March-April 2020
ISSN: 0193-4120 Page No. 2043 - 2048

Hybrid DCT based Approach for Duplicate Region Detection

Punam S. Raskar
Dept. of E & TC, SCOE Pune Savitribai Phule Pune University, Pune, India
punamraskar4@gmail.com
Sanjeevani K. Shah
Dept. of E & TC, SKNCOE Pune Savitribai Phule Pune University, Pune, India
skshah@sinhgad.edu

Article Info
Volume 83
Page Number: 2043 - 2048
Publication Issue:
March - April 2020

Article History
Article Received: 24 July 2019
Revised: 12 September 2019
Accepted: 15 February 2020
Publication: 18 March 2020

Abstract

Identification of even minor modifications in images belongs to an intensifying branch of multimedia forensics. Numerous solutions have been identified and employed to detect the common attacks made to tamper the image. Copy-Move is most commonly used attack chosen by forger to tamper the image. Detection of copy-move is mainly carried out by using block matching and key-point based methods. This paper proposes hybrid framework for copy-move tamper detection. This hybrid approach combines traditional Discrete Cosine Transform and Principal Component Analysis (DCT-PCA) based feature extraction. The proposed method is evaluated for 8x8 and 16x16 block size and effectively works for both block sizes. K-means clustering is used for block division which is faster than other techniques block clustering algorithms. Results show that, overall accuracy of the system is increased by applying K-means clustering approach. Experimental analysis indicates that system can handle various attacks successfully such as Translation, Rotation, Distortion and Combination of two or more transformations. Proposed system gives 90% success rate with minimum execution time.

Keywords – *Copy-Move Forgery, DCT, K-means, Image Forensics, Region Duplication*

I. INTRODUCTION

In the rapid development of the technology, numerous smart gadgets have been developed for acquisition of images, audio and videos. Images are main source of information in various sectors such as military, sports, journalism, social media, commercial, entertainment etc. to convey the information. In this wireless era images can share very easily using different apps. In fact most of the people use images for online marketing of their product. However, authenticity and integrity of images are in troubled due to various easily operated and low cost editors. Images shared over wireless media are questionable, whether it is original or fake. People having bad intention can tamper images using various image editors. Thus security and authenticity of such images are one of the important issues which need to be address in today’s multimedia world. Various methods have been developed to address these issues. The techniques are primarily categorized as Active and passive. Active methods need watermark for false finding detection in an images. Passive approaches don’t need any reference for tamper detection. Ng. et al. [1] suggested challenges and techniques to detect image forgery.

Continuing segments of the paper are structured as follows. Section II give details about related work with respect tamper detection in images. Various techniques implemented so far for fast copy-move attack recognition are discussed in the third section. Section IV illustrates experimental results and comparative analysis. The conclusion and upcoming scope is discussed in last section .

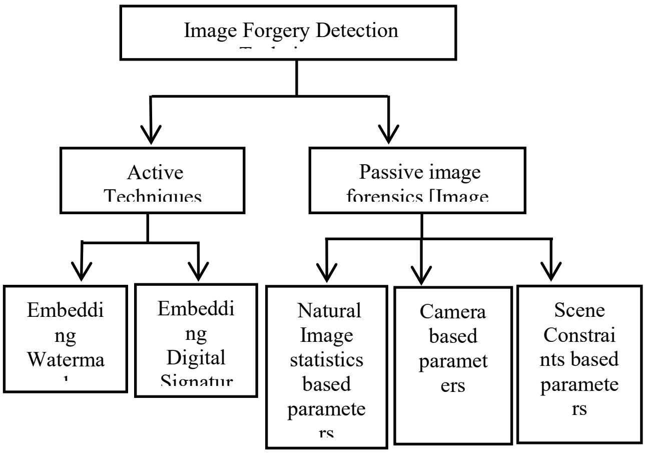


Image Forgery Detection
Active Techniques
Passive image forensics [Image
Embedding Waterma
Embedding Digital Signatur
Natural Image statistics based parameters
Camera based parameters
Scene Constraints based parameters

