DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4316

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

AUTHENTICATION BASED IMAGE FORGERY DETECTION USING OPTIMIZED FEATURES IN JPEG IMAGES

Amandeep Kaur, Isha Vats
Department of Computer Science and Engineering
PTU, Punjab, India

Abstract: With the current development in technology, image manipulation and particularly image splicing has been termed as a regular and established concern. The swift growth in commercial image editing programs and software for instance Adobe Photoshop has significantly elevated the number of forged, doctored and tampered images on a daily basis. This situation has resulted into extreme consequences, minimizing the authenticity and reliability of such images as well as creating untrue beliefs in a wide range of ideal-world relevance. The authenticity of a digital image suffers from severe threats due to the rise of powerful digital image editing tools that easily alter the image contents without leaving any visible traces of such changes. The splicing forgery can be done by copied a one/more region from source image and pasted into a target image to produce a composite image called spliced image. Therefore, this type of forgery is considered very challenging from tampering detection point of view. To make the matter worst some post-processing effects such as blurring, JPEG compression, rotation and scaling maybe introduced in the spliced image. In previous paper, we study found the problems in forgery detection in Jpg images. Robust feature extraction techniques used in block based copy move image forgery detection require a high computation time. There is a need for reduced computation time for detection schemes to be practical for use with large images and in real time environments. Utilization of GPU to compute the processes can highly parallelize the tasks involved to reduce computation time. Current CPU based algorithms that have been designed are not suitable to be directly adopted in a GPU based scheme. It must be determined how a parallel copy move image forgery detection scheme can be designed for use with a GPU. Digital images provide a new way to represent pictures and scenes that only film and a darkroom could supply before. In this research work, we implement the feature extraction using principle component analysis and optimization (ant colony optimization) algorithm to detect the forgery image in JPG images. In optimization approach to classify the features and match the training feature if training and testing features has matching then detect the forgery image in the jpg images. Evaluate the performance parameters PSNR (Peak Signal to Noise Ratio), Error rate Accuracy and compare the existing parameters i.e accuracy.

Keywords: Image Forgery, Robust feature extraction, Ant colony Approach and Neural Network

1. INTRODUCTION

Image Forgery has been emerging as a remarkable analysis in applications of CV (computer vision), DIP (Digital Image Processing) , technology in biomedical and forensics laboratory etc…[1] It has more impressive and experiments,(i) when software tool is powerful for image processing are so(ii) famous and popular that we can't authorize whether imagery(iii) is changed by uncovered eyes. Image Forgery detection is a single type of passive approaches using blind methods to detect suggestions of tampering in an assumed image without previous info. and security program files [2].

The image could be forgery by splicing explanations from itself, which is known as copy-move pictures or from the other pictures known as spliced pictures. Due to the modifications the corresponding detection approaches are implemented[3].

Fig 1. Image Forgery Dataset Images

In this research work., major objectives on algorithm and methods for image COPY-MOVE or duplicated and spliced identification in the existing years. Classifies them based-on the path to procedure in-put image. The classification approach could be verified into following general types:

- Move and Copy Forgery
- Image Splicing and
- Image Re-touching [4]

In this method from all of these types could be developed including as

(i) Active and
(ii) Passive

The active method is main concept with the information abstraction methods such as, watermarking and digital signatures, where in previous data is evaluated essential and integrated into the main image. Abstract the data method embed some secondary information into the main image. Normally, the image watermarking is either embedded at the interval [5] of time of the image acquisition, although special devices or advanced after further processing of the real image. However, the approach might de-grade the quality of the main image.

In passive method forgery detect are mainly categorized as being (i) Visual and (ii) Statistical. Visual techniques are a based-on visual clue that doesn't require any software tools [6].

In this research work, this thesis encompasses a set of objectives that is associated with milestone of this process. The objectives are mentioned below.

a) To collect database in forgery images and verifying the image acquisition given image, in order to connect a given image, as demonstration of origin authenticity.
b) To implement the K-mean Clustering Algorithm for divide the data in clusters index and centroid, Extraction features based component analysis and optimize the extracted features.
c) To evaluate the performance parameters in proposed work i.e PSNR, FAR and FRR, Accuracy and compare the existing performance parameters.

