International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

Image forgery detection using support vector machine

Dr PALANIVEL .N
Associate Professor,
Department of Computer Science and Engineering,
Manakula Vinayagar Institute of Technology,
Puducherry.
npalani76@gmail.com

ARTHI.Z
Department of Computer Science and Engineering,
Manakula Vinayagar Institute of Technology, Puducherry.
arthi033@gmail.com

DEEPIKA.G
Department of Computer Science and Engineering,
Manakula Vinayagar Institute of Technology, Puducherry.
deepikagurumurthy1998@gmail.com

LATHA.S
Department of Computer Science and Engineering,
Manakula Vinayagar Institute of Technology, Puducherry.
lathasl1509@gmail.com

Abstract- *Now-a-days, it is very easy to manipulate an image by adding or removing some features in an image without leaving any clue of editing the original image. They use advanced tools to digitally manipulate images to create forged image without finding a clue on it to find the forged region of an originality of images. These modifications are not visible when we see it into the naked eye. Splicing and Copy-move forgeries are most common forgery techniques. In splicing forgery, a small region in one image is cut and paste over an another image. Whereas in copy-move, a small region of an image is copied and pasted over a same image. The devices like cameras are getting more and more digitized, there is an increase in the need for digital image authentication, validation and forgery detection. This paper has an approach for the Splicing and Copy-move forgery detection. Copy-move and Splicing are the passive image forgery detection techniques. Initially, an image is taken as an input for both copy-move and splicing forgery. For both copy-move and Splicing detection, pre-processing and enhanced threshold methods are used to extract the features in an image. After feature extraction, using SVM we find whether it is authentic or forged by using RBF. If the given input image is authentic then the output will be the Black screen(No forged region). When the SVM identified it is forged, then using PCA algorithm we remove the authentic region and shows only the forged region as an output.*

Keywords: ***Multimedia Technology; ulterior; Image manipulation; investigations; Splicing ; Copy-Move ; Image Forgery ; support- Vector Machine; Enhanced Threshold Method; Radial Basis Function; Principle Component Analysis.***

I. INTRODUCTION :

With the availability of powerful digital image processing platforms, such as Photoshop, it is relatively very easy to create digital forgeries from one or more images. Due to the development of computer technology and image processing software, digital image forgery has been increasingly easy to perform. However, digital images are a popular source of information, and the reliability of digital images is thus becoming an important issue. In recent years, more and more researchers have begun to focus on the problem of digital image tampering. Of the existing types of image tampering, a common manipulations of a digital image are cut-paste and copy-move forgeries, which is to paste one or several copied region of an image onto other parts of the same image or on another image. plotting the cumulative graph shows whether the image is splicing forged or not. During the copy and move operations, some image processing methods such as rotation, scaling, blurring, compression, and noise addition are occasionally applied to make convincing forgeries. Because the copy and move parts are copied from the same image, the noise component, color character and other important properties are compatible with the remainder of the image some of the forgery detection methods that are based on the related image properties are not applicable in this case.

In previous years, many forgery detection methods have been proposed for copy-move forgery detection. According to the existing methods, the copy-

move forgery detection methods can be categorized into two main categories: block based algorithms and feature key point based algorithms. The existing block based forgery detection methods divide the input images into overlapping and regular image blocks then, the tampered region can be obtained by matching blocks of image pixels or transform coefficients. As an alternative to the block based methods, key point based forgery detection methods were proposed, where image key points are extracted and matched over the whole image to resist some image transformations while identifying duplicated regions.

II. LITERATURE SURVEY:

Pun et al. proposed a method which is based on noise discrepancies between the original image and spliced image. Initially, the noise level function is calculated and analyzed at pixel level on various scales. The region which is not under the noise level, termed as suspicious area and inconsistent level of noise indicate the presence of tampering in spliced segments. This technique performs better for multiple spliced object detection. F. Hakim proposed a method based on improved local binary pattern (LBP) and discrete cosine transform (DCT). The chrominance component of the image is divided into nonoverlapping blocks. Then improved LBP is calculated for all blocks and using 2D-DCT, it is transformed into frequency domain. Further the frequency coefficients are evaluated to find the standard deviation for all blocks which are used as features for classification using k-nearest neighbour.

