Ch Priyanka* et al.
(IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH
Volume No.6, Issue No.6, October - November 2018, 8994-8996

# Blur-Invariant Copy-Move Forgery Detection Technique With Improved Detection Accuracy Utilizing SWT-SVD

**CH PRIYANKA**
M. Tech student, Dept of ECE, Siddhartha Institute of Engineering And Technology, Hyderabad, TS, India.

**T NAGARAJU**
Assistant Professor, Dept of ECE, Siddhartha Institute of Engineering and Technology, Hyderabad, TS, India.

*Abstract*— **With the increase in interchange of data, there is a growing necessity of security. Considering the volumes of digital data that is transmitted, they are in need to be secure. Among the many forms of tampering possible, one widespread technique is Copy Move Forgery (CMF). This forgery occurs when parts of the image are copied and duplicated elsewhere in the same image. There exist a number of algorithms to detect such a forgery in which the primary step involved is feature extraction. The feature extraction techniques employed must have lesser time and space complexity involved for an efficient and faster processing of media. Also, majority of the existing state of art techniques often tend to falsely match similar genuine objects as copy move forged during the detection process. To tackle these problems, the paper proposes a novel algorithm that recognizes a unique approach of using Hu's Invariant Moments and Log-polar Transformations to reduce feature vector dimension to one feature per block simultaneously detecting CMF among genuine similar objects in an image. The qualitative and quantitative results obtained demonstrate the effectiveness of this algorithm.**

*Keywords*—**Copy Move Forgery; Hu's Moments; Log-Polar Transformations; Region Duplication Forgery;**

## I. INTRODUCTION

With the advancements in imaging technologies, the digital images are becoming a concrete information source. Meanwhile, a large variety of image editing tools have placed the authenticity of images at risk. The ambition behind the image content forgery is to perform the manipulations in a way, making them hard to reveal through the naked eye, and use these creations for malicious purposes. For instance, in 2001, after the 9/11 incident, several videos of Osama bin Laden over the social media were found counterfeited through the forensic analysis [1]. In the same way, in 2007, an image of tiger in forest forced the people to believe in the existence of tigers in the Shanxi province of China. The forensic analysis, however, proved the tiger to be a "paper tiger" [2]. Similarly, in 2008, an official image of four Iranian ballistic missiles was found to be doctored, as one missile was revealed to be duplicated [3]. Hence, the famous saying "seeing is believing" [4] is no longer effective. Therefore, ways that can ensure the integrity of the images especially in the evidence centered applications are required.

In recent years, an exciting field, digital image forensics, has emerged which finds the evidence of forgeries in digital images. The primary focus of the digital image forensics is to investigate the images for the presence of forgery by applying either the active or the passive (blind) techniques. The active techniques such as watermarking and digital signatures depend on the information embedded a priori in the images. However, the unavailability of the information may limit the application of active techniques in practice . Thus, passive techniques are used to authenticate the images that do not require any prior information about them.

## II. LITERATURE REVIEW

Fridrich et al proposed the first CMFD algorithm using exact match technique where every pixel was counted as a feature and robust CMFD algorithm using DCT coefficients as features of the blocks. Huang et al [2] improved the DCT algorithm to compute the results faster. Farid and Popescu [3] proposed an algorithm to detect CMFD using considerably less feature vector dimension using Principle Component Analysis (PCA) algorithm. Kang et al proposed an algorithm to curb copy move forgery using Singular Value Decomposition (SVD) algorithm which was effectively robust against induced noise. Zhang et al used Discreet Wavelet Transform (DWT) to reduce the complexity of the program as compared to the other existing schemes. Yang et al [3] used Dydadic Wavelet Transform by decomposing the forged image into four sub-bands and removing the low frequency components in it. Muhammad et al [7] proposed a similar algorithm using DyWT which was capable of utilizing both low and high frequency components in an image to eliminate as many false positives as possible. Rahul et al [8] proposed a blur invariant CMFD technique using SWT-SVD algorithm. A method using Fourier

  

Mellin Transform was developed in which proved to be efficient in detecting forgery in highly compressed images. Guangjie et al proposed an algorithm using Hu's invariant moments, proving its robustness against several post processing techniques. Huang et al proposed an algorithm using DWT and SVD for robust feature extraction. The PCA algorithm was further developed by Sunil et al [3] to increase its robustness to JPEG compression and noise using DCT-PCA algorithms. PCA is mainly used to reduce the feature vector dimension in the given matrix.

## III. PROPOSED METHOD

We now propose a novel algorithm to reduce the feature vector dimension and simultaneously making the algorithm more effective in differentiating between similar objects in image and actual copy move forgery detection using Hu's invariant moments and log-polar transformations. This algorithm can be discussed in detail as follows:

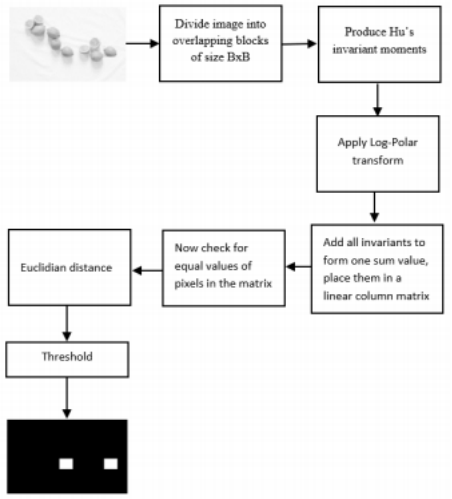


**Fig. 1 Proposed Block Diagram for Copy Move Forgery Detection**

Input: Copy Move Forged image.

Output: Binary image showing the regions of duplication.

