Copy-Move Forgery Detection with GLCM and Euclidian Distance Technique in Image Processing

Parul sharma, Harpreet Kaur

ABSTRACT--- The approach using which the forgery part of an image can be detected is called image forgery detection. The copy-move part of an image can be detected using copy-move forgery detection technique. The various techniques have been designed so far for the copy-move forgery detection. The techniques which are designed for the copy-move forgery detection are based on the three steps which are feature extraction, Euclidian distance and image marking. In the previous method DWT algorithm is applied for the feature extraction and Euclidian distance is calculated for the forgery part detection. The GLCM algorithm is applied in this research for the feature extraction and Euclidian distance is calculated for the pixel detection. MATLAB simulator is used to implement the proposed technique and perform evaluations by calculating various parametric values.

Keywords— Copy-move forgery, DWT, GLCM, Euclidian distance

INTRODUCTION

The technology through which raw images that are collected from cameras available on various sources can be improved such that the information that is important can be extracted from them is known as image processing [1]. Several techniques have been developed over the time within this technology to provide enhancements such that the complex data can be extracted. Several applications have been using this technology over the time. The military [2], medical and research fields [3] have been using it most widely. Personally also, several organizations have been using it to ease the human workload and perform certain activities. For enhancing the visual appearance of images, image processing is widely applied within several applications [4]. Several computations are also performed in order to prepare the images [5-6]. Digital image processing is another name of image processing. It however provides both optical and analog image processing in it [7]. Several techniques are applied in this technology, which are studied here. Imaging is defined as the image acquisition. It is feasible to perform optical and analog image processing. Several fields [8] such as computer graphics are available in this approach through which it is possible to generate images [9]. In attempt to hide the not required parts of an image, certain part of another image is cut and pasted on that image which is called copy-move forgery. Since it is very simple and highly effective, this tampering technique is used very commonly [10]. The technologies are getting advanced with each day due to which this technique is being used in several applications. Relying on the manner in which it is used, it can be either beneficial or harmful to the users [11]. It is possible to hide the real information when the fake images are generated by this tampering technique. To perform copy-move forgery [12], the textured regions are used in the form of similar color and noise variation properties from the textured regions [13]. Detecting the changes in image statistical properties is not possible for a human eye. Blurring is used on the border of modified image such that the irregularities among original and pasted region can be reduced [14].

A general framework which is applied to detect particularly this type of forgery is explained in the figure 1 shown above.

a. Pre-Processing: The type of application in which this approach is applied is the major factor of this step. The colored image is converted into gray scale and the noise is also removed from input images using image enhancement [15].

b. Feature Extraction: In order to represent in image properly, the features are identified or extracted from an input image through feature extraction process [16]. Avoiding redundancy within the original image and minimizing the dimensionality of data are the two general needs which must be available in features [17].

c. Matching: For identifying a huge similarity or matching amongst the feature descriptors, the process applied is known as matching [18]. The similarity is interpreter as a sign of duplicate area if it is identified in the image. There are several techniques proposed to perform matching.

d. Post-Processing: The transformation utilized amongst the original and the copy-moved region is identified using post-processing in case when the image is categorized as non authentic [19].

Revised Manuscript Received on May 15, 2019.

Parul sharma, Research Scholar Chandigarh University, Mohali, India. (parulsharma2095@gmail.com)

Harpreet Kaur, Assistant professor Chandigarh University, Mohali, India. (harpreet8307@gmail.com)

