DOI: http://dx.doi.org/10.26483/ijarcs.v9i1.5255

Volume 9, No. 1, January-February 2018

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

COPY MOVE FORGERY DETECTION USING FFT COEFFICIENTS AND MORPHOLOGICAL OPERATIONS

Nancy Sahota
Research Scholar
Department of Computer Science & Engineering
Asra College of Engineering and Technology
Bhawanigarh, Punjab, India

Er. RajnishKansal
Assistant Professor
Department of Computer Science & Engineering
Asra College of Engineering and Technology
Bhawanigarh, Punjab, India

Abstract: Nowadays, digital images have been used in many areas such as a evidence in a courtroom or for insurance claim, in a scientific fraud, within the medical patient history etc. Development of new powerful image editing software is also increasing parallel to increase on the usage of images in daily life. Two approaches to ratifying the authenticity of a digital image can be categorized as active and passive (blind).The active approach does not use actual digital content. Unlike the active approach, digital image forensics (also called passive image forensics) is a form of image analysis for finding out the condition of an image without the need for a priori information (such as embedded watermarks or signatures). The objective of copy-move forgery is to hide vital and useful information or data and perform region duplication in some section of an image. In this work, block based feature extraction has been proposed in which Fast Fourier Transform (FFT) coefficients has been evaluated for non-overlapping blocks at each pixel neighborhood for similarity matching. First of all, mean has been evaluated for each block and each block is put into a particular box of four pixel intensities such that 256 intensity values has been divided into 64 categories . After those FFT coefficients has been used for similar matching in which the Euclidean distance and the actual coordinate distance of the two blocks has been used so that different matching locations can be detected. Based on these location, whole image is divided into two categories i.e. Forged and non-forged area. For better accuracy morphological operations has been implemented on the segmented forged pixels so that noisy or mis-detected forgery areas can be eliminated. Proposed method gives 99-100% accuracy in copy move forgery detection

Keywords: Fast Fourier Transform (FFT), Euclidian distance, CMFD, Block-based etc.

1. INTRODUCTION

These days, because of the progression of computerized image preparing programming and altering instruments, animage can be effortlessly controlled and adjusted [1]. It is exceptionally troublesome for people to distinguish outwardly whether the image is unique or controlled. There is quick increment in carefully controlled phonies in prevailing press and on the Internet [2]. This pattern shows genuine vulnerabilities and abatements the validity of advanced images. In this way, creating strategies to confirm the uprightness and genuineness of the advanced images is vital, particularly considering that the pictures are exhibited as confirmation in an official courtroom, as news things, as a piece of restorative records, or as budgetary reports. In this sense, image imitation recognition is one of the essential objectives of picture forensics [3].

Approaches for Digital image forgery detection

1)Active Approach

In active approach, the advanced image requires preprocessing of image, for example, watermark inserting or signature age, which constrains their application practically speaking.

2)Passive Approach

Passive image forgery detection techniques roughly can be divided into five categories, these are: Pixel Based Techniques, Format Based Techniques, Camera Based Techniques, Physical-env. Based Techniques, Geometry Based Techniques

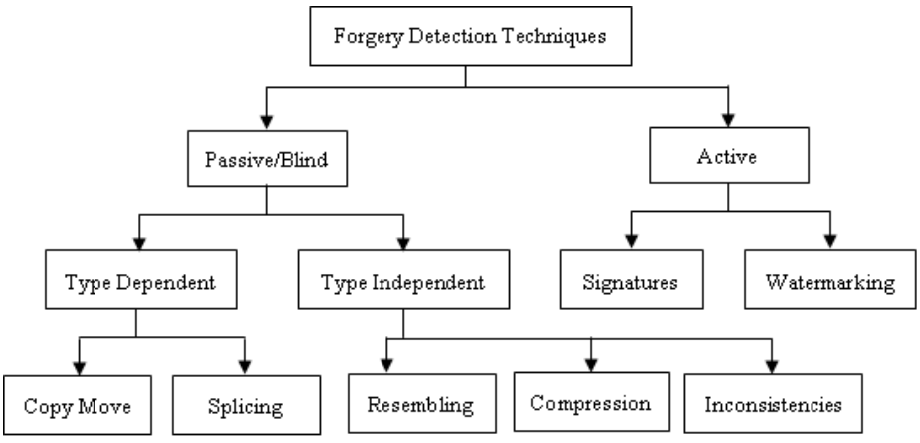

Figure 1: classification of Image forgery detection techniques

Image Forgery Detection based on Pixel

1)Cloning (Copy-Move)