Shi et al.proposed a natural image model, which educe statistical moments of characteristics function by treating the neighbouring differences of BDCT of an image as 1-D signal and the dependencies between neighbouring nodes along certain directions have sculpted as Markov model. SVM classifier considered these features as discriminative features for classification. Wang et al. proposed a method in which gray level cooccurrence matrix (GLCM) is considered along certain direction (horizontal, vertical, main and minor diagonal) to extract edge images and educed edge images serve as discriminative features for classification. Xuefang Li et al. proposed a method in which Hilbert-Huang transform and moment of characteristic function of wavelet transform are used for forgery detection. SVM is used as a classifier for spliced image classification in their method and achieved an accuracy of 85.86%.
Qu et al. proposed a algorithm to detect splicing image forgery with visual cues in 2009. Authors used a detection window and divided it into nine sub-squares. VAM (visual consideration model) is used to distinguish an obsession point and afterward feature extraction is used to extract the spliced region in the digital image.

III. TYPES OF DIGITAL IMAGE FORGERY:

Image forgery is characterized as ”inserting, replacement, or removing some important features from an image without leaving any clue. There are many different techniques to utilize forging regions of an image. Taking into account these method is used to make forged images. Digital image forgery can be divided into three primary classifications: Copy-Move, splicing, and Image re-sampling.

A. Copy-move Forgery

In copy-move forgery, some portion of an image at any size and shape is copied and pasted to another region in the same image to modify some important feature. The copied region is pasted over the same so that the pixel of the block will varies. This is very difficult to find the forged region in it. Digital image forgery techniques are used many different techniques to manipulate an image without leaving any clue on it.

B. Splicing Forgery:

Image splicing means a part of region of one image is cut and paste over an another image to create a suspicious image is called Image Splicing. When compared to copy-move forgery detection Splicing Forgery detection is very difficult to find. Previously many techniques are developed to find the forged region in splicing but it results in failure. When splicing is performed, the borders between the spliced regions can visually be impossible. Splicing, disturbs the high order Fourier statistics.

IV. PROPOSED WORK:

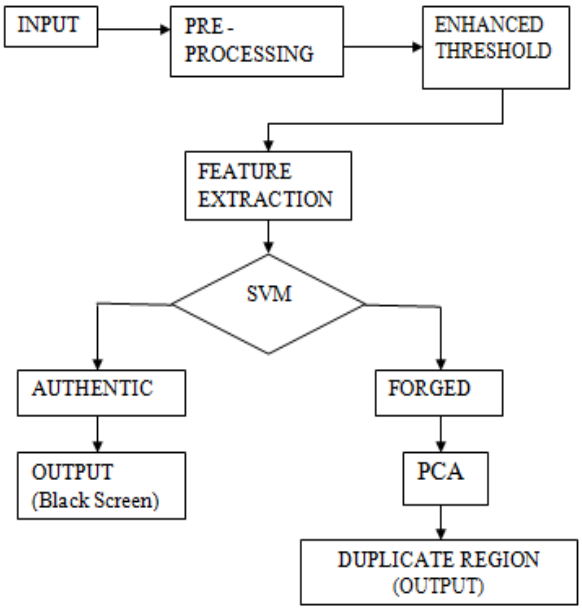
This paper proposes a technique to find a duplicate region in an image. Duplicate region is finded by using the PCA algorithm and SVM classifier.

Steps in Proposed work:

1. Dividing the grayscale image into fixed sized overlapping blocks using SVM.

2. Extracting Gaussian RBF kernel PCA-based features from each DCT square block.
3. Matching similar block pairs.
4. Removing the isolated block and output the duplicated regions.

A. BLOCK DIAGRAM:



B. SUPPORT VECTOR MACHINE:

SVM is mainly used for classification purpose. In order to avoid computational complexity it uses recognition tools by high dimension. There are many studies using SVM as a classifier in image forgery Detection.