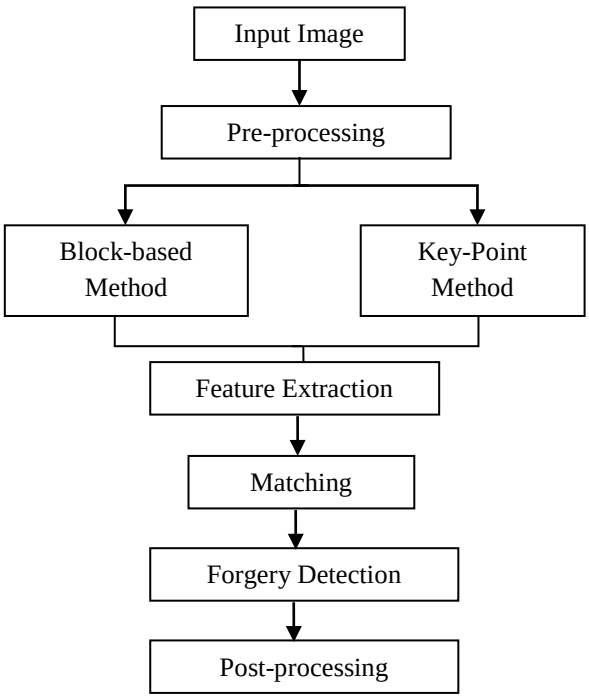


Figure 1 General Frame work for Copy-Move Forgery detection

Literature Review

Yong Yew Yeap, et.al (2018) studied about the Copy Move Forgery Detection (CMFD) technique using which images are tampered [20]. A new featuring method was proposed in this paper to improve the existing CMFD technique. Images involved in different geometrical attacks were used in this research to perform evaluations on the proposed approach. For performing evaluations on images, two different databases were used. It was seen that by applying proposed technique around 84.33% and 82.79% of accuracies were achieved for the two databases. Thus, the true positive rate was higher than 91% for the tampered images.

Yue Wu, et.al (2018) proposed a new deep neural network through which the forgery masks could be recognized and predicted easily. Recognizing the issues of copy-move forgery was possible in this proposed approach. To extract the block-like features from an image, a convolutional neural network was used in this paper. It was also possible to calculate the self-correlations in various blocks. A point-wise feature extractor was used for localizing the matching points. For the reconstruction of a forgery mask, a deconvolutional network was used [12]. It was seen through the simulation results that as compared to the results achieved by previous approach, highly efficient results were achieved when proposed approach was applied. It was highly feasible to apply proposed technique to protect the information from unknown attacks.

Geetika Gupta, et.al (2017) proposed a new approach in which the information relevant to original image was not needed. From the grayscale image, the overlapping blocks were designed [22]. For comparing the performances, the existing and proposed techniques were implemented in this research. The false matches available in previous approach were reduced by using the present offset threshold value as per the simulation outcomes. Also, it was seen that for two different attacks being induced on the proposed approach, highly efficient and better security measures were taken. It was concluded towards the end of this research that highly efficient results were achieved in terms of various performance parameters.

Dhanya R, et.al (2017) reviewed the studies performed on copy-move forgery over the previous few years. The previously designed techniques along with their proper steps were discussed in this paper. However, the existing techniques have not been applied commonly in latest applications since they have their own limitations. Thus, these techniques have a scope of improvement [23]. This technology has been facing certain major challenges. Further, for extracting the important information so that accurate values of certain parameters could be achieved, several operations were performed. Thus, a new method was designed that removed the previously mentioned limitations. It was seen that with respect to cost effective designing of image forensic applications, highly efficient results were achieved.

Hanieh Shabanian, et.al (2017) proposed a novel block-based method through which the copy-move forgery could be detected from within the digital images. The proposed method used the structural similarity as a similarity matching step such that a unique property could be provided [24]. It was possible to improve the run-time speed of the approach by applying Gaussian pyramid decomposition approach. Thus, it was possible to reduce the time-consuming issue without using any feature extraction method in the proposed approach. It was possible to simplify the calculation and analysis method by the proposed method which performed a significant specification. The efficiency was improved along with level of sensitivity as per the simulation results achieved when conducting experiments.

Rahul Dixit, et.al (2017) proposed a new mechanism using which the images could be split into overlapping blocks of fixed size. The frequency domain and the statistical features of an image are considered in this method [25]. For testing the proposed method and testifying its performance in comparison to existing algorithms, the certain metrics like DA and FPR were calculated in this paper. Based on the experiments, the proposed approach provided better results. Improvement in accuracy and false positive rate were achieved in this research.

