Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

An Image Forgery Detection using SIFT-PCA

Pooja Bhole
Computer Science and Engineering
St. Vincent Pallotti College of Engineering and Technology
Nagpur, India

Dipak Wajgi
Computer Engineering
St. Vincent Pallotti College of Engineering and Technology
Nagpur, India

***Abstract*—Digital Images plays an important role for transferring the information and are widely used in all areas of day-to-day life. Although, with the development of modern technologies, multiple software's are developed. This leads to the forgery of digital images. Copy-move Image Forgery Detection is one of the forensic techniques in which selected area of an image is get copied and then moved onto the other portion of the image. In this research, the main aim is to detect the forged region from the image. A method is proposed to detect the copy-move forgery in an image, by comparing extracted key points. The SIFT (Scale Invariant Feature Transform) algorithm is used for extracting the invariant features from an image and then extract blocks by using PCA.**

Keywords—Digital Image, Copy-move Forgery, SIFT

I. INTRODUCTION

Copy-move forgery detection in Digital image is an intelligible and effective technique. In this category of forgery, a part of the image is copied and moved to another part of the same image. Copy-move simply requires the pasting of image blocks in same image and hide an important information form an image. Consequently, this changes the originality and reduce the authenticity of the image. Digital image forgery detection techniques are divided into two approaches i.e., Active approach and Passive approach. In Active approach, the digital image requires some prior information and mainly uses techniques like signature and watermarking which are stored within the image at the time of creation. In passive approach, do not depends on the prior information of image and its features but it utilizes the statistics and the content of the available information to detect trace of tampering. A number of methods proposed to detect copy-move forgery which can be classified into two categories such as Block-based methods and Key-point based methods. There are several methods by which forgery attacks can be detected.

With the advancement of digital imaging methods, it has turn out to be terribly uncomplicated to maintain any occurrence of a digital image and this digital imaging data is being extensively operated for a range of numerous applications like forensics, multimedia, electronic media and observation scheme. Due to the advancement in latest altering tools, anyone can modify the authentic information of an image and harm it.

In copy-move forgery, some transformations such as, scaling, rotation can be made. To detect those transformations some methods are available. Digital imaging has fully developed to become the dominant technology for creating, processing and storing pictorial memory and evidence. This technology brings many advantages, it can be used as an ambiguous tool for hiding facts and evidences. This is because now digital images can be manipulated in such perfection that forgery cannot be detected visually. The security task of digital content has arisen a long time ago and different techniques for validating the integrity of digital images have been developed. There are many ways to categorize the image tampering and some operations are performed in image tampering are:

- Adding new object into the image
- Hiding or deleting a region from an image
- Improper representation of image

In the fields such as forensics, medical imaging, e-commerce, authenticity and integrity of digital images is important. In medical field physicians and researchers make diagnoses based on images which is crucial as one is dealing with human life. E-commerce has drastically increased in recent years due to the advancement of information technology and internet. This is current market of approximately 50 million internet users who have made an online retail purchase. [1]

Online marketing is mainly based on multimedia with images and videos as basic elements of product description. With the increase of sophisticated and advanced image processing and manipulation software coming into picture unworthy a thousand true words. "The introduction and rapid spread of digital modification to still and moving images raises social issues of truth, deception, and digital image integrity". [2]

The foremost key point reliant method demonstrated in [3], in which many un identical features are considered such as SIFT. Geometric alterations are changed as well alteration of pixel co-ordinates. RANSAC approximate such parameters [4]. Latest variant of techniques experience concern of identical sections by hierarchical agglomerative clustering. [5]

II. LITERATURE SURVEY

In [2], author has proposed new methodology based on Transform Invariant Features. The main is based on MPEG-7 image signature tools that forms a part of MPEG-7 standard. These tools are used for fast image and video retrieval. Primarily, such tools are designed to detect the duplicated region in an image or in video, but in separate image. Author aims to fins the duplicated region in a same image.

In [6], Dempster-Shafer Theory of Evidence is used. The aim of the paper is decision fusion strategy for image forensics. The proposed system operates by combination of the measurement level thus it permits to retain the relevant information. The proposed framework includes:

- The use of soft reasoning method based on Dempster-Shafer theory of evidence.
- The ease with which new information can be included as soon as it becomes available.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

- The framework which provides hierarchical structure, allows to trade-off between granularity about information provided by the fusion.

In [8], SIFT characteristics are selected to place the cloning section from beginning to end correlation map. But data set not mentioned and this way is not taken into consideration for more than one forgery. In [7] more than one forgery is considered by evaluating the SIFT identical method and clustering of main points to differentiate the separated cloned area. Anyhow, the process is taken just for cloning uncovering and not for extract alteration identification.

The proposed method in [9], is based on a new feature measuring the presence of demo sacking artefacts at local level. Demo sacking is the digital process used to re-construct a full colour image from incomplete image sample output from an image sensor overlaid with a colour filter array. Green channel extraction is used for extracting the features and then Map generation and Filtering is used for creation of forgery map.