In this paper, a technique is developed to detect image forgery which includes removal, addition, and replacement of regions in an image. SVM classifier is used to find similar regions of an image by matching image blocks. Image, texture pixel value based features and edges are extracted to analyze the images for forged regions. After analyzing the image, hash values are calculated for feature extraction. This process consists of two phases they are training phase and a testing phase. In training phase, SVM train a set of image. SVM is used to classify the image whether it is authentic or forged.

SVM first identify the decision boundaries in the training phase and then the technique will give the good generalization in high dimensional input images. Classification using SVM is mainly based on the concept of decision making and that defines the decision boundaries. A decision plane separates a set of objects having different class memberships and a set of objects having different class relationships. SVM determine a vectors called "support vectors" that easily identify the separators which gives the wide separation of classes and objects.

SVM classifier supports both the binary and multiclass targets. Support Vector Machine models must have a similar functional form for block based network and radial basis functions, both are well-knowned data mining techniques. Since, neither of these algorithms has the very new theoretical approach to regularize the format, that forms the basis of SVM. The quality of generalization and ease of training in SVM is based on the capacities of those traditional methods. The SVM map the original data points from the input image to the high dimensional, feature block making classification problem simpler in feature space. This kind of mapping is done by a suitable choice of a kernel basis function.

C. PCA:

The image is changed over from colour to grayscale. The image is isolated into a few little sized blocks, which are broken to vectors. This is vastly improved than the BruteForce strategy for finding the matches. The PCA technique is utilized to break the diverse blocks in an option way. PCA is fit for recognizing even minor variations because of noise and/or compression. This strategy is just for grayscale images. Be that as it may, the strategy can be made to work for colour images also by preparing the image for every colour channel which outcomes three duplication maps. At that point PCA is connected to every map independently to recognize the forgeries. This technique has a decent proficiency in detecting Copy Move forgeries furthermore gives the less number of false-positives.

In any case, the productivity drops as the piece size reduces furthermore in case the nature of image is low. The goal of PCA is to enlarge the variance between data without considering class separation. There are distinctive methodologies proposed for a feature extraction piece. Distribution shows multidimensional raw

data which is every now and again troublesome. Normally, evacuating features those are proposed to catch and address the distributions in a lower-dimensional space may unravel this mission.

The PCA is frequently used for pre-processing of multi-spectral remote sensing images for the explanations behind change detection. Change, regardless, is interesting in connection to the interpretation that is used here. In remote-sensing, the change is fathomed as the technique of perceiving contrasts in the condition of an article in space by watching it at various times, for instance a vegetable canopy. In case there is no learning of what the change might be, it is not clear whether the representations in a lower-dimensional space will offer support. The PCA will analyze each pixel of the image and then classify it.

D. PCA ALGORITHM:

Step 1: The input image should changed from color to GreyScale Image.

Step 2: Then the image is isolated into few little sized blocks and which are broken into vectors.

Step 3: Column or row vector of size N2 represents the set of M images (B1, B2, B3…BM) with size N*N

Step 4: And then we need to calculate the co-variance matrix.

Step 5: Then Measure the Eigen vectors and Eigen values of these co-variance matrix of an image. The PCA is also used to recognise even minor variation because of noise and compression.

E. EXPERIMENTAL RESULTS:

The result shows only the duplicate region of the image.

- If the image which we give as an input is authentic then the output result will be a black screen. The black screen shows that the given image is authenticated.

INPUT

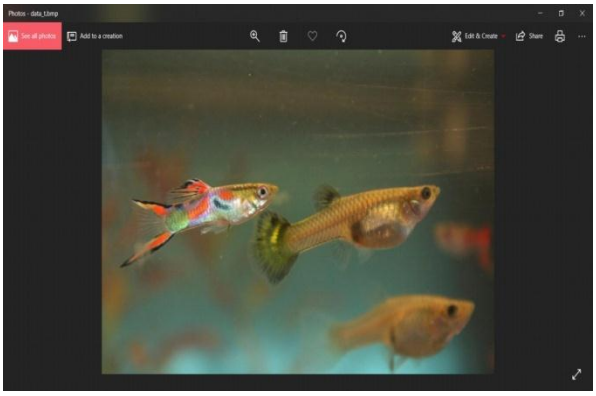


Fig.1 Input image(Authentic image to detect forged region)