Research Methodology

In order to perform CMF detection and localization, a technique is proposed which uses both SWT and DCT. The translation invariance and localization properties which exist within spectral and spatial domains are the major reason of choosing SWT. The translation invariant SWT is applied here to decompose the input image into four subbands. Further, the feature extraction is performed by using the overlapping blocks which are generated by dividing the approximation subband generated in previous step. The DCT is applied to each overlapping block for achieving a reduced dimension of feature. The robustness of post-

processing operations is the major reason due to which the DCT is applied on the overlapping blocks of approximation subband of SWT. Thus, the diversity of representing features increases due to the integration of SWT and DCT. Also, within CMFD, it is better to apply this integration. Following are the steps performed to develop CMFD approach:

a. Pre-processing: Following are the mathematical equations which are applied to transform the input image in question into YC_bC_r:

$$Y = \left(\frac{77}{256}\right)R + \left(\frac{150}{256}\right)G + \left(\frac{29}{256}\right)B \quad (1)$$

$$C_b = -\left(\frac{44}{256}\right)R - \left(\frac{87}{256}\right)G + \left(\frac{136}{256}\right)B + 128 \quad (2)$$

$$C_r = \left(\frac{131}{256}\right)R - \left(\frac{110}{256}\right)G - \left(\frac{21}{256}\right)B + 128 \quad (3)$$

b. Feature extraction: The detailed procedure of extracting feature is defined below:

i. SWT: DWT does not provide the property of shift invariance due to which it is not being used much currently. There are low pass l[m] and high pass h[m] filters present within the input image in case of SWT. However, no decimation is performed for achieving wavelet coefficients. LH, HL, and HH were the sub-images which denoted the horizontal, vertical and diagonal subbands, respectively.

ii. Applying DCT for reducing feature dimension: The overlapping image blocks $B_i(i = 1,2,\dots,T_b)$ are generated by applying SWT which divides the LL of the obtained image. Here, a sliding window of size $w \times h = 8 \times 8$ is also utilized.

Gray Level Co-occurrence Matrix (GLCM): The texture which includes spatial relationship of pixels is examined through the statistical method named as GLCM. The number of times certain pairs of pixels with particular values appear in a matrix is calculated by GLCM functions for characterizing the texture of an image. Thus, a GLCM is created and then the statistical measures are extracted. An N-order matrix through which the joint distribution probabilities of pixel pairs are described is called GLCM. Here, the image gray level is represented by N. At pre-processing stage, the image gray level is lowered to 8, 16 or 32 such that the computing complexity is reduced and the texture characteristics are highlighted.

For extracting texture features the matrices of co-occurrence are the most known and used. The properties of images in relevance to second-order statistics are estimated. The probability of appearance of pairs of pixel values that are localized at a distance in the image is measured using a co-occurrence matrix. For two joining pixels $P_{d,\theta}(i,j)$ where i and j are the two values with distance d and an orientation angular, the probability is defined by the matrix.

c. Feature matching and filtering: Following are steps performed here:

i. Generating feature matrix: Through the placement of all the feature vectors in relevance to the every extracted B_i, a feature matrix $\mathfrak{F}_m$ is generated which is of the size Tb × 6 as:

$$\mathfrak{F}_m = \begin{bmatrix} f_{1,z} \\ f_{2,z} \\ . \\ . \\ . \\ f_{T_{b,z}} \end{bmatrix}$$

Here, z = 1,2,…6

ii. Corresponding block pairs with high similarity: There are two different constraints employed named as block distance threshold and block similarity threshold. The requirements of CMFD approach are fulfilled as there are non-intersecting tampered regions available and there is overlapping of the image blocks.

d. Visual detection results are pre-processed: The filtered block pairs that are stored within the set Ω are utilized for generating the final required output O_i for the proposed approach. Further, in order to eliminate the falsely detected regions of O_i, the morphological opening operation is applied along with a structural element which is of width 8. The final detection results are seen generally, by highlighting all the detected pair of blocks that include original and tempered regions.