1. Input the forged image of size M x N, convert it to grey scale.

2. Divide the image into overlapping blocks of size B x B.

3. Calculate Hu's invariant moments for each of the divided blocks in step 2 up to 7th order.

4. Apply the log-polar transformation over each of the Hu's invariant moment order.

5. Use 'format long' in MATLAB to check on every value up to its respective 15th decimal.

6. Calculate the sum of all 7 invariant moments produced for each block and write this value into a new linear column matrix.

7. Add two additional columns to the matrix formed in step 5 indicating the location of the corresponding block's first pixel.

8. Lexicographically sort the formed matrix.

9. Now check if adjacent rows first value is the equal up to 15th decimal digit.

10. If the values match, check the number of times a value is repeating. Also, compute the Euclidean distance between the matching blocks.

11. Apply user specified threshold to eliminate false matches.

12. Create a binary image with one's in the duplicated regions as a result of detecting the forgery.

The previous state of art CMFD process using Hu's invariant moments used moment values up to 4th order as features of each block, mainly because of the reason that the value of Hu's invariant moments above 4th order generally tend to go beyond 10-6 units reducing its impact over generation of features. Generation of four invariant moments sufficed the purpose of distinguishing the block among others. In this paper, we propose an algorithm where all the computed Hu's moments are summed to produce one feature value that can distinguish the block from other blocks. Summing up to only 4 th order moments leads to several false matches. Therefore, in order to reduce false matches to the maximum extent, we produce 7 invariant moments and apply log-polar transform to convert the values beyond 10-6 units to significant floating values. The accuracy of identifying blocks can further be increased by using 'long format' variables which could display and compute the values generated up to 15th decimal number. Here, if the feature value's matches with one another up to 15th decimal we can have a benefit of doubt that they are duplicated regions. False matches among these are further curbed by calculating Euclidian distance among the matched blocks. The idea here is that, if a cluster of blocks are copied from a region and are duplicated in the same image, the distance between corresponding copied and duplicated block must be the same for every matched pair. A user-specified threshold is applied onto the image to eliminate singular false positives and the remaining matched regions are marked as copy-moved.

Certain feature extraction algorithms such as Scale Invariant Feature Transform (SIFT) or Speeded Up Robust Features (SURF) are commonly used for CMFD purposes. These algorithms mark the features on objects present in the image which

  

provides an advantage of having more robustness towards post processing techniques and geometrical transformations over the pasted region. Since, these algorithms concentrate their key features over objects and drastic pixel flow changes in the image, they often tend to confuse between copy move forgery and genuine similar products in the same image. Using Hu's invariant moments and log-polar transformations to calculate one feature value per block can reduce the chance of false representation over two or more genuine similar products. Hu's moments are sensitive towards the slightest changes in the pixel values which helps' us distinguish between similar products since it's practically impossible to have two or more genuine elements in an image with exactly the same corresponding matching pixels due to the influence over environmental factors, illumination factors and many more. Moments have well known applications in image processing, computer vision, machine learning and other related fields which are normally used to derive invariants with respect to specific transformation classes.

## IV. EXPERIMENTAL RESULTS


Fig. 2 Input Forgery Image

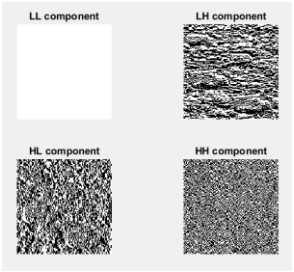


Fig. 3 After Applying 2 D-SWT a) LL component b) LH component c) HL component d) HH component

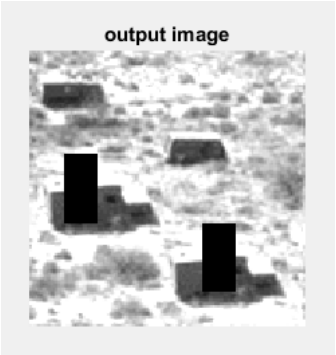


Fig. 4 output Image

## V. CONCLUSION:

Passive forensics technology of digital image is one of the rapidly growing fields of research. Our brief review of image CMFD technologies indicates that the research is still in the phase of vigorous development and has a huge potential for the future research and development applications. Two classical models of copy-move forgery and two frameworks of CMFD technologies are presented at first. Then, block-based and keypoint-based CMFD methods are reviewed from different aspects, respectively, including the classical CMFD technologies and the state-of-the-art algorithms for CMFD in recent several years. The performance evaluation criterions and frequently used datasets for evaluating the performance of the CMFD schemes are collected. The future directions of this topic are given at last. With the help of the advanced technologies, some CMFD schemes with high performance are expected to become standard tools in the future. We also hope that this survey will provide related information to scientists, researchers, and relevant research communities in this field. The investigation on image forensics is still a continual, sustainable process and it will continue to explore forensics technologies with high accuracy and robustness.

## VI. REFERENCES

[1] Photo Tampering throughout History [Online]. Available: http://pth.izitru.com/2008_07_01.html.

[2] D. Vaishnavi and T. S. Subashini, "A passive technique for image forgery detection using contrast context histogram features," International Journal of Electronic Security and Digital Forensics, vol. 7, no. 3, pp. 278-289, 2015.

[3] H. Yao, S. Wang, X. Zhang, C. Qin, and J. Wang, "Detecting image splicing based on noise level inconsistency," Multimedia Tools and Applications, vol. 76, no. 10, pp. 12457-12479, 2017.

[4] B. Bayar and M. C. Stamm, "On the robustness of constrained convolutional neural networks to JPEG postcompression for image resampling detection," in Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, New Orleans, LA, USA, 2017, pp. 2152-2156.

[5] J. Chen, X. Kang, Y. Liu, and Z. J. Wang, "Median filtering forensics based on convolutional neural networks," IEEE Signal Processing Letters, vol. 22, no. 11, pp. 1849-1853, 2015.

  