This is the most widely recognized sort of image imitation and this is otherwise called duplicate move phony. In the duplicate move a piece of the image is reordered elsewhere inside the image.

2) Resampling (Resize, Stretch, Rotate)

To make a composite of two people it might be possible that one person may have to be resized, stretched to match the relative height of other people. So this process needs to resample original image into a new sampling lattice [4].

2. LITERATURE REVIEW

Kumar et. al. [5]presented that SIFT gives high performance in terms of correctness and robustness. Whereas ORB is faster than SIFT, SURF in terms of time. Although key-point based techniques have better time complexity and robustness to post-processing operations like scaling and rotation, there are some shortcomings as well.

Asgharet. al. **[6]**discussed in detail two popular types of image forgeries (copy-move and splicing) and provided the critical analysis of the state-of-the-art methods developed to detect and localize copymove and splicing forgeries.

Yuan et al. [7] proposed A *Multi-Level Dense Descriptor* (*MLDD*) extraction method and a Hierarchical Feature Matching method to detect copy–move forgery in digital images.

Ustubiogluet. al. [8]proposed an enhanced duplicate move fabrication location technique in light of shading minutes and CLDs in their paper. Shading minutes are utilized to bunch covering obstructs as per their shading comparability.

Grantyet. al. [9]presented an efficient method for image retrieval and detection of copy-move forgery and the resultant performance of the same was discussed. Images were retrieved by sparsification of graph Laplacian using spectral hashing and copymove forgery was detected by spectral-hashing-based Polar Cosine Transform.

Sun et al. [10] proposed a scheme to detect the copy-move forgery in an image, mainly by extracting the key points for comparison.

Shaktidev et al.[11]In their paper, they studied that copy move forgery detection has many issues. There are many techniques suggested to detect such type of tampering with the original image but, many issues still remained either unsolved or there is a lot of scope for performance improvement.

Ansari et. al. [12]surveyed and talked about different methodologies of pixel-based picture falsification recognition. Every one of the strategies and methodologies examined in this paper can identify fraud.

Chen et al.[13] proposed a novel watermarking approach to provide enhanced tampering localization and self-recovery. A cross chaotic map is used to confuse the blocks generated by the original image.

3. GENERAL PROCESS OF COPY-MOVE FORGERY DETECTION

The general process of copy-move forgery detection used in earlier approaches consists of the following steps.

Step 1 Divide the input image into overlapping blocks.

Step 2 Produce feature vectors from blocks using FFT coefficients.

Step 3 Sort the blocks using feature vectors by taking mean of the blocks.

Step 4 Find duplicate vectors using similarity matching based on Euclidian distance and co-ordinates of the blocks.

Step 5 Perform block matching.

Step 6 Apply post processing operations i.e. dilation, erosion in order to detect the forgery.

Steps for passive copy-move and splicing forgery detection

The following are the major steps of the general framework for passive copy-move and splicing forgery detection in images.

Image preprocessing: Before feature extraction, some operations are performed on images to enhance the structural changes that have occurred in images due to forgery, such as transforming an RGB image into suitable color space, conversion to gray scale, in order to decompose an image into frequency-scale components for better description of the geometrical information of the texture of an image.

Feature extraction: The goal of feature extraction is to compute the specific representation of the data that can highlight relevant information. The dimension of the feature space constructed by the feature extraction techniques may be prohibitive, can involve redundant information and can cause the efficiency of a classifier to deteriorate.