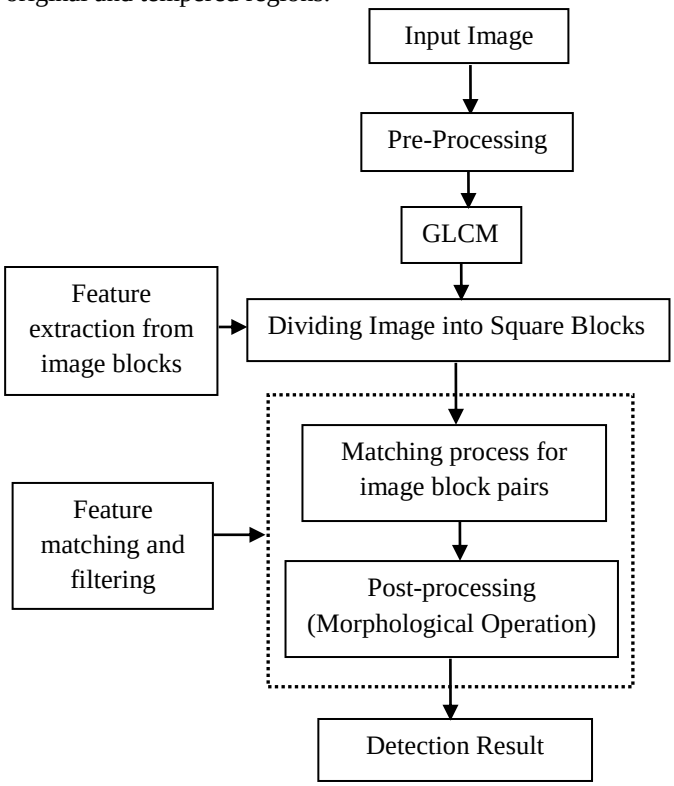


Figure 2: Proposed CMFD Technique Architecture

Result and Discussion

Copy-move forgery is detected in this research work. The dataset is collected from the different internet sources. For detecting the forgery region of image, the Euclidian distance is applied to compare pixel values of the image. In the proposed technique, features are extracted from input image using GLCM algorithm. Comparisons of proposed and existing algorithms are made with respect to PSNR, MSE and accuracy.

a. PSNR: Ratio to maximum power of possible signal to the power of corrupting noises is called PSNR. This causes great effect on the image representation. The logarithmic decibel scale is used to describe the PSNR values because there is dynamic range of different signals lies within the applications.

The Mean Square Value is used to define the PSNR values, which can be defined as:

$$PSNR = 10.log_{10}(\frac{MAX_I^2}{MSE})$$

$$= 20.log_{10}(\frac{MAX_I}{\sqrt{MSE}})$$

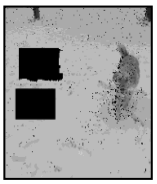
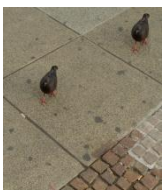
b. MSE (Mean Square Error): The standard statistical metric values which measure the error between Original Image and watermarked Image. The MSE is calculated by using below mentioned formula:

$$MSE=\frac{1}{M*N}\sum_{i=0}^{i=M-1}\ \sum_{i=0}^{i=N-1}[I\ i,j\ -\ K(i,j)]2$$

c. Accuracy: It is the parameter which describes the number of points which are correctly classified from the total number of points.

$$Accuracy = \frac{Number\ of\ points\ classified}{total\ number\ of points}$$

Table 1: Comparison Results

Forged Images	Existing method's Results	Proposed Method Results
		
		

As illustrated in table 1, the existing method results with use Euclidian distance and DWT for the forgery detection are presented. To perform feature extraction, GLCM algorithm is used in the proposed work and the results are evaluated here. It is analyzed from the pictures that proposed method detects forgery more accurately than the existing method

