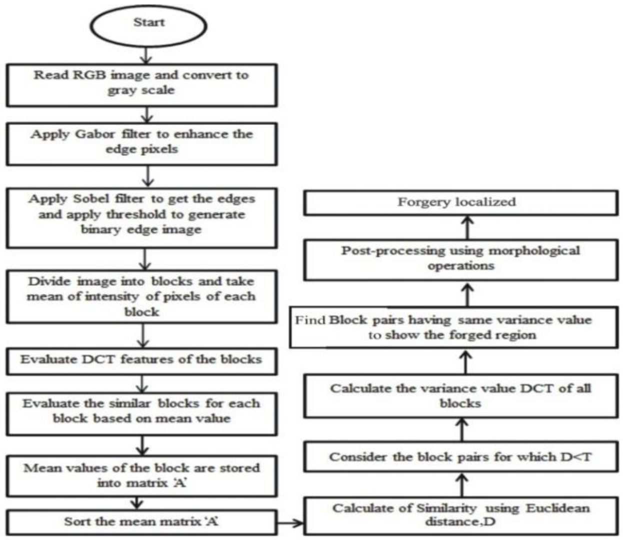

Start
Read RGB image and convert to gray scale
Apply Gabor filter to enhance the edge pixels
Apply Sobel filter to get the edges and apply threshold to generate binary edge image
Divide image into blocks and take mean of intensity of pixels of each block
Evaluate DCT features of the blocks
Evaluate the similar blocks for each block based on mean value
Mean values of the block are stored into matrix 'A'
Sort the mean matrix 'A'
Calculate of Similarity using Euclidean distance.D
Consider the block pairs for which D<T
Calculate the variance value DCT of all blocks
Find Block pairs having same variance value to show the forged region
Post-processing using morphological operations
Forgery localized

Fig 3: Flowchart of the presented method

IV. RESULTS AND DISCUSSIONS

The presented edge-DCT technique is implemented in MATLAB software. Then we check our data for RGB evaluation's [11-12]. The performance evaluation of presented method, sensitivity, specificity and accuracy has been calculated for each image. The classification accuracy is the degree to which the classifier can effectively group the model sand is outlined as confusion matrix to the test data. This is characterized as the proportion of the quantity of effectively arranged examples the positive and negative aggregate number of examples (species) grouped which is given in equation (1).

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{1}$$

- **Sensitivity**

The classifier is the fraction of the image samples correctly classified as that specific species class. It is defined by equation (2) below:

$$Sensitivity = \frac{TP}{TP+FN} \tag{2}$$

- **Specificity**

The specificity is defined as the part of normal pixel as normal class. It is also called selectivity. It is defined in equation(3) below.

$$Specificity = \frac{TN}{TN+FP} \tag{3}$$

The results for the actual pixel location using ground truth has been described with above parameters .

Table I: Sensitivity, specificity and accuracy parameters for the tested cases from CoMoFoD Database

Parameters	TP	TN	FP	FN	Sensitivity	Specificity	Accuracy
Case1	2994	257877	1273	0	1	0.9950	0.9951
Case2	28372	230270	3502	0	1	0.9850	0.9866
Case3	6716	254754	652	22	0.9967	0.9974	0.9974
Case4	3274	258166	676	28	0.9915	0.9973	0.9973
Case5	11710	246638	746	3050	0.7933	0.9969	0.9855