Fig. 1. Classification of image forensic methods

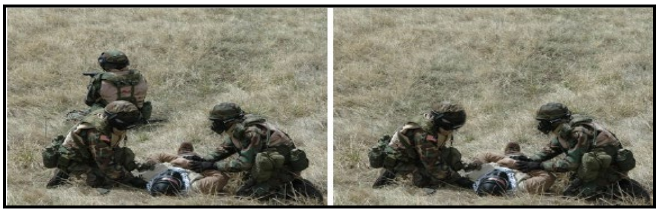


Fig. 2. Simple Copy-move attack

Many forensic investigator and researchers have developed approaches and techniques to deal with copy-move attacks mentioned above. Block and key point based methods are currently in practice to find the tamper detection in images. Figure 2 shows simple example to depict copy-move forgery [13], wherein first picture is original image and second is fake image. These kinds of attacks change the contents of image and hence information, which mislead the person by concealing the truth. Work carried out to discover copy-move attack is explored in the next section

II. Relates work

Copy-Move attack is carried out by stealing the objects from the image and placing it to the another location in the same image in order to modify the entrails of that image. Block based approach uses techniques such as Discrete Cosine Transform (DCT), Stationary wavelet transforms (SWT), Patch match, triangle matching method, discrete wavelet transforms (DWT) etc. Block based method to find copy-move attack by computing DCT was first introduced by Fridrcih [2]. This work was demonstrated on lossy JPEG image. Method found robust when retouching and en-hancement carried out for tampering. In [3] dyadic wavelet transform (DyWT) and DCT is implemented and tested for various size of images. In [4] RANSAC was used for block matching in image stabilization operation for videos. Error rate was reduced to great extent due to application of RANSAC. Pan [5] used key-point based method for feature extraction and RANSAC for feature matching. Key-point features unresponsive to geometrical and light distortions for tamper detection are extracted by using Scale Invariant Feature Transform (SIFT). Zhao [6] suggested identical image match by developing progressed RANSAC- SIFT algorithm. The work proposed by them was highly applicable in mobile robots for identification, tracking and location of target. Fadl [7] suggested DCT based for-gery detection along with k-means clustering for block matching. The system was little robust to compression, blurring and rotation. Azra [8] carried the same research with radix sort as a distinguished method for feature matching and k-means for clustering. They got fair accuracy with less execution time compare to [7]. Kumar [9] proposed DCT-PCA based combined approach for discovering copy-move tamper detection. They are the first to introduced PCA with DCT for feature extraction. Experimentation was carried for various block sizes and execution time is compared with [2].

III. Proposed Method

This section describes proposed method used for detection of coy-move attacks. Scheme of the proposed framework is discussed detailed in following steps. The major contribution of proposed framework is developing hybrid approach which uses traditional DCT-PCA along with K-means clustering and lexicographical sorting for feature matching and sorting process. By taking advantage of these algorithms; proposed technique performs superior amongst state-of-art methods.

1. First step is the conversion of input color image to gray image.
2. B*B overlapping blocks are formed by taking gray input image.
3. Apply DCT and PCA for feature extraction.
4. Formation of cluster using K-means.
5. Apply lexicographical sorting.
6. Highlight the forged region by discarding unmatched blocks.

A. Gray Scale Conversion

Initially input image is converted to gray image by using formula shown by equation 1. If the gray image denoted by I then,

$$I = 0.288R+0.587G+0.114B \quad (1)$$

B. Block Partitioning

The gray image is input to this stage. Gray image is further into overlapping blocks. In this work we have selected three different blocks size i.e. 4x4, 8 x 8, 16 x 16 for experimentation. If the size image is of x * y, then no. of overlapping blocks b x b can be calculated by equation no 2, where OB are the total blocks that can be computed.

$$OB = (x-b+1) \times (y-b+1) \quad (2)$$

C. Feature Extraction using DCT-PCA

DCT coefficients play vital role in feature extraction. In this step features are extracted by applying DCT to each block having block size 'b'. This can be computed by applying forward 2D-DCT to get zigzag order coefficients of DCT which reshapes b x b blocks. Here low frequency components are down sampled which makes DC component almost zero. Then property of PCA applied further to reduce the vector dimensionality. Value of 'd' will decide coefficients to be retained. So the resultant matrix 'A' by applying PCA and lexicographical sorting can be represented by modifying equation 2 as:

$$(x- b+1) \times (y- b+1) \times db^2 \quad (3)$$

D. Clustering using k-means

In this stage clustering is carried out by using k-means algorithm on feature sets computed by DCT-PCA. The clusters are formed based on heuristic which identifies centroid seeds. Objects are assign to cluster based on minimum distance of object from centroid. K-means used here is faster than traditional hierarchical approach.

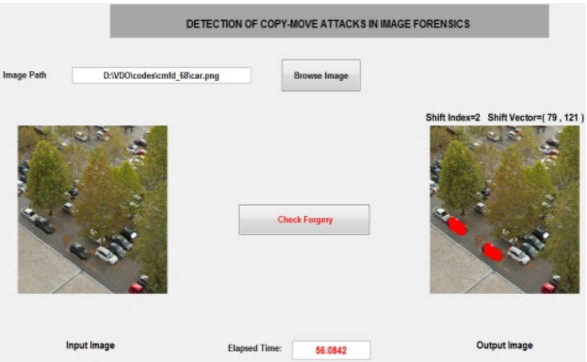
E. Forgery Detection and localization

Correlation is then computed between the sorted blocks of an image. This correlation is compared with the predetermined threshold value. After removing false matches, forged region is highlighted on the basis of matched pairs. Generally clusters containing three or more matching pairs are considered for highlighting forged region.

IV. Experimental Results and analysis

The proposed framework is executed using MATLAB 2018a on Core i3 processor having 4 GB RAM with 64-bit OS. The comparative analysis is carried out by selecting three kinds of block sizes; 4x4, 8x8, and 16x16. Performance of proposed algorithm tested on forged images taken from dataset provided in [12]. We got worst results for 4x4 block size. Hence research carried forward with only 8x8 and 16x16 block sizes. Experimentation was conducted on 60 images for calculating evaluation metrics such as True Positive (tp), True Negative (tn), False Negative (fn) and False Positive (fp). Proposed technique is also evaluated on the basis of execution time with various methods discussed in the paper. The sample results of copy-move tamper detection are presented in figure 3.

A. Sample Outcomes of proposed system



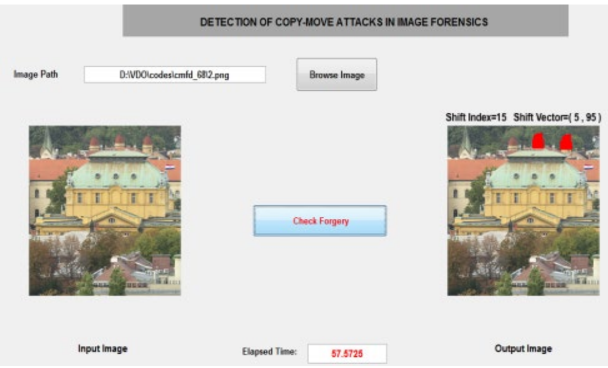
DETECTION OF COPY-MOVE ATTACKS IN IMAGE FORENSICS

Image Path: D:\VDO\codes\cmfd_68\car.png

Shift Index=2 Shift Vector=(79 , 121)