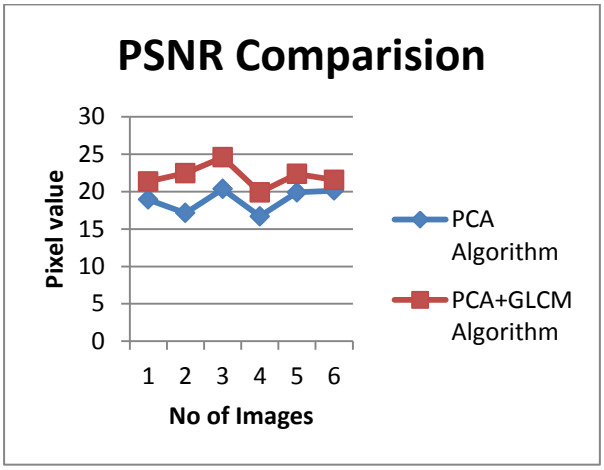


Figure 3: PSNR Comparison

Figure 3 shows the comparative analysis of proposed and existing techniques on various sets of images by calculating their PSNR value. The results show that in comparison to existing method, the PSNR value of proposed method is high.

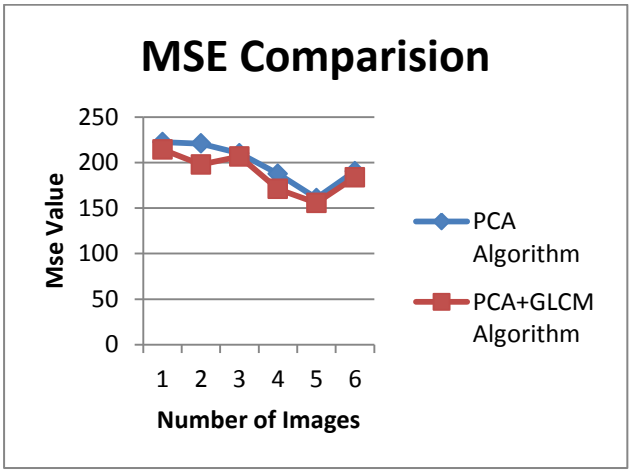


Figure 4: MSE Comparison

Figure 4 shows the comparative analysis of proposed and existing methods in terms of MSE value. The results show that in comparison to existing approach, the value of MSE for proposed approach is less.

CONCLUSION

In this paper, it is concluded that copy-move forgery detection technique has the three steps which are feature extraction, Euclidian distance calculation and forgery marking. The technique of GLCM is applied for the feature extraction which can detect the forgery part more accurately. MATLAB simulator is used to implement the proposed method and certain parametric values are calculated to analyze the results. The proposed algorithm has high accuracy, PSNR and low MSE value as compared to existing method