The feature selection process is then used to reduce system complexity and time complexity by eliminating the insignificant features before classification. In these FFT coefficients has been used as feature extraction phase.

Forgery Area detection: An appropriate classifier or similarity measure is selected or designed and is then trained on the training set of images. During the training phase the parameters of a classifier are tuned. In this Euclidian distance has been used as a similarity matching of the features of the two blocks

4. RESULT AND DISCUSSIONS

1. Dataset

Tampered images used in the experiment has been shown below

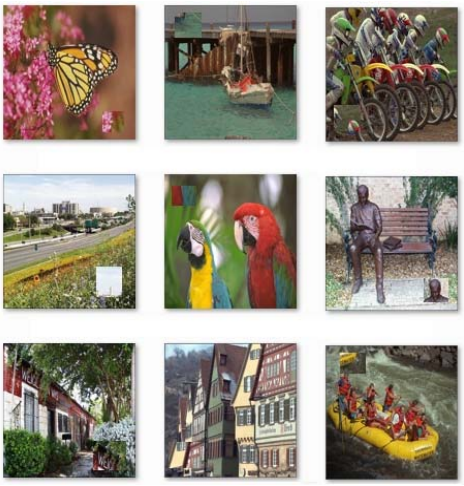

Figure 2: A set of tampered images

5. RESULT AND DISCUSSIONS

In this section, screenshots has been provided for variety of images using existed and proposed method.

Figure 3: Input image

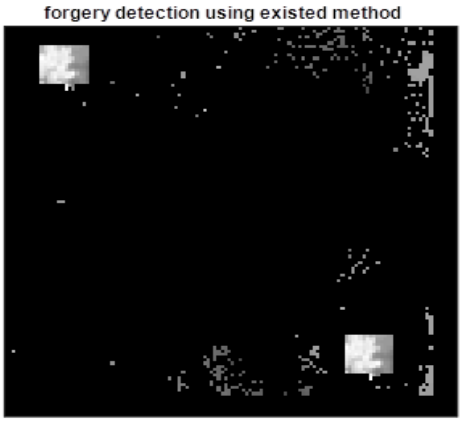

Figure 4: Forgery detection by DCT method before post processing

Figure 5: Forgery detection by DCT method after post processing

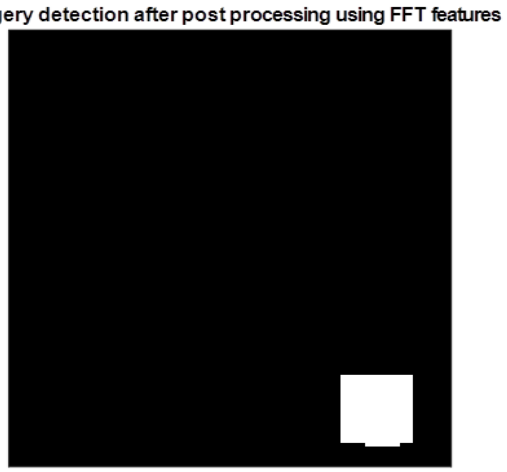

Figure 6: Forgery detection by FFT method after post processing

Table 1: Forgery detection evaluation using sensitivity, specificity and accuracy parameters

Parameters and method used	Sensitivity	Specificity	Accuracy
DCT based forgery detection	99.906	45	98.498
FFT based forgery detection	99.937	100	99.9389

Below are the bar graphs for sensitivity, specificity and accuracy parameters for the other images

