INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
(Volume2, Issue4)
Available online at: www.Ijariit.com

Novel approach for Image Forgery Detection Technique based on colour illumination using machine learning approach

K. Sharath Chandra Reddy
Research Scholar
CBS Group of Institution, Jhajjar, Haryana

Tarun Dalal
Assistant Professor (CSE Department)
CBS Group of Institution, Jhajjar, Haryana

Abstract*— With the advancement of high resolution digital cameras and photo editing software featuring new and advanced features the chances of image forgery has increased. The images can now be altered and manipulated easily. Image trustworthiness is now more in demand. Images in courtrooms for evidence, images in newspapers and magazines, and digital images used by doctors are few cases that demands for images with no manipulation. Some forgery images that result from portions copied and moved within the same image to "cover-up" something are called as copy-move forgeries. In previous year author use different-different methods such as Principle Component Analysis (PCA), Discrete Wavelet Transform (DWT) & Singular Value Decomposition (SVD) are time consuming. In past many of the algorithm were failed many times in the detection of forged image, because single feature extraction algorithm is not capable to contain the specific feature of the images. So to overcome the limitation of existing algorithm we will use meta-fusion technique of HOG and Sasi features classifier also to overcome the limitation of SVM classifier. Logistic regression would be able to classify the forged image more precisely.

Keywords: Forgery Detection Techniques, SVM, HOG and SASI classifier.

I. INTRODUCTION

In the past ten years, image forgery detection has being emerged as a remarkable research in applications of computer vision, digital image processing, biomedical technology, criminal investigation, image forensics, etc. It becomes more attractive and challenging when powerful software tools for image processing are so popular and sophisticated that we cannot confirm whether an image is manipulated by naked eyes[1]. Image forgery detection is one kind of passive techniques using blind algorithms to detect traces of tampering in a given image without prior information or security codes.

Figure 1: Image forgery [2]

1.1 Types of image forgery

There are several types of digital forgery. Each instance falls into one of three major categories, depending on the process used in the image's creation. These groups consist of Image Retouching, Image Splicing, and Copy-Move.

- **Image Retouching**

  Image Retouching is an incredibly common and potentially least-harmful kind of digital alteration. Instead of completely changing the subject of the photo, retouching is enhancement or reduction of certain features in the image (see Figure 2). The most common users of this technique are magazines or other photo-heavy publications [3].

Figure 2: Image retouching forgery [3]

- **Image Splicing**

  Image Splicing is a much more aggressive technique than retouching. Creating a completely new image occurs by copying a part from one image and pasting to another one [4]. In Figure 3, there is an insertion of a breaching Great White Shark into the base image of the helicopter rescue.

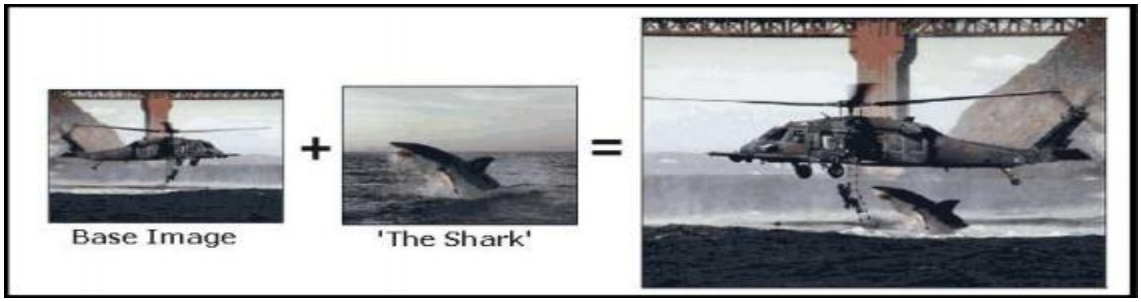

Figure 3: Image splicing forgery [4]

- **Copy-Move**

  Copy-move is again similar to the previous category. Unlike Image Splicing, a copy of a region of an image is pasted in the same image. The difference lies in using the base image itself as both source and recipient of the copied portion [5].

Figure 4: Copy-move forgery [5].

1.2 Image forgery techniques:

Digital image forgery detection techniques are classified into active and passive approaches . In active approach, the digital image requires some pre-processing such as watermark embedding or signature generation at the time of creating the image, which would limit their application in practice.

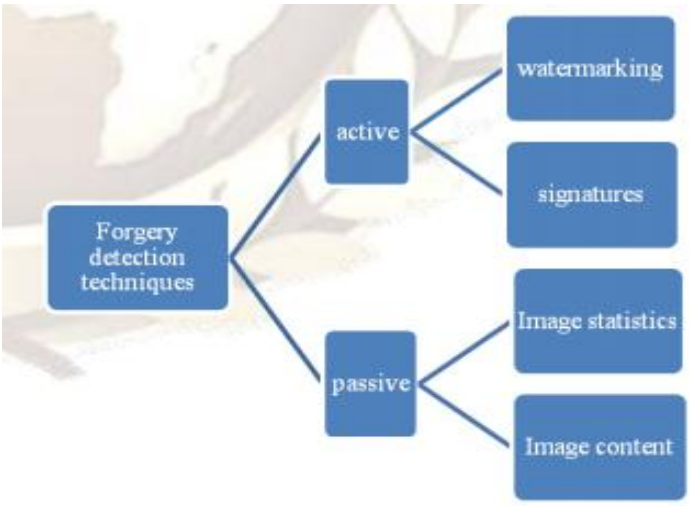

Figure 5: classification of Forgery detection techniques [16]

1.3 Image Forensic Tools

1. **Pixel-based techniques-**These techniques includes that tools which helps in detecting statistical anomalies introduced at the pixel level. Pixel-based techniques emphasize on the pixels of the digital image. These techniques are roughly categorized into four types. We are focusing only two types of techniques copy-move and splicing in this paper. This is one of the most common forgery detection techniques. Figure 6 shows categorization of pixel based forgery detection techniques.