Elapsed Time: 56.0842

Fig. 3 (a) Car.png- combination



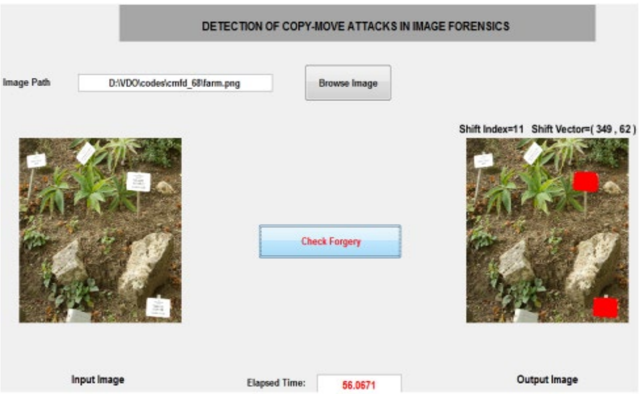
DETECTION OF COPY-MOVE ATTACKS IN IMAGE FORENSICS

Image Path: D:\VDO\codes\cmfd_68\2.png

Shift Index=15 Shift Vector=(5 , 95)

Elapsed Time: 57.5725

Fig. 3 (b) temple.png- Translation



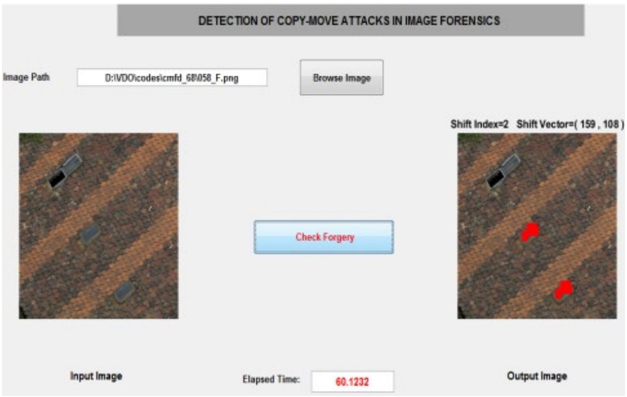
DETECTION OF COPY-MOVE ATTACKS IN IMAGE FORENSICS

Image Path: D:\VDO\codes\cmfd_68\farm.png

Shift Index=11 Shift Vector=(349 , 62)

Elapsed Time: 56.0671

Fig. 3 (c) farm.png- Distortion



DETECTION OF COPY-MOVE ATTACKS IN IMAGE FORENSICS

Image Path: D:\VDO\codes\cmfd_68\058_F.png

Shift Index=2 Shift Vector=(159 , 108)

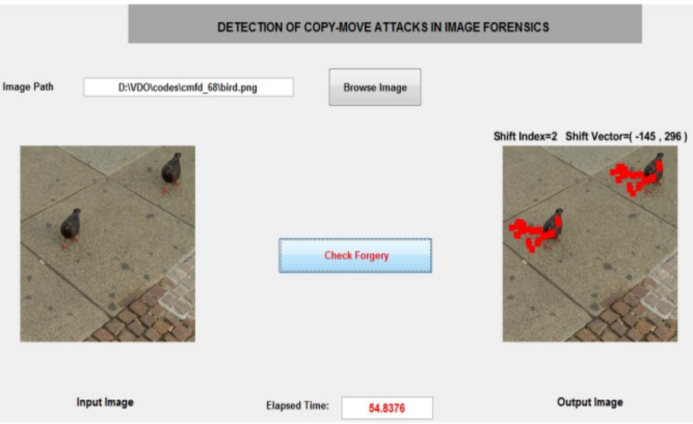
Elapsed Time: 60.1232

Fig. 3 (d) Roof.png- Rotation

The proposed algorithm is tested for five types of copy-move attacks: Combination, Translation, Rotation, Distortion and Scaling. An algorithm works effectively and accurately for all types of attacks except scaling. Experimentation is carried out on 60 forged images. Statistics for evaluative measures are illustrated in table 1.

Table I. Evaluative Measures For Attacks

Attack	tp	tn	Fn	fp
Translation	59	58	2	1
Rotation	56	55	5	4
Distortion	60	59	1	0
Combination	60	59	1	0
Scaling	50	52	8	10



DETECTION OF COPY-MOVE ATTACKS IN IMAGE FORENSICS

Image Path: D:\VDO\codes\cmfd_68\bird.png

Shift Index=2 Shift Vector=(-145 , 296)

Elapsed Time: 54.8376

Fig. 4. Bird.png- Scalling

B. Observations and Comparative Study

Figure 3 (a, b, c, d) shows sample outcomes of proposed method for Combination, Translation, Distortion and Rotation attack respectively. Figure 4 shows example of scaling which is less robust. From table 1 it is clear that algorithm after computing evaluative measures proposed system is robust to Translation, Rotation, Distortion and combination. However it shows less robustness to scaling and gives ideal results for plain copy-move images. Proposed method is also tested for execution time for images downloaded from [12] having 512 x 512. Experimental analysis shows that proposed system is much faster, since average execution time for forgery detection is 56 sec. which less compare to [10]. Comparative analysis for the block size, feature extraction, clustering and fine matching is studied as shown in table 2. Sunil et al. [8] implemented DCT only successfully for all three block sizes. Later this research was extended using PCA for two block sizes. Parveen et al. also used DCT for extracting features for 8x8 block size along with K-means clustering. Proposed method is implemented using DCT-PCA and K-means clustering for 8x8 and 16x16 block size successfully.

TABLE II. COMPARATIVE STUDY BETWEEN PROPOSED METHOD AND STATE-OF-ART

Sr. No	State-of-art	Block Size	Method of Feature Extraction	K-means Clustering
1	Sunil et al. [8]	4x4,8x8,16x16	DCT	X
2	Sunil et al. [9]	4x4, 8x8	DCT-PCA	X
3	Parveen et al. [10]	8x8	DCT	√
4	Das et al. [11]	Sub bands	SWT	X
5	Proposed Method	8x8, 16x16	DCT-PCA	√

Form experimental analysis and outcomes demonstrates that, proposed framework is strong method than SWT. Block size is one of the crucial factors in the process of feature extraction, when we increase the block size; it takes long time for execution. However, proposed system got fair accuracy for both block sizes 8x8 and 16x16 with less execution time. Accuracy, Sensitivity and Specificity are considered to check the performance of this work. Performance parameters are calculated as below,

Method	Accuracy (%)	Sensitivity (%)	Specificity (%)
Only DCT	88	93	94
SWT [11]	93	90	96
Proposed method	95	94	95

1. Accuracy = (tp+tn) / (tp+fp+tn+fn)
2. Sensitivity = tp / (tp+fn)
3. Specificity = tn / (tn+fp)
4. Success Rate = tp / (tp+fp+fn)

TABLE III. PERFORMANCE MERTICS COMPARISION

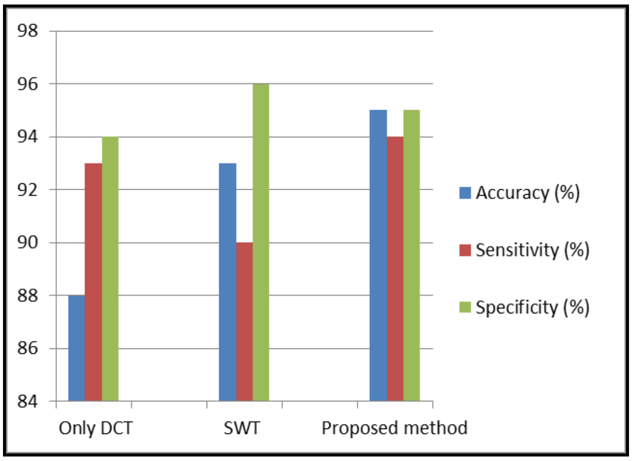


Fig.5 Graphical representation of comparison

Table 3 illustrates comparative scheme of different techniques. Proposed system is compared for three performance parameters listed above with two other methods. Initially we have implemented region duplication by applying DCT only (results are shown in table 3). Outcomes of proposed system are matched with existing SWT method proposed by Das et al. [11] and only DCT. Proposed framework gives better Accuracy than SWT. Proposed system works satisfactorily for all performance parameters. Figure 5 depicts the graphical analysis for different methods for three evaluating measures Accuracy, Sensitivity and Specificity. Proposed framework gives balanced performance in comparison with rest two algorithms used for the comparative analysis.