2. RELATED WORK

Tu K.Huynh, Thuong Le-Tien, 2015 [7], the author did their research as a survey on Image forgery which is based on both sliced and copy-move images. In this survey, author reviews select papers from last 10 years and study them to find similarity factor between them and make their survey report accordingly. The similarity factor does not depend upon the method, but here in this research, it's based on the similarity factor of problem formulation. The method followed by researchers to process images and classification of forgery part depends upon the input area of the image. According to that pre-processing and feature extraction structure changed to classify better results. This research contains the limitation of existing methods and classification problems along with their optimization in future. The whole process used to classify the better method among previous study and their future enhancement.

Tanzeela Qazi, Khizar Hayat, Samee U. Khan, 2013 [8], as in this research the technology provide various facilities and misuse ofthis technology in image manipulation become a challenging for detection of image forgery. The process of image forgery is to find the copy-move part of the actual image and classify the selected area. Tempering of images is the main issue all the time when it arises in the area of forensic verification. In this survey, the author did their research to check various methods for image forgery. Also, it covers various forgery areas.

Mohsen Zandi, Ahmad Mahmoudi-Aznaveh, 2014 [9], the author did their research to find the forgery area from the image. Various methods are there for detecting forgery from the input image. They are used to find the copied area of the image and highlight from the other part of the image. The two different techniques are used for verifying the forgery area as block processing or blocking based technique and another is copy and move. The block-based process classifies smoothly area from the input image and this process cause many negative matches from the actual input. The author proposed the adaptive method based on threshold process. It overcomes the limitation of previous methods due to nearby match of the found part in the input image. The proposed method compared to the basis of detection accuracy and negative matches. It also reduces the cost and execution time to detect the forge area.

Ramesh Chand Pandey, Sanjay Kumar Singh, and K.K.Shukla, 2014 [10], the author worked on the video processing in this research to detect the forge area of the video. This process used various pre-processing steps for the execution and other steps of classification of Forge area. As various video editing software are there for editing the videos and copy move frames. It makes this process more challenging. In the video stream, the relationship between video frames is in special segments and it makes the process easy to detect the copy and pasted frame from on to another location. It processes the frames in the bases of feature extraction process which followed by the SIFT algorithm. Proposed approach also worked with some noise reduction processes which make the image quality improved. The proposed approach detected more efficiently for temporal images and provides better results with high accuracy rate.

Ainuddin Wahid Abdul Wahab, Mustapha Aminu Bawa, 2014 [11], technology provide a various feature to modify images and videos faster and easily. This process makes the forge part detection very difficult. The author proposed a passive forgery detection procedure which processes the input data provide authentic output for the detection. This process makes the multimedia communication more secure. The proposed approach process and find the forged part if the multimedia content and also used for the pattern recognition process and information security. The proposed approach pre-process the input sample and extraction various features for checking the forged part of the input data. The proposed approach improve the forgery detection with eliminating the limitation of existing methods and provide less false recognition rate in overall output.

Condos M.Fadl, Noura A.Semary, 2014 [12], detection of forge images in a recent year becomes very popular. Due to technology enhancement and service provided by the software increases the crime rate in both image and video forgery. The author proposed a block-based matching algorithm which processes the input and provides the authentic output with forge part of the image. The proposed approach worked with other enhancement with k-mean clustering approach to find the similarity factor and divide input data into various clusters. The clustered data passed through feature extraction process to find the unique properties and forgery data from the input image. The overall output is calculated with the help of nearby method to find the similarity factor. The process classifies more efficiently and provides accurate results in 50% reduced time as in other existing approaches.

3. RESEARCH METHODOLOGY

This section presents the used tool for the simulation of results. Also a brief for the method to generate GUI is elaborated. The proposed concept of forging of digital imagery is also discussed in this section.

Step I: Upload the image from the dataset. Conversion rgb2gray scale form to reduce pixel of the image matrix and plot the histogram to define numeric data in number of bits.

Step II: Convert the RGB image into YCbCr colour space.

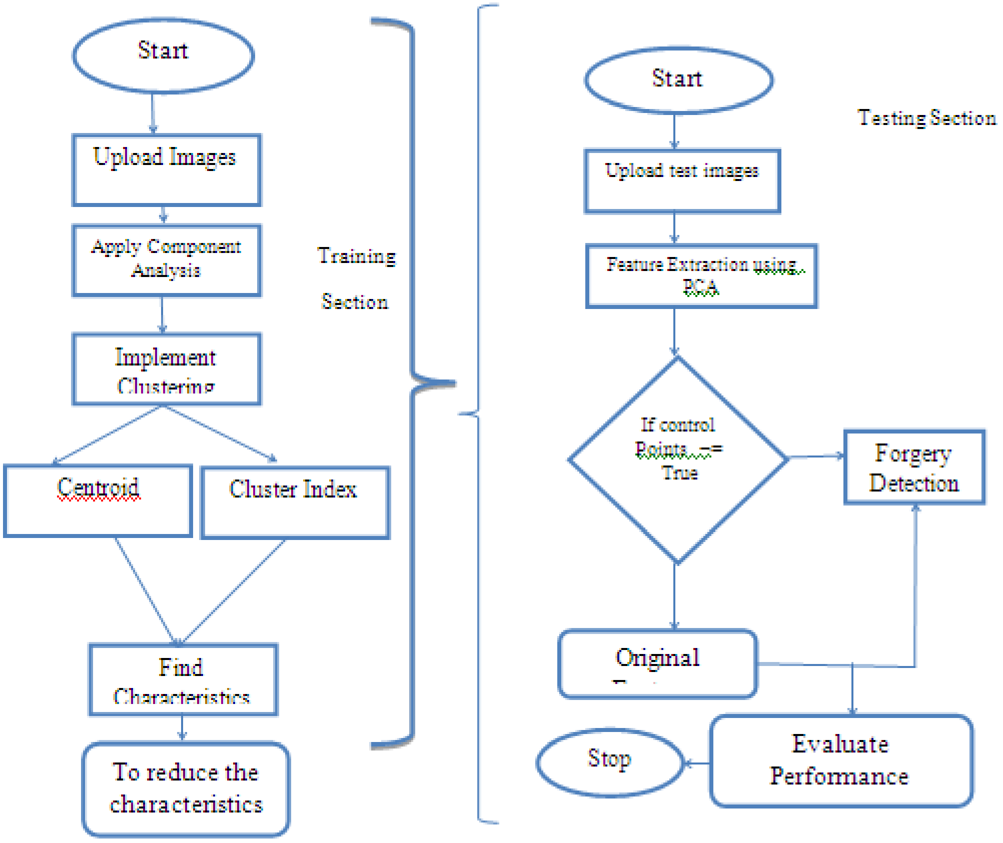

Fig Proposed Flow chart

Step III: Apply the segmented image form the rgb2gray image. We segmented the image in three level bases in Level-0, Level-1 and Level-2. K-mean clustering used to convert the image format in cluster form.

Step IV: Determine the most effective feature extraction using Principle component analysis. This is accomplished experimentally by identify the texture based features like Eigen values and vectors.

Step V: Implement the new proposed approach technique i.e ANT optimization used for classify the forgery regions based on unique features.

Step VI: Compute Error rate , Accuracy and Peak Signal To Noise Ratio for all decomposed block featured image and compared the performance parameters based on existing work.

4. PROBLEMS IN IMAGE FORGERY

Robust feature extraction techniques used in block based copy move image forgery detection require a high computation time. There is a need for reduced computation time for detection schemes to be practical for use with large images and in real time environments. Utilization of GPU to compute the processes can highly parallelize the tasks involved to reduce computation time. Current CPU based algorithms that have been designed are not suitable to be directly adopted in a GPU based scheme. It must be determined how a parallel copy move image forgery detection scheme can be designed for use with a GPU. Digital images provide a new way to represent pictures and scenes that only film and a darkroom could supply before. This new way to capture and store images opens a door to mischievous individuals wishing to forge or otherwise deploy original authentic images. The digital photography is improving and becoming more widely used by the average photographer, a need exists to provide countermeasures against malicious forgers.The validity of the image is indefinite; with very little skill a “forged” variety was digitally produced using the computer software Adobe Photoshop. It is very durable, if impossible, for the human eye to detect digital manipulation at face value. This is just one example of the need for a tool to aid in the discovery of digital image altering. The research in this thesis attempts to address this need and provide some insight into this challenging problem.

5. SIMULATION RESULTS

The proposed image processing concept is implemented in MATLAB with GUI (Graphical User Interface). The considered GUI is shown in figure 2. Here, the considered buttons are Image Acquisition, pre-processing, clustering, feature extraction and optimization as well as classification.

Fig 3. Uploaded Image

The above figure uploads the original image form the data set. Convert the rgb2gray scale form image. We plot the histogram that performance as a graphical representation of the tonal distribution in a digital image. It plots the number of pixels for each tonal value. By looking at the histogram for a specific image a viewer will be able to judge the entire tonal distribution at a glance.

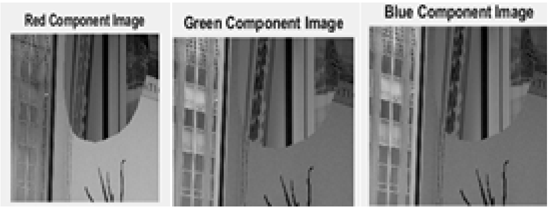

Fig 4. RGB components

The above figure defined that the rgb component calculates. RGB (red, green, and blue) refers to a system for representing the colors to be used on a computer display. Red, green, and blue can be combined in various proportions to obtain any color in the visible spectrum. Levels of R, G, and B can each range from 0 to 100 percent of full intensity. Each level is represented by the range of decimal numbers from 0 to 255 (256 levels for each color), equivalent to the range of binary numbers from 00000000 to 11111111, or hexadecimal 00 to FF. The total number of available colors is 256 x 256 x 256, or 16,777,216 possible colors.

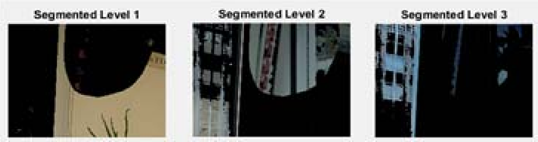

Fig 5. Segmented Image

The above figure represents that the segmentation applied to identify the region area. We apply the k-mean clustering approach to calculate the data in cluster form and segmentation level defined images LEVEL-1, LEVEL-2 and LEVEL-0.

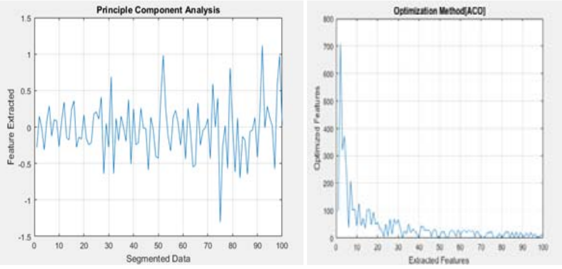

Fig 6. Feature Extraction and Optimization

The above figure defined that the feature extracted using principle component analysis. We calculate the features in the form of Eigen Values and Eigen Vectors. Extracted Features save in database. The reduce the extracted features in the form of graph representation. In ACO algorithm used to optimize the features only selected the relevant features.

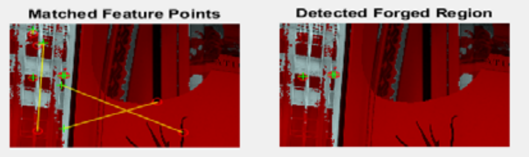

Fig 7. Matched Data and Forgery Area Detect in the Image

The above figure defined that the testing phases to identify features and matching process. In testing Phase, match the features in training and testing phases. If features are matched in both cases then detect the forgery area. And calculate the performance parameters i.e error rate, accuracy and peak signal to noise ratio.