OUTPUT:

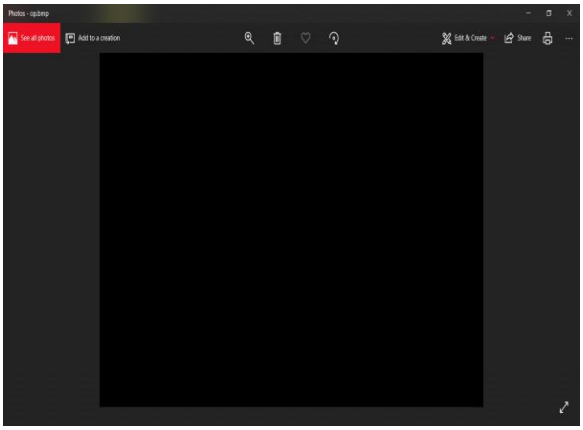


Fig .2 Output Image(Which shows no forged region in an image)

- If the given image is forged then the output result will be the duplicate region of the image.

INPUT:

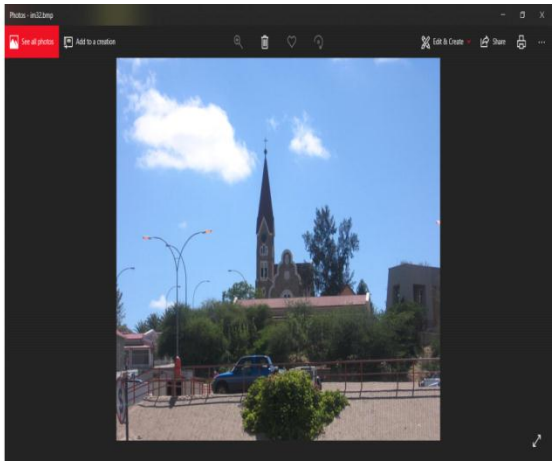


Fig 3: Original Image(Pure image with no modification in it)

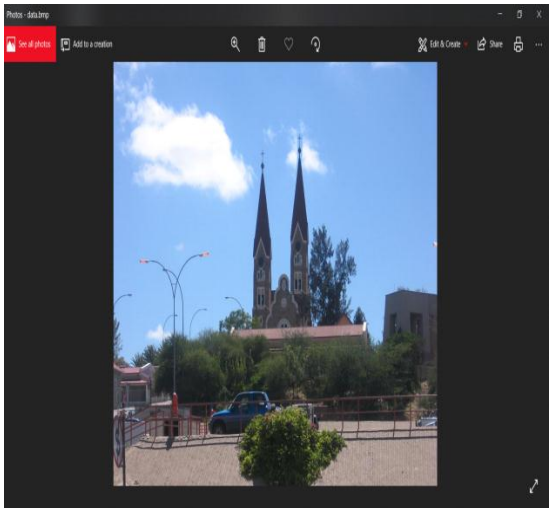


Fig 4: Forged image(small region is altered in an image)

OUTPUT:

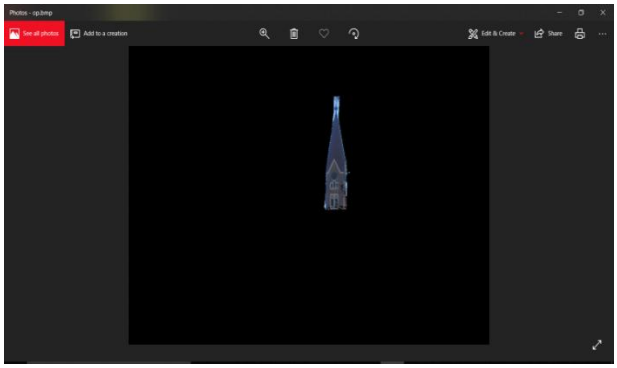


Fig 5: Output Image(shows the forged region)

V. CONCLUSION

With the increase in digital image forgery, the need for forgery detection algorithms has increased. In this paper, copy-move and splicing forgery detection are done at the same time. The suspicious image is taken as an input and then extract the features in it. Using SVM and PCA algorithm the original region of an image is eliminated. Then duplicate regions of an image is highlighted and marked as an output. In future work, we focus on accuracy of detecting duplicate regions.