V. Conclusion

A new framework for the detection of copy-move attack by applying hybrid approach is proposed in this paper. Feature extraction is carried out by DCT-PCA for 8x8 and 16x16 block size, K-means is used for fast clustering. This combination gives robust detection with less execution time. Proposed system is also tested against various transformation attacks such as Translation, Distortion, Rotation, and Combination. Proposed framework handles all attacks successfully except some cases for scaling with 90% success rate. Compression and image splicing is further scope for this research work with variety of image size.

VI. References

[1] Ng, T. T., Chang, S. F., Lin, C. Y., & Sun, Q.: Passive-blind image forensics. In Multimedia security technologies for digital rights management (pp. 383-412). Academic Press, (2003).

[2] Fridrich, J., Soukalm, D., Lukáš, J.: Detection of copy-move forgery in digital images. In: Digital Forensic Research Workshop, Cleveland, OH, pp. 19–23 (2003) Oxford: Clarendon, 1892, pp.68-73 Aug. (2003).

[3] Muhammad, G., Hussain, M., Mirza, A. M., & Bebis, G.: Dyadic wavelets and DCT based blind copy-move image forgery detection, IET Conference on Image Processing IPR (2012).

[4] Liu, K., Qian, J. and Yang, R..: Block matching algorithm based on RANSAC algorithm. In International Conference on Image Analysis and Signal Processing (pp. 223-227). IEEE, (2010).

[5] Pan, X. and Lyu, S.: Region duplication detection using image feature matching. IEEE Transactions on Information Forensics and Security, 5(4), pp.857-867,(2010).

[6] Zhao, M., Chen, H., Song, T. and Deng, S.: Research on image matching based on improved RANSAC-SIFT algorithm. In International Conference on Optical Communications and Networks, (pp. 1-3). IEEE,(2017).

[7] Fadl, S.M., Semary, N.A.: A proposed accelerated image forgery copy–move forgery detection. In: Proceedings of Visual Communications and Image Processing Conference, pp. 253–257, (2014).

[8] Kumar, S., Desai, J. and Mukherjee, S.: A fast DCT based method for copy move forgery detection. IEEE Second International Conference on Image Information Processing, (pp. 649-654). IEEE, (2013).

[9] Sunil, K., Jagan, D. and Shaktidev, M..: DCT-PCA based method for copy-move forgery detection. In ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol II (pp. 577-583). Springer, Cham, (2014).

[10] Parveen, A., Khan, Z.H. and Ahmad, S.N.: Block-based copy–move image forgery detection using DCT. Iran Journal of Computer Science, 2(2), pp.89-99, (2019).

[11] Das, T., Hasan, R., Azam, M.R. and Uddin, J.: A robust method for detecting copy-move image forgery using stationary wavelet transform and scale invariant feature transform. In International Conference on Computer, Communication, Chemical, Material and Electronic Engineering (IC4ME2) (pp. 1-4). IEEE, (2018).

[12] Tralic D., Zupancic I., Grgic S., Grgic M.: CoMoFoD - New Database for Copy-Move Forgery Detection. In Proc. 55th International Symposium, pp. 49-54, September (2013).

[13] Christlein, V., Riess, C., & Angelopoulou, E. (2010). : A study on features for the detection of copy-move forgeries. Sicherheit 2010. Sicherheit, Schutz und Zuverlässigkeit.