REFERENCES

1. X. Kang, and S. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in International Conference on Computer Science and Software Engineering, 2008, Vol. 3, pp. 92630.
2. H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," in Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Vol. 2, Dec. 2008, pp. 2726.
3. G. H. Li, Q. Wu, D. Tu, and S. J. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWTand SVD," in Proceedings of IEEE International Conference on Multimedia and Expo, Beijing, Jul. 2007, pp. 17503.
4. Wing Commander, Nimit Kaura, Dr Sunita Dhavale, "Analysis of SIFT and SURF features for Copy-Move Image Forgery Detection", 2017 International Conference on Innovations in information Embedded and Communication Systems (ICIIECS)
5. Fengyong Li, Mingquan Xin, Jinguo Li, Jiang Yu, "IMPROVED DETECTION FOR COPY-MOVE FORGERY WITH MULTI-SCALE SLIDING WINDOWS", 2017 International Symposium on Intelligent Signal Processing and Communication Systems
6. Regina Lionnie, Rizal Broer Bahaweres, Said Attamimi, Mudrik Alaydrus, "A Study on Pre-Processing Methods for Copy-Move Forgery Detection Based on SIFT", Proc. of the 2017 IEEE Region 10 Conference (TENCON)
7. Junlin Ouyang, Yizhi Liu, Miao Liao, "Copy-Move Forgery Detection Based on Deep Learning", 2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI 2017)
8. Alaa Hilal, Taghreed Hamzeh, Samer Chantaf, "Copy-Move Forgery Detection using Principal Component Analysis and Discrete Cosine Transform", 2017, IEEE
9. SHAN JIA, ZHENGQUAN XU, HAO WANG, CHUNHUI FENG, AND TAO WANG, "Coarse-to-fine Copy-move Forgery Detection for Video Forensics", 2017, IEEE
10. M. Ghorbani, M. Firouzmand, and A. Faraahi, "DWT-DCT (QCD) based copy-move image forgery detection," in 18th IEEE International Conference on Systems, Signals and Image Processing (IWSSIP), 2011, pp. 14.
11. I. Amerini et al., "A SIFT-based forensic method for copymove attack detection and transformation recovery," IEEE Trans. Inf. Foren. Sec., Vol. 6, no 3, pp. 1099111, 2011.
12. J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy move forgery in digital images," in Proceedings of the Digital Forensic Research Workshop, Aug. 2003, pp. 58.
13. A. C. Popescu, and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, 2004.
14. Mohamed A. Elaskily and Heba K. Aslan, Osama A. Elshakankiry and Osama S. Faragallah, Fathi E. Abd El-Samie, Mohamed M. Dessouky, "Comparative Study of Copy-Move Forgery Detection Techniques", 2017, IEEE, 41458-ACCS'017&PEIT'017
15. S. A.Thajeel, G. Sulong, "A survey of copy-move forgery detection Techniques," Journal of Theoretical and Applied Information Technology, ISSN: 1992-8645.
16. S. Sharmila, S. Prajakta, S. Hiral, "Image Forgery Detection Techniques for Forensic Sciences,"ijournals, ISSN-No: 2347-4890,vol 2, issue 8, August 2014.
17. Resmi S, Chithra A S, "Recent Block-based Methods of Copy-Move Forgery Detection in Digital Images," International Journal of Computer Applications (0975 – 8887) Volume 89 – No 8, March 2014.
18. J. Fridrich, D. Soukal, and J. Lukáš, "Detection of copy-move forgeryin digital images," in Proc. Digital Forensic Research Workshop,Cleveland, OH, Aug. 2003.
19. N. D. Wandji, S. Xingming, And M. F.Kue, "Detection Of Copy-MoveForgery In Digital Images Based OnDct," International Journal OfComputer Science Issues (Ijcsi), Vol.10, 2013.
20. Yong Yew Yeap, U. U. Sheikh, Ab Al-Hadi Ab Rahman, "Image Forensic for Digital Image Copy Move Forgery Detection", 2018 IEEE 14th International Colloquium on Signal Processing & its Applications (CSPA 2018)
21. Yue Wu, Wael Abd-Almageed, and Prem Natarajan, "Image Copy-Move Forgery Detection via an End-to-End Deep Neural Network", 2018 IEEE Winter Conference on Applications of Computer Vision
22. Geetika Gupta, Akshay Girdhar, "A ROBUST PASSIVE METHOD FOR DETECTION OF COPY-MOVE FORGERY IN IMAGES", 2017, IEEE
23. Dhanya R1, R Kalai Selvi, "A State of the Art Review on Copy Move Forgery Detection Techniques", Proceedings of 2017 IEEE International Conference on Circuits and Systems (ICCS 2017)
24. Hanieh Shabanian, Farshad Mashhadi, "A New Approach for Detecting Copy-Move Forgery in Digital Images", 2017, IEEE
25. Rahul Dixit, Ruchira Naskar and Aditi Sahoo, "Copy–Move Forgery Detection Exploiting Statistical Image Features", IEEE WiSPNET 2017

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication