International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Joint Forensic System to Detect Image Forgery using Copy Move Forgery Detection and Double JPEG Compression Approaches

Dhara Anandpara[1], Rohit Srivastava[2]

[1, 2]Computer Engineering Department, Parul Institute of Engineering and Technology, Vadodara, India

Abstract: ***With advent of many powerful editing tools in the digital image processing, image forgery is the big concern today in Digital Forensics Industry. Image forgery can be apply either in single image by coping some region of image and pasting it to another place in the same image or in composite image by combining two or more images together. The focus of my research work is to develop a forensic system to detect both type of forgery within a single place. Many Copy-move Forgery Detection (CMFD) algorithms have been developed to detect forgery within single image but are not robust to geometric transformation. Double JPEG compression is used extensively for localization of regions for composite images forgery such as Image Slicing, In-painting etc. A proposed system is a fusion based system which will allow to detect the image tampering using both techniques i.e. CMFD and DJPG. This gives insights of using both image detection algorithms within same image and in single framework so that detection is evident at single place. A system will compute a likelihood map to indicate the forged area that is accrued due to Copy. To reduce computational cost of system features are extracted from taking the mean value of DCT (discrete cosine transform) coefficients. The proposed scheme is not only robust to copy-move forgery, but also to blurring or nosing adding and with low computational complexities.***

Keywords: Digital Image Forensics, image forgery detection, manipulation detection, copy-paste forgery detection, tampering detection.

1. Introduction

1.1 Problem definition

Due to the availability of higher solution digital cameras, hi-tech personal computers, powerful software and hardware tools in the image editing and manipulating field, it become possible for someone to create, alter and modify the contents of a digital image and to violate its validation. Fake images are many times used to publicize in social medias and news papers. Many cases are noted in regard to the defaming business as well as political leaders by using fake photos and videos. For e.g. in Figure 1, image which is now-a-days passing in social media as Mr. Barack Obama, an American President very interestingly watching Narendra Modi on TV, which is totally forged and altered with actual picture which was taken before 3 years in which Obama is seen watching a televised speech by the then Egyptian President Hosni Mubarak in the Outer Oval office. This makes, it very essential to know about the integrity of the photos so as to detect the truth.

1.2 Literature survey

Digital image forgery detection methods are categorized into active and passive (blind) methods. In Active method, digital image require preprocessing treatment such as watermark embedding or signature generation at the time of digitalization, that may limit their application in practice[1]. Unlike active approach methods, passive approach does not have prior information of image.

Figure 1: A forged lower image in which American president watching Narendra Modi's speech on TV. This is forged by original Upper image.

Our main focus is on passive images, where forgeries in images are detected with no information. Many approaches are formulated in passive approach, but can be categorized in two ways. One of the way is forgery done within image (copy-paste of region within same image). This is commonly known as CMFD method (Copy – Move Forgery Detection) is useful in detecting the image tampering and region extraction of tampering within single image.

To find copy move forgery (CMFD) many researchers have used square blocks (exact match) for matching purpose. Fridrich [14] used DCT-based features instead of exhaustive search to detect region duplication, which is more effective, but their method is sensitive to variations in duplicated regions owing to additive noise. Later, Huang et al. [15] improved the performance by reducing the feature vector in

dimension; however, they failed to consider the multiple copy-move forgery. In [11], Popescu proposed a new method by adopting the PCA-based feature, which can endure additive noise, but the detection accuracy is low. Bayram et al.[16] applied Fourier-Mellin transform (FMT) to each block, FMT values are finally projected to one dimension to form the feature vector. [4] took the advantage of the SIFT features to detect the duplication regions and their experiments show the robustness of their approach. Yet, the methods mentioned above have higher computational complexity, since the quantized square blocks are directly used for matching, that the dimension of feature vector is higher, hence, affecting the efficiency of detection, especially when dealing with high-resolution digital images.
Another approach of passive image is getting it done through JPEG compression artifacts. Double-compression in JPEG images occurs when a JPEG image is decompressed to the spatial domain and then resaved with a different (secondary) quantization matrix. We call the first quantization matrix the primary quantization matrix. JPEG recompression artifacts are also one of the important characteristics to localize probability of forged area. Such artifacts are classified into two classes [2], i.e. aligned and non-aligned. After recompression, if DCT (discrete cosine transformation) is aligned with first compression it is aligned double JPEG compression (A-DJPC) where second case is known as non-aligned double JPEG compression (NA-DJPC). For A-DJPC, starting from [17], recompression produces artifacts and discontinuity in histogram in forged image, to detect region. In [18], leading to performance improvement and accuracy by drawing the probability matrix. For NA-DJPC, BACM (block artifact characteristic matrix) [19] is given to detect blocking artifact of 8 X 8 blocks. But all of above methods only work on JPEG type of images. Double-compressed images are also frequently produced during image manipulation. By detecting the traces of recompression in individual image segments, we can be able to identify the forged region because the non-tampered part of the image will exhibit traces of double-compression [3] .

1.3 Proposed system

Because of above limitations of CMFD and DJPG techniques, we develop a more general proposed system, which operates independently for any kind of forgery apply on both single and composite images. The proposed system will be the software framework which will allow system to detect the image tampering using both techniques i.e. CMFD and DJPG. This gives insights of using both image detection algorithms within same image and in single framework so that detection is evident at single place. The rest of the paper is organized as follows: in Section 2 the proposed approach is described. Section 3 gives some experimental results and gives the corresponding analysis. Conclusion is drawn in Section 4.

2. Proposed Approach

2.1 System flow

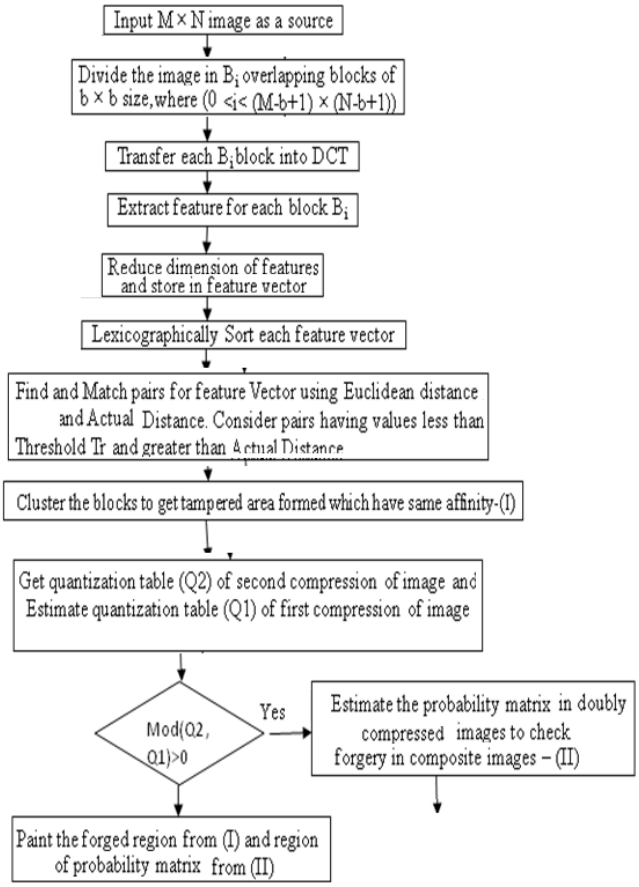

Figure 2: System flow

- Divide image into blocks: The image of size M X N is divided into blocks. For each blocks, apply DCT and get two things: i) Feature vector by mean of each sub-block divided into four region ii) get DCT co-efficients of each block of image and get traces of recompression through histogram.
- Lexicographical Sorting and probability matrix:-Sort each feature and compute the Euclidean distance of neighbor vectors. Filter out pairs above Threshold and get positions of each block. For each DCT coefficients, build probability matrix (PO) for each DCT co-efficients
- Detect suspected region and draw probability matrix: For all matched pairs and with probability matrix, paint the detected forged area having block with same affinity. Probability matrix will give probable forged region in case image splicing, computer content forgery etc. while matched pairs will give accurate forgery within image.

2.2 Dataset of images

We have built the data set comprising of images of PNG, JPG formats. A dataset of original images with different resolution is taken from different sources as below:

- PNG images taken from [14], used for research purpose. About 20 images are taken for testing purpose of size 128 X 128 pixels.

- JPEG images taken from [1], are used as benchmark database for research purpose. There are about 100 images in the benchmark database, from that we have used about 30 image set of different resolution of about 1000 X 1024 pixels, 512 X 512 pixels, 960 X 960 pixels.
- Images taken from Sony CyberShot (7.2 MP). 20 images of size 480 X 640 pixels are shot of JPEG format.

In order to do tampering and forgery in image, 3 different types of image forgery is taken up in order to support the proposed work.