In [10], The author has proposed a spliced image detection technique based on Markov feature in DCT and DWT domain. The proposed system consists of two kinds of Markov features which are generated from the transition probability matrices e.g. the expanded Markov in DCT & DWT domain. The author uses DCT domain to capture the correlation between DCT coefficients an DWT domain is used to characterize the dependency among wavelet coefficients across positions, scales and orientations.

In [11], an improved DCT based method has been developed to detect the specific artefact. Basically, the image is divided into fixed-size overlapping blocks and DCT is applied to each block to represent its features. Trimming is use to reduce the dimension of the feature vectors are lexicographically sorted and duplicated image blocks will be neighboring in the sorted list. Thus, identical image blocks will be compared in the matching step.

In [12], The SIFT algorithm have been used which is able to detect the copy-move forgery done in an image and to estimate the parameters of the transformation used. It detects the cluster of points belonging to cloned areas. First the image goes under the feature extraction and matching in which the key points are extracted from the image and then matched to the original image. After that the clusters are formed using hierarchical clustering and then forged regions are detected.

III. PROPOSED METHOD

As per the elaboration in the II we came to know the determining is an essential feature. Even after some alteration, the features of the identical blocks are similar. Technique relied on the copy move, is dependent on invariant. SIFT is sort of invariant, demonstrated by Lowe et al. and justified invariant to picture and rotation. Moreover, robust to distortion caused by affine ranges, alteration of viewpoint, noise, illumination change and compression [13]

A. Scale Invariant Feature Transform

SIFT basically a technique to take out distinct invariant characteristics as of pictures. It has main point sensor along with local characteristics representation. For categorization 4 steps referred here:

1) Scale-space extreme detection: Initial research or scales and location of picture, operated to see the extremes local in the space of scale. It consisting of:
   - Search over scales and location
   - Locate local extremes
   - A cascade filtering approach
   - Scale-space images for octave
2) Key point localization: To formative position and scale at every entrant location a comprehensive representation is well. In addition to key points are elected based on procedures of their firmness.
   - Choose key points from local extremes
   - Recognition of local key points
   - Exclusion of key points.
3) Orientation assignment: For every main point single otherwise, extra orientations are given relied on confined picture slope guidelines. Whole next time operations are carried on picture information that altered comparative to the assigned direction.
4) Key point descriptor: The local picture gradients are calculated at chosen scale area in the region of every main point. These are altered into a depiction that permits amend in illumination for noteworthy levels of limited form deformation.

First and foremost, detection of main points has been done by employing filtering which uses efficient a log to judge candidate place or location that are then investigated for extended detail. Location identification is∇ an initial step to detect the main points and also scale that can be repeat under separate view in the context of the item. Sensing the positions that are stabilize to scale altered picture need looking intended for steady characteristics transversely total practicable amendment of scale, by means of a constant meaning of scale acknowledged at the same time as level gap.

Koenderink and Lindeberg (1994) depicted the assumptions that simply potential scale-space kernel is the Gaussian function. So that, space of a picture is stated as a variable-scale Gaussian, G (x, y, σ), with an input image

l (x, y):

$$L(x, y, \sigma) = G(x, y, \sigma) * l(x, y)$$

Where * is the convolution operation in x and y and G (x, y, σ) $= (1/2\Pi\ \sigma^2) * e^{-(x*x + y*y)/2\sigma\hat{}2}$

In context for correctly sensing detect steady key point positions in scale space, reliant scale space peaks in the differentiation of Gaussian function present by means of the picture, D (x, y, σ), dissimilarity of two in close proximity scales estranged through steady aspect k:

$$D(x, y, \sigma) = (G(x, y, k\sigma) - G(x, y, \sigma)) * l(x, y)$$
$$= L(x, y, k\sigma) - L(x, y, \sigma)$$

Numerous reasons for selection of this particular function. Initially, it is a mainly competent function to computed in any case for scale space feature description, and D can therefore be computed by simple image subtraction.

Furthermore, the difference-of-Gaussian function gives a close estimate to the scale-normalized Laplacian of Gaussian, $\sigma^2\Delta^2G$, the normalization of the Laplacian with the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

factor σ^2 is needed for correct scale invariance. In elaborated work, the maxima and minima of $\sigma^2\Delta^2G$ generate the mainly steady image features compared to a variety of extra likely image functions such as the gradient, Hessian, or Harris corner function. The relationship between D and $\sigma^2\Delta^2G$ can be understood from the heat diffusion equation:

$$\frac{\partial G}{\partial \sigma} = \sigma\nabla\hat{}2G$$

∇^2G Can be computed from the finite difference approximation to $\frac{\partial G}{\partial \sigma}$ using the difference of nearby scales at k σ and σ:

$$\sigma\nabla^2G = \frac{\partial G}{\partial \sigma} \approx G(x, y, k\sigma) - G(x, y, \sigma)/ k\sigma - \sigma$$

$$G(x, y, k\sigma) - G(x, y, \sigma) \approx (k-1)\sigma^2\nabla^2G$$

B. Principal components analysis (PCA)

PCA is one of the group of procedures for taking high-dimensional information, and utilizing the conditions between the variables to speak to it in a more tractable, lower-dimensional structure, without losing an excessive amount of data. PCA is one of the least complex and most powerful methods for doing such dimensionality decreases.