VI. REFERENCE

[1]. Amerini S, Ballani P, Caldellan Y, Seeran G (2018) A sift-based forensic method for copy–move detection and transformation recovery. IEEE Trans Inf Forensics Secure 6(3):1099–1110

[2]. Amarini K, Bala K, Caldalli R, Bimbosh A, Tongo LD,(2014) Copy-move forgery detection by means of robust clustering with j-linkage. Signal Process Image Communication 28(6):659–669

[3]. Andreopolos Z, Tsokso J (2012) Object recognition directions forward. Computing Vis Image Understanding 117(8):827–891

[4]. Barne C, Shechtmoni P, Finkel L, Goldman CB (2009) Patchmatch Algorithm: A randomized correspondence algorithm for structural image editing. ACM Graph 28(3):24–1 Multimedia Tools Application.

[5]. Bayiram O, Sensar TH, Menon N (2008) An efficient and robust method for detecting copy-move forgery. In: Acoustics, Speech and Signal Processing, 2008. ICASSP 2009. IEEE International Conference on, pp 1053–1086. IEEE

[6]. Bianchin M, Pivash K (2016) Image forgery localization via block grained analysis of .jpeg artifacts. IEEE Transition Information Forensics Secure 7(3):1003–1017

[7]. Bosh S, Yuansh Q, Wangelton S, Zhao C, Li S (2014) Enhanced state selection markove model for image splicing detection. EURASIP J Wirel Communication Network 2014(1):7

[8]. Bravo-Solonio P, Nanditha TS (2011) Automatic detection and localization of duplicate regions affected by reflection, rotation and scaling in image forensics. Signal Process 91(8):1754–1770

[9]. Campos FM, Correia L, Calado JMF (2015) Robot visual localization through local feature fusion: an evaluation of multiple classifiers combination approaches. J Intelligence Robust System 77(2):377–390

[10]. Caoli Y, Gaola T, Li Feo, Yangush Q (2018) A robust detection algorithm for copy-move forgery in digital images. Forensic Sci Int 214(1):33–43

[11]. Chen L, Wei L, Ni J, Sun W, Huang J (2013) Region duplication detection based on harrister corner points and step sector statistics. J Vis Communication Image Represent 24(3):244–254

[12]. Christleguin V, Riuess C, Jordan J, Rtiess C, Angelopoulou E (2012) An evaluation of popular copy-move forgery detection approaches. IEEE Trans Information Forensics Secur 7(6):1841–1854

[13]. Dollar P, Wojevk C, Schiuele B, Peerona P (2012) Pedestrian detection: An evaluation of the state of the art. IEEE Trans Pattern Anal Mach Intellect 34(4):743–761

[14]. Donjbg J, Wakljng W, Tanley T (2013) Casia image tampering detection evaluation database. In: Signal and information processing (ChinasSIP), 2013 IEEE China Summit & International Conference on, pp 422– 426. IEEE

[15]. El-Alfky E-SM, Quryeshi MA (2015) Combining spatial and dct based markov features for enhanced blind detection of image splicing. Pattern Anal Application 18(3):713–723

[16]. Fischler MA, Bollses RC (1981) Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography. Commun ACM 24(6):381–395

[17]. Fridrich AJ, Sodfukal BD, Luka´s AJ (2003) Detection of copy-move forgery in digital images. In ˇ Inproceedings of Digital Forensic Research Workshop. Citeseer

[18]. Gionisa A, Inidyk P, Maotwani R et al (1999) Similarity search in high dimensions via hashing. In: VLDB, vol. 99, pp 518–529

[19]. Gusdo J-M, Liu Y-F, Wu Z-J (2013) Duplication forgery detection using improved daisy descriptor. Expert System Appl 40(2):707–714

[20]. Hakshiimi F (2015) Image-splicing forgery detection based on improved lbpogb and k-nearest neighbors algorithm. Electron Inf Plan, 3