- Tampering within image: Images of PNG format are tampered using MATLAB, where portion of image is copied and pasted within image and then again saved (using Matlab's imwrite function).
- Tampering for generating composite image: Here, JPEG images with QF1 is opened and portion of uncompressed PNG from different image is replaced. Finally overall "manipulated" image is JPEG compressed (again in MATLAB) with another given quality factor QF2. In all dataset, QF1and QF2 are taken from the set [50, 60…. 90] and [55,… 95] respectively for each 30 tampered images of different resolution.
- Tampering of combination within image and composite image: PNG images are tampered where portion of image is copied and pasted within image and save in JPEG format using quality factor QF1. Then, portion of different image (PNG or JPEG format) is replaced and save in JPEG format with QF2. 30 images of different resolution is built for forgery detection.

3. Experimental Result and Analysis

We use Photoshop 8.0 to modify the images and all tests are carried out on MatlabR2009a and executed on a computer of CPU 1.8GHz with main memory 1GB and secondary storage memory of 160 GB. We used sub-block and divided block into four segments, then taken the average energy of each segments. Compared to other literatures given in [10], [11] and [12], feature dimensions are reduced to 4. Table 1 gives comparison with them.

Table 1 Comparison of Feature Dimension

Literature	*Extraction Method*	*Feature Dimension*
[10]	DCT (Exact Match)	64
[11]	PCA	32
[12]	Improved DCT	16
Ours	MEAN OF BLOCKS	4

3.1 Single image forgery detection results

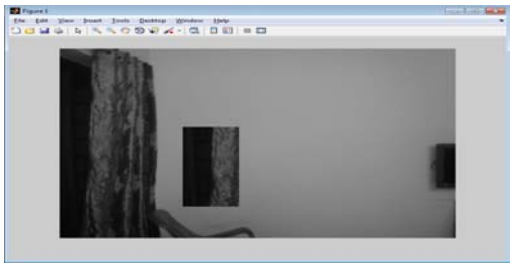

Figure 3: tampered image where a portion of curtains is copied and pasted at different place.

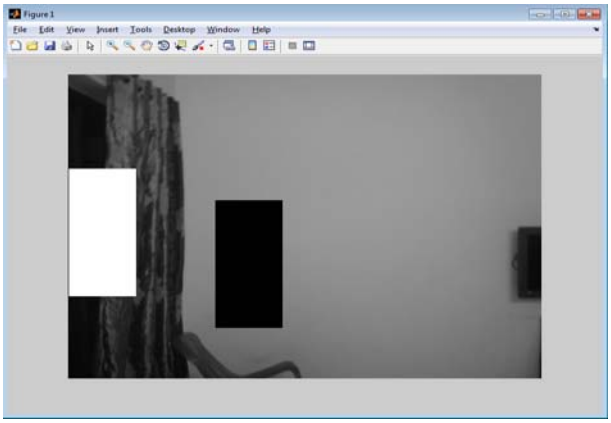

Figure 4: Shows the detection result

Here tampered area is displayed as black portion and copied area with white portion. This method uses copy-move forgery detection to detect the results.

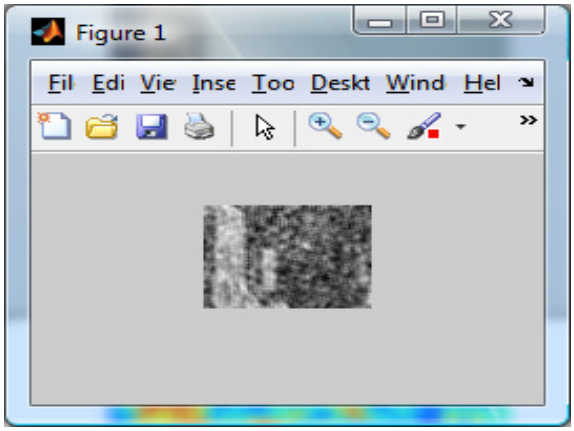

Figure 5: Shows the detection result of the tampered area by using double JPEG compression method Here, results are not evident compared to copy-move forgery detection method.

From figure, 3 to 5, shows that our algorithm can locate the tampered regions within image soundly, despite there are large and similar regions in the image. Moreover, if we see the result, if there is tampering done within image, copy-move algorithm gives the substantial results compared to double JPECT compression results.

3.2 Composite image forgery detection results

Figure 6: Shows the tampered image of the car, where portion of another image is copied and paste as well as copy of wheel portion is replaced in top-right area to do tampering

within image. This is example of image tampering within image as well as multiple images as source.

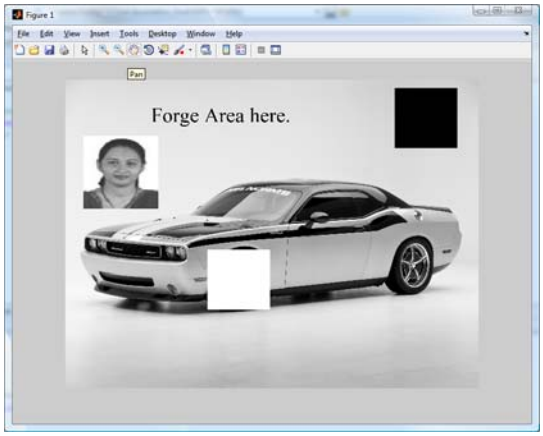

Figure 7: Result of Copy-move forgery detection method. Which identify duplicate regions but cannot identify the portion which is copied from another image.

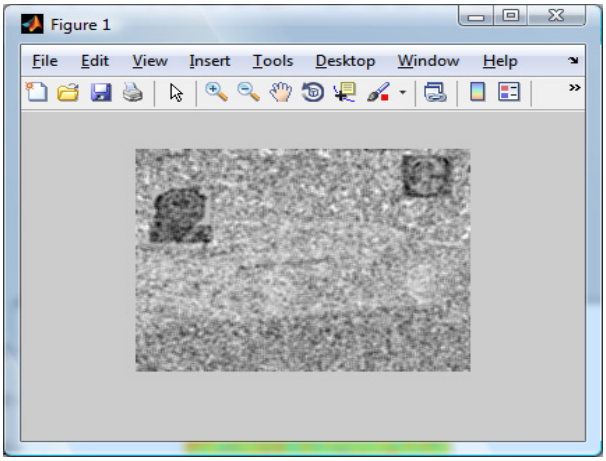

Figure 8: Result of DJPG method which identify the portion which is copied from another image.

Figure 9: tampered image of fonts where a text has been copied and before pasting it is rotated by 90̊.

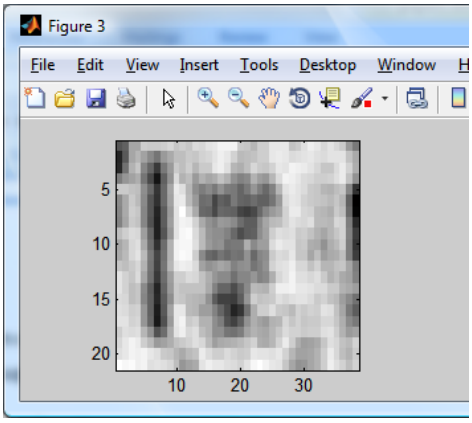

Figure 10: Result of fig 9.

Table 2: Comparison of methods to get the results

Size of an image	*Time taken to get result in second*		
	CMFD method	*DJPEG method*	*Proposed method*
128 × 160	0.112137	3.2	2.5
400 × 159	0.248835	5.64876	5.7566
400× 300	0.409662	5.79026	6.80001
1920 × 1440	7.032354	30.34526	30.111344
2560 ×1920	7.51167	80.11009	90.345561
3264 × 2448	13.866463	150.4455	200.66778

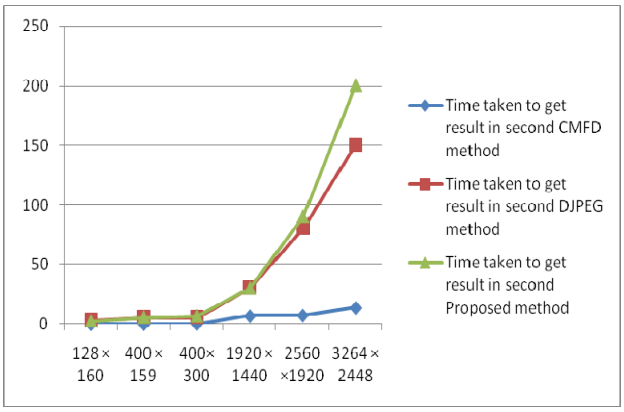

Figure 11: shows the as the image size increases computational time increases

From this with proposed work algorithm, there is exponential increase in the time taken to detect the tampering as the image size increases. The computation time for DCT co-efficients and getting probability matrix makes the proposed work with performance hit. However, a proposed work gives the complete forensic scenario to detect on one single platform. Further work can be enhance to work with other copy move approaches like DWT, PCA etc so that it compensate overall all inabilities of each algorithm.