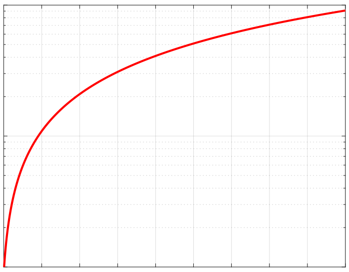

Fig 8. Accuracy in Proposed Work

In the above fig 8 . defined that the detect the accuracy. In ACO algorithm used to detect the forgery data and area in less time consumed.

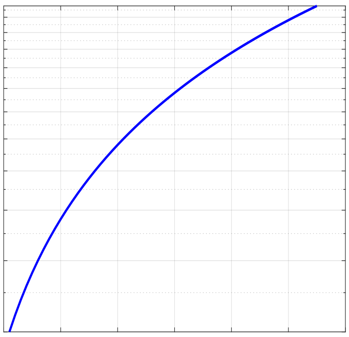

Fig 9. Peak Signal to Noise ratio

The above figure defined that the peak signal to noise ratio used to calculate the quality of the image. It often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is most easily defined via the mean squared error.

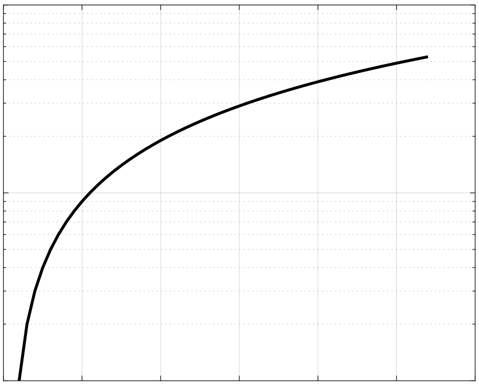

Fig 10. Error Rate

The above figure shows that the number of errors per unit time. The error ratio is the number of bit errors divided by the total number of transferring bits during a studied time interval. Error ratio hasbeen unit less presentation amount, often articulated as a percentage.

Table 1: Proposed Performance Parameters

Number of Images	Error rate	Accuracy	PSNR
1	0.0053	94.6	6.49
2	0.00692	99.3	6.03
3	0.0075	99.2	5.94

In this table 1 describe the performance parameter values in Error Rate, Accuracy and PSNR.

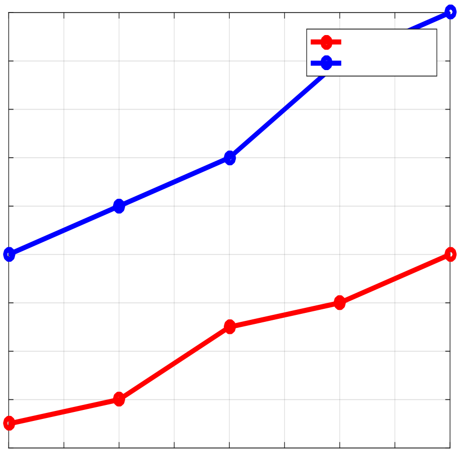

Fig 11 Comparison Between accuracy (proposed and existing work)

The above figure defines that the comparison between accuracy (proposed and existing work). We improve the performance parameters with ACO and PCA approach to detect the forgery data in less time and improve the proposed parameters i.e accuracy.

Table 2. Comparison between Accuracy (Proposed and Existing Work)

Number of Images	Accuracy [Proposed]	Accuracy [Existing]
1	82	75
2	86	79
3	92	82

6. CONCLUSION AND FUTURE SCOPE

Due to the advances in digital image editing techniques, there are many tools which can edit an image easily without leaving obvious traces to the human eyes. So the authentication of digital images is an important issue in our life. The digital images can be used as a source of information and evidence in many applications such as newspapers, courts of law et cetera. Thus, the authenticity of digital images cannot be taken for granted. Detecting the tampering in digital images is very challenging and still remains an open problem. To date, almost all digital cameras do not equip with digital signatures such as watermarking that can help to verify image authentication. Therefore, passive techniques are needed to detect image splicing. Image splicing is a common and fundamental in image tampering, it involves a composite of two or more images which are combined to create a fake image. Several methods have been developed to detect image splicing at image-level with promising results; however, most methods failed when the copied region is rotated and scaled. The aim of this study is to design a novel image splicing forgery detection system that can handle the above-mentioned splicing tactics with improved accuracy rate.

The future scope of this research area, the activities and accomplishments presented in this thesis paved a new dimension for automatic spliced image detection and tampered region localisation. Despite few noteworthy contributions several potentially new areas remain unexplored. Amongst others: (1) Shallow Depth of Field photographic images and alike, where the object of interest has a sharp resolution with blurry background. This type of image is very challenging to determine its authenticity because the blurry effect creates a big gap in terms of intensity value between the blurry part and the object of interest. (2) Tampered region location: It is a very challenging task to precisely localise the whole tampered region using a block-based approach because of intensity differences between the boundary pixels of the tampered region and the whole image.

7.REFERENCES

1. L. Wang, A. Ngom, and L. Rueda. "Sequential Forward Selection Approach to the Non-unique Oligonucleotide Probe Selection Problem," presented at the Proceedings of the Third IAPR International Conference on Pattern Recognition in Bioinformatics, Melbourne, Australia, 2008.
2. Gharehchopogh, Farhad Soleimanian, Neda Jabbari, and Zeinab Ghaffari Azar. "Evaluation of fuzzy k-means and k-means clustering algorithms in intrusion detection systems." International Journal of Scientific & Technology Research 1, no. 11 (2012).
3. Li, Jian, Xiaolong Li, Bin Yang, and Xingming Sun. "Segmentation-based image copy-move forgery detection scheme." IEEE Transactions on Information Forensics and Security 10, no. 3 (2015): 507-518.
4. Deshpande, Pradyumna, and Prashasti Kanikar. "Pixel based digital image forgery detection techniques." International Journal of Engineering Research and Applications 2, no. 3 (2012): 539-543.
5. Y. Zhang, C. Zhao, Y. Pi, and S. Li, "Revealing Image Splicing Forgery Using Local Binary Patterns of DCT Coefficients," in Communications, Signal Processing, and Systems. vol. 202, Q. Liang, W. Wang, J. Mu, J. Liang, B. Zhang, Y. Pi, and C. Zhao, Eds., ed: Springer New York, 2012, pp. 181-189.
6. S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on, 2009, pp. 1053-1056.
7. Huynh, Tu K., Khoa V. Huynh, Thuong Le-Tien, and Sy C. Nguyen. "A survey on image forgery detection techniques." In Computing & Communication Technologies-Research, Innovation, and Vision for the Future (RIVF), 2015 IEEE RIVF International Conference on, pp. 71-76. IEEE, 2015.
8. Qazi, Tanzeela, Khizar Hayat, Samee U. Khan, Sajjad A. Madani, Imran A. Khan, Joanna Kołodziej, Hongxiang Li, Weiyao Lin, Kin Choong Yow, and Cheng-Zhong Xu.

"Survey on blind image forgery detection." IET Image Processing 7, no. 7 (2013): 660-670.

9. Zandi, Mohsen, Ahmad Mahmoudi-Aznaveh, and Azadeh Mansouri. "Adaptive matching for copy-move Forgery detection." In Information Forensics and Security (WIFS), 2014 IEEE International Workshop on, pp. 119-124. IEEE, 2014.
10. Pandey, Ramesh Chand, Sanjay Kumar Singh, and K. K. Shukla. "Passive copy-move forgery detection in videos." In Computer and Communication Technology (ICCCT), 2014 International Conference on, pp. 301-306. IEEE, 2014.
11. Wahab, Ainuddin Wahid Abdul, Mustapha Aminu Bagiwa, Mohd Yamani Idna Idris, Suleman Khan, Zaidi Razak, and Muhammad Rezal Kamel Ariffin. "Passive video forgery detection techniques: a survey." In Information assurance and security (IAS), 2014 10th International Conference on, pp. 29-34. IEEE, 2014.
12. Fadl, Sondos M., and Noura A. Semary. "A proposed accelerated image copy-move forgery detection." In Visual Communications and Image Processing Conference, 2014 IEEE, pp. 253-257. IEEE, 2014.