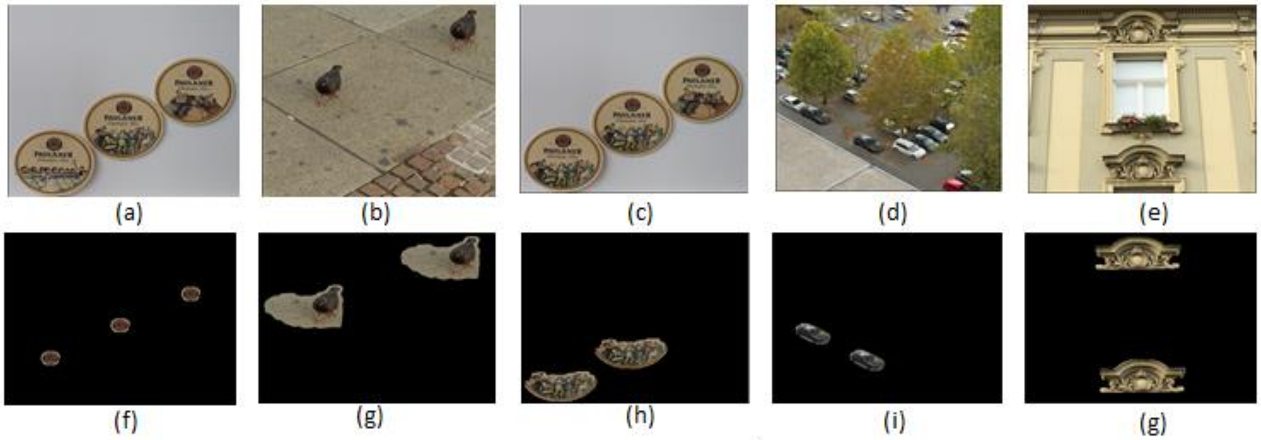


Fig 4(a-e): forged cases, Fig 4(f-g) forgery detected Cases by presented methodology.

Fig 4 above shows the accuracy for the copy-move forged cases taken from CoMoFoD Database where (a-e) are forged cases and (f-g) are forgery detected cases by presented methodology. Below is the box plot graph for Sensitivity, Specificity and accuracy.

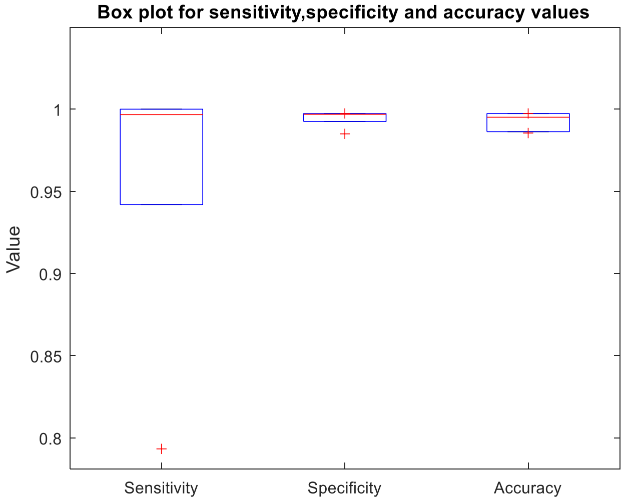


Fig 5:- Box Plot Graph For the Parameters

A box plot graph is shown in above fig 5. It represents the range b/w the maximum and minimum values for the parameters sensitivity, specificity and accuracy. One can see that the maximum value for the sensitivity is 1 and minimum value is 0.7933. The maximum value for specificity is 0.9974 and the low value is 0.9850 and the highest accuracy value is 0.9974 and minimum value is 0.9855 which is better than the existing techniques.

It has been found that Presented method of forgery detection is effective when a patch or block of an image is copy moved to another places. As Euclidian distance gives minimum error or difference between two feature sets, an exact replica of a patch of forging can be easily detected by the Presented method. Small artefacts or noisy forged detected blocks have been eliminated using morphological operations, higher accuracy has been achieved which conforms accuracy of about 99-100 per cent. We compared the latest technique results with our technique and found that the result been better with our proposed method.

Table II- Accuracy Comparisons of Related Work

S.no	Paper	Average Accuracy
1.	Proposed Method	99.23%
2.	Rahul Dixit(2017)	98.39%
3.	Khizar Hayat(2017)	73.62%
4.	XiuliBi (2017)	96.63%
5.	Avinash Kumar(2018)	87.5%

V. CONCLUSION

Image forgery can be carried out using number of ways in which mostly likely found is copy move forgery in which we transform a small content of the image to the different image. The major drawback of existed methods is that they are time consuming as well as they are not able to detect whole copy moved portion which results in lower accuracy rate of forgery detection. The author implemented edge based detection which is overlapping block based method using Mean feature that exclude large number of blocks in matching process which decreases the computation time. Experimental Results has been taken for a number of images taken from CoMoFoD Database in which average accuracy rate reaches 98-100 % for almost all images in copy move forgery detection. Even the comparison b/w the proposed method and the existing ones is showing more accurate results. The presented method has yet to be tested for compressed images that may be considered as future work.

References

[1]Birajdar GK, Mankar VH (2013) Digital image forgery detection using passive techniques: a survey. Digit Invest: 226–245

[2]Chauhan A (2015) Digital watermarking-revisit. J.ComputSciInfTechnol 6(1):833–838

[3] Kumar Sunil, Desai Jagan, and Mukherjee Shaktidev, “DCT-PCA Based Method for Copy-Move Forgery Detection” Published in: ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India- Vol II pp 577-583

[4] J. Li, X. Li, B. Yang and X. Sun, "Segmentation-Based Image Copy-Move Forgery Detection Scheme," Published in: IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 507-518, March 2015.