4. Conclusion and Future work

We have presented an efficient and automatic image forgery detection method for detecting Copy-Move as well as image splicing type of forgery. Compare with previous methods such as given in [1], this approach used less features to represent each blocks. The experiments show that the proposed method detects duplicate area with any type of geometric transformation. Thus, we believe this method can give a little contribution to the area of forensic science. I believe that future work will be on the performance to

reduce computational complexity that proposed system may carry forward. This is important aspect because to get outcome of forged area of any kind of forgery, proposed system need to execute both the technique at the same time.

References

[1] V. Christlein, C. Riess, J. Jordan, and E. Angelopoulou "An Evaluation of Popular Copy-Move Forgery Detection Approaches" IEEE, Vol. 7, No. 6, DECEMBER 2012
[2] J. Redi, W. Taktak, and J.-L. Dugelay, "Digital image forensics: A booklet for beginners," *Multimedia Tools Applicat.*, vol. 51, no. 1, pp. 133–162, Jan. 2011.
[3] B. Tiziano, P. Alessandro, "Image Forgery Localization via Block-Grained Analysis of JPEG Artifacts", IEEE Trans on Info forensics and Security, Vol. 7, No. 3, June 2012
[4] Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, and G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 1099–1110, Sep. 2011.
[5] S. Battiato, G. Maria, E. Messina, and G. Puglisi, "Robust Image Alignment for Tampering Detection", ", IEEE Trans on Info forensics and Security, Vol. 7, No. 4, Aug 2012
[6] Xiang Hua Li1, Yu Qian Zhao, Miao Liao, Frank Y Shih and Yun Q Shi "Detection of tampered region for JPEG images by using mode-based first digit features" EURASIP Journal on Advances in Signal Processing 2012
[7] Tiziano B. and Alessandro P., "Image Forgery Localization via Block-Grained Analysis of JPEG Artifacts", IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, June. 2012
[8] Huang H, Guo W, Zhang Y "Detection of copy-move forgery in digital images using SIFT algorithm". IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, 2008
[9] Bertalmio M, Sapiro G, Ballester C, Caselles V (2000) Image inpainting. In: Proc. Computer Graphics, SIGGRAPH 2000, pp 417–424
[10] J. Fridrich, D. Soukal, and J. Luk, "Detection of copymove forgery in digital images," Proc. Digital Forensic Research Workshop, Cleveland, OH, August 2003
[11] Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions", Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, 2004.
[12] Y.Huang, et al., "Improved DCT-based detection of copy-move forgery in images", YForensic Science International,2011, 178–184
[13] Y. Cao, T.Gao, L. Fan, Q. Yang "A robust detection algorithm for copy-move forgery in digital images", Forensic Science International 214 (2012) 33–43
[14] Fridrich, et al., "Detection of Copy-move Forgery in Digital Images", 2003.
[15] Y. Huang, et al., "Improved DCT-based detection of copy-move forgery in images", Forensic Science International 206 (1–3) (2011) 178–184.
[16] S. Bayram, H.T. Sencar, N. Memon, An efficient and robust method for detecting copy-move forgery, in: IEEE International Conference on Acoustics, Speech and Signal Processing, IEEE Press, New York, 2009.
[17] X. Fg and G. Doer, " JPEG recompression detection", in Media orensics and Security II, Feb. 2010, vol. 7541, Ser. Proc. SPIE, pp. 75410J–75410J-12.
[18] T. Bianchi, A. D. Rosa, and A. Piva, "Improved DCT coefficient nalysis for forgery localization JPEGimages," in *Proc. ICASSP 2011*,May 2011, pp. 2444–2447.
[19] Z. Fan and R. de Queiroz, "Identification of bitmap compression history JPEG detection and quantizer estimation," *IEEE Trans. Image Process.*, vol. 12, no. 2, pp. 230–235, Feb. 2003.

Author Profile

Dhara Anandpara is pursing as Masters of Engineering (Computer) degree in Parul Institute of Technology, Vadodara (Gujarat – India). She has received her Bachelor in Engineering (Computer) from Vyavasayi Vidya Pratishthan Engineering college, Rajkot (Gujarat – India) in year 2006. She was head of department (H.O.D) in Parul Institute of Technology, Vadodara before she started her Masters of Engineering (Computer). Her area of interest is Image Processing, Data Mining and Computer Graphics.