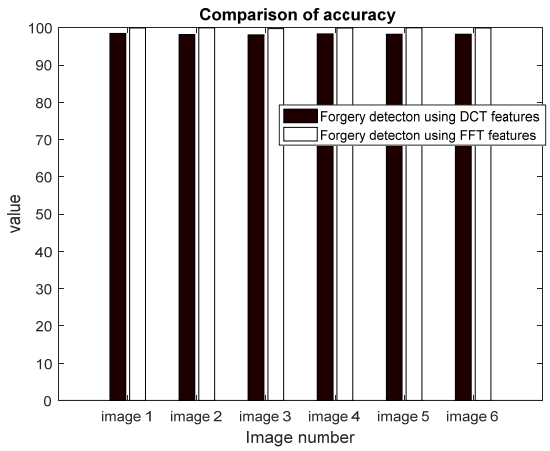

Figure 7: Comparison of accuracy

It has been found that proposed method of forgery detection is effective when a patch or block of an image is copy moved to another places.The FFT is a useful computational tool that provides an efficient means for detecting directionality or periodicity in the frequency domain. An image is a spatially varying function. The Fourier method is useful in converting a spatial description of an image in terms of image frequency components. The FFT method works recursively by dividing the original vector into two halves, computing the FFT of each half, and then putting the results together. 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 proposed method. Small artefacts ornoisy forged detected blocks have

been eliminated using morphological operations, higher accuracy has been achieved which conforms accuracy of about 99-100 per cent.

6. CONCLUSION

Copy-move is a common method for image forgery. It works without any digital watermarks or signature information.There are many techniques suggested to detect such type of tampering with the original image but, many issues still remained either unsolved or there is a lot of scope for performance improvement. The most commonly used algorithm to detect such type of tampering is block matching algorithm. Robustness against post processing operations and the time taken by the detection techniques are few of the major challenges. Change of intensity of the copy moved part is one of the post processing operations that may be employed by the attacker to evade the image forgery detection methods. This is successfully addressed in the proposed algorithm. Fast Fourier Transform and morphological operations has been used has been used to represent and compress the feature vector of overlapping blocks respectively and Euclidian distance has been used for similarity matching for forgery detection. It has been concluded that proposed method is effective when there is copy move type of forgery in the same image and gives 99-100 accuracy in forgery detection of pixels.

REFERENCES

[1] Judith A. Redi, WiemTaktak, Jean-Luc Dugelay, "Digital image forensics: a booklet for beginners" Published in: Multimedia Tools and Applications January 2011, Volume 51, Issue 1, pp 133–162

[2] WANG Jun-Wen, LIU Guang-Jie, ZHANG Zhan, DAI Yue-Wei, WANG Zhi-Quan, "Fast and Robust Forensics for Image Region-duplication Forgery" Published in: ActaAutomaticaSinica, Vol. 35, no. 12, pp. 1488, 95, Dec. 2009.

[3] 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

[4] J. Granty Regina Elwin, T. S. Aditya and S. Madhu Shankar, "Survey on passive methods of image tampering detection," 2010 International Conference on Communication and Computational Intelligence (INCOCCI), Erode, 2010, pp. 431-436

[5] Sunil Kumar & Swati Nagori, “Key-point based copy-move forgery detection in digital images” Published in: Journal of Statistics and Management Systems Volume 20, 2017 - Issue 4, Pages 611-621

[6] KhurshidAsghar, ZulfiqarHabib& Muhammad Hussain, “Copy-move and splicing image forgery detection and localization techniques: a review” Published in: Journal Australian Journal of Forensic Sciences, 2017 Volume 49, Issue 3, Pages 281-307.

[7] Xiuli Bi, Chi-Man Pun, Xiao-Chen Yuan, “Multi-Level Dense Descriptor and Hierarchical Feature Matching for Copy–Move Forgery Detection” Published in: Information Sciences Volume 345, 1 June 2016, Pages 226-242

[8] 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.

[9] Regina Elwin J Granty& G Kousalya, “Spectral-hashing-based image retrieval and copy-move forgery detection” Published in: Australian Journal of Forensic Sciences Volume 48, 2016 - Issue 6, Pages 643-658.

[10] 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

[11] 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

[12] MohdDilshad Ansari, S. P. Ghrera&VipinTyagi , “Pixel-Based Image Forgery Detection: A Review” Published in Journal IETE Journal of Education Volume 55, 2014 - Issue 1

[13] 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