III OVERVIEW OF PROPOSED CMFD SYSTEM

We illustrate a method that is hybrid in order to detect the forgeries relied on the SIFT and technique PCA. A method is represented in fig.1. First SIFT identify feature points and extracted by PCA, the next is to check the forgery, third step is to localize the copied region and detect the forged from an image. The work and process are summed up for detection of tampering.

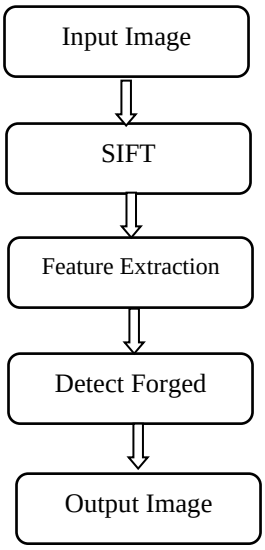

Fig. 1: Depiction of CMFD Flowchart

EXPERIMENTAL RESULT

Fig. 2 Original image

Fig. 3 Gray Scale image

Fig 4 Segmented image

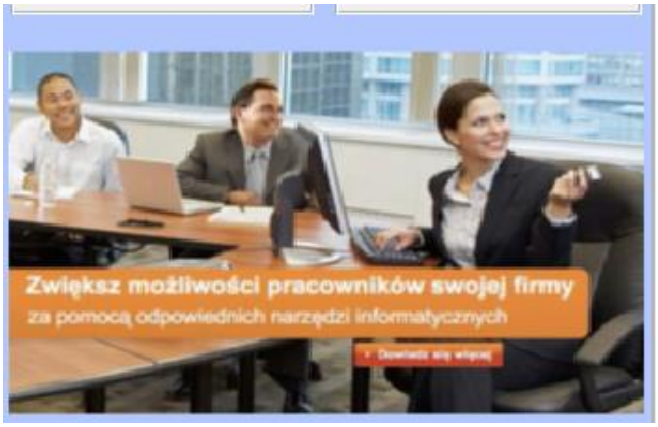

Fig. 5 Forged Image

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

Fig. 6 Detection of forged region

Fig.2 is an original image which is taken from dataset. Next is conversion of RGB image into gray scale image as shown in fig. 3 for discarding unnecessary information. After that, segmentation is done in fig. 4 for represent the image in a meaningful information and easy for analyzing it. Forged image is selected from dataset in fig. 5 and detection of forged region is shown in fig. 6.

We compare our dataset result with another dataset. The result showed that our execution time is less for each step
leading to a decrease in the average execution time for image tampering detection. The matches among the SIFT key points are larger than the existing System.

CONCLUSION

The proposed approach support image forensics investigation based on SIFT features. Given a suspected image, it can reliably detect if a certain region has been duplicated or forger. Time improvement is done using the proposed system and results are better than it is stated in earlier papers. This method detecting two challenging forgery techniques copy-move and splicing. We hope our work can serve as an initial building block to improve the security of images on the web.

REFERENCES

[1] I Amerini, L Ballan, R Caldelli, A DelBimbo, L D Tongo, Giuseppe Serra, “Copy Move Forgery Detection And Localization By Means Of Robust Clustering with JLinkage”.
[2] T Bianchi and A Piva, “Image Forgery Localization via Block-Grained Analysis of JPEG Artifacts” IEEE Transactions on Information Forensics And Security
[3] Tang, and H-V Shum, “Detecting Doctored Images using Camera Response Normality and Consistency”.
[4] S.-F. Chang Hsu, Y.-F, and, “Image splicing detection using camera response function consistency and automatic segmentation”.
[5] A. Swaminathan, M. Wu, and K. J. R. Liu, “Digital Image Forensics via Intrinsic Fingerprints”.
[6] Andrea Costanzo, Irene Amerini, Roberto Caldelli, and Mauro Barni, “Forensic Analysis of SIFT Keypoint Removal and Injection”, IEEE Transactions on Information Forensics and Security.
[7] Gou H, Swaminathan A, and Wu M, “Noise features for image tampering detection and steganalysis”.
[8] Chao Shao, Li and Jing, "Image Copy-Move Forgery Detecting Based on Local Invariant Feature".
[9] S and N Sudha, P Kakar Exposing post processed copy–paste forgeries through transform-invariant features.
[10] T Bianchi, P Ferrara, A De Rosa, and A Piva, “Image Forgery Localization via Fine-Grained Analysis of CFA Artifacts”.
[11] I Amerini, L Ballan, R Caldelli, A Del Bimboand G Serra “A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery”.
[12] S Battiato, G M Farinella, E Messina, and G Puglisi, “Robust Image Alignment for Tampering Detection”, IEEE Transactions On Information Forensics And Security,
[13] F Peng, Y Nie and M Long, "A complete passive blind image copymove forensics scheme based on compound statistics features"
[14] V Christlein, C Riess, J Jordan, C Riess, and E Angelopoulos “An evaluation of popular copy-move forgery detection approaches”.