[5] B. Ustubioglu, G. Ulutas, M. Ulutas& V. V. Nabiyev, “Improved copymove forgery detection based on the CLDs and colour moments” Published in: Journal The Imaging Science Journal Volume 64, 2016 - Issue 4, Pages 215-225.

[6]Huan Wang, Hong-Xia Wang, Xing-Ming Sun, Qing Qian, “A passive authentication scheme for copy-move forgery based on package clustering algorithm” Published in: Multimedia Tools and Applications May 2017, Volume 76, Issue 10, pp 12627–12644

[7] Mostafa Mokhtari Ardakan, Masoud Yerokh, Mostafa Akhavan Saffar, "A New Method to Copy-Move Forgery Detection in Digital Images Using Gabor Filter", Fundamental Research in Electrical Engineering pp 115-134, 2018

[8] Avinash Kumar, Choudhary Shyam, Prakash, Sushila Maheshkar, Vikas Maheshkar, "Markov Feature Extraction Using Enhanced Threshold Method for Image Splicing Forgery Detection", Smart Innovations in Communication and Computational Sciences pp 17-27, 2018

[9] Neelesh Kumar Jain, Neeraj Kumar Rathore, Amit Mishra, "An Efficient Image Forgery Detection Using Biorthogonal Wavelet Transform and Improved Relevance Vector Machine", Wireless Personal Communications August 2018, Volume 101, Issue 4, pp 1983–2008

[10] Alaa Hilal, Samer Chantaf, "Uncovering copy–move traces using principal component analysis, discrete cosine transform and Gabor filter", Analog Integrated Circuits and Signal Processing August 2018, Volume 96, Issue 2, pp 283–291

[11] Rahul Dixit, Ruchira Naskar and Aditi Sahoo," Copy–Move Forgery Detection Exploiting Statistical Image Features." published in IEEE , 2017, pp-2277-2281

[12]Zupancic, D. Tralic, S. Grgic, and M. Grgic, “CoMoFoD-New database for copy–move forgery detection,” in 55th IEEE International Symposium ELMAR 2013

[13]Khizar Hayat, Tanzeela Qazi," Forgery detection in digital images via discrete wavelet and discrete cosine transforms", in journal of Computer & Electrical engineering, vol.62 in 2017.

[14] Weiqi Luo, Jiwu Huang and Guoping Qiu, "Robust Detection of Region-Duplication Forgery in Digital Image," Published in: 18th International Conference on Pattern Recognition (ICPR'06), Hong Kong, 2006, pp. 746-749.

[15] X. Bo, W. Junwen, L. Guangjie and D. Yuewei, "Image Copy-Move Forgery Detection Based on SURF," Published

in: 2010 International Conference on Multimedia Information Networking and Security, Nanjing, Jiangsu, 2010, pp. 889-892.

[16] X. Kang and S. Wei, "Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensics," Published in: 2008 International Conference on Computer Science and Software Engineering, Wuhan, Hubei, 2008, pp. 926-930

[17] Xiaojun Tong, Yang Liu, Miao Zhang, Yue Chen, “A novel chaos-based fragile watermarking for image tampering detection and self-recovery” Published in: Signal Processing: Image Communication Volume 28, Issue 3, March 2013, Pages 301-308

[18] Yuenan Li, “Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching” Published in: Forensic Science International Volume 224, Issues 1–3, 10 January 2013, Pages 59-67.

[19] V. Christlein, C. Riess, J. Jordan, C. Riess and E. Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches," in IEEE Transactions on Information Forensics and Security, vol. 7, no. 6, pp. 1841-1854, Dec. 2012

[20] N Kanwal, A Girdhar, L Kaur, JS Bhullar," A Taxonomy and Analysis of Digital Image Forgery Detection Techniques," in Journal of Engineering, Science & Management Education, vol.10, in 2017

[21] N Kaur, N Kanwal, " Review and Analysis of Image Forgery Detection Technique for Digital Images," in International Journal of Advanced Research in Computer Science, vol.8, in May 2017

[22] Xiuli Bi, Chi-Man Pun," Fast Reflective Offset-Guided searching Method for Copy-Move Forgery Detection", in Information Science, vol.418-419, in 2017.