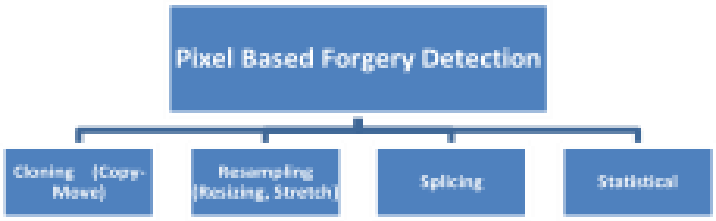

Figure 6: Pixel-based

2. **Format-based techniques:** These techniques includes that tools which leverage the statistical correlations introduced by a specific lossy compression scheme. Format based techniques are another type of image forgery detection techniques. These are based on image formats and work mainly in the JPEG format. These techniques can be divided into three types (Figure 7). If the image is compressed then it is very difficult to detect forgery but these techniques can detect forgery in the compressed image

Figure 7: Format-based

3. **Camera-based techniques-** These techniques includes that tools, which exploit artifacts, introduced by the camera lens, sensor, or on-chip post-processing. Whenever we capture an image from a digital camera, the image moves from the camera sensor to the memory and it undergoes a series of processing steps, including quantization, color correlation, gamma correction, white balancing, filtering, and JPEG compression. These processing steps from capturing to saving the image in the memory may vary on the basis of camera model and camera artifacts. These techniques work on this principle. These techniques can be divided into four categories as shown in Figure 8.

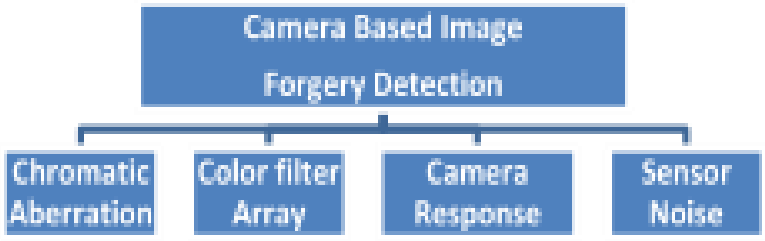

Figure 7: Format-based

4. **Physically based techniques-** These techniques includes that tools whichexplicitly model and detect anomalies in the three dimensional interaction between physical objects, light, and the camera. Consider the creation of a forgery showing two movie stars, rumored to be romantically involved, walking down a sunset beach. Such an image might be created by splicing together individual images of each movie star. In so doing, it is often difficult to exactly match the lighting effects under which each person was originally photographed. Differences in lighting across an image can then be used as evidence of tampering. These techniques work on the basis of the lighting environment under which an object or image is captured. Lighting is very important for capturing an image. These technique are divided into three categories as shown in Figure 8.

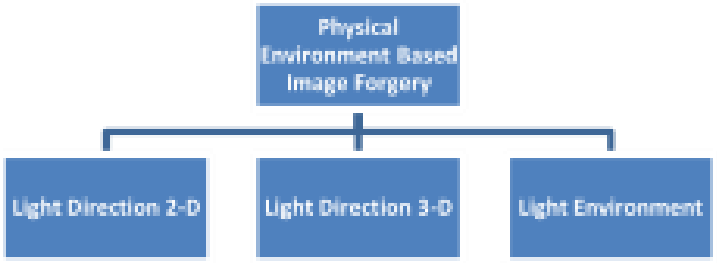

Figure 8: Physically -based

5. **Geometric-based techniques-** These techniques includes that tools which make measurements of objects in the world and their positions relative to the camera.[5] Grooves made in gun barrels impart a spin onto the projectile for increased accuracy and range. These grooves introduce somewhat distinct markings to the bullet fired, and can therefore be used to link a bullet with a specific handgun. In the same spirit, several image forensic techniques have been developed that specifically model artifacts introduced by various stages of the imaging process. Geometry-based techniques make measurement of objects in the world and their position relative to the camera. Geometry-based image forgery techniques are divided into two categories (Figure 9).

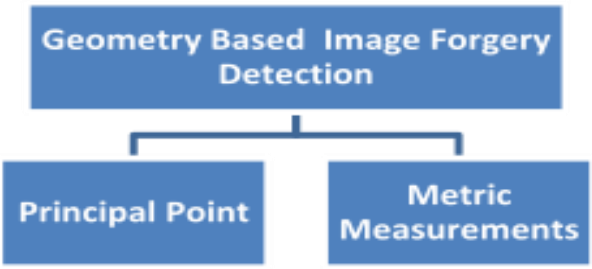

Figure 9: Geometric -based

II. LITERATURE REVIEW

Weiqi Luo [6] proposed an algorithm to extract image features by using seven characteristics features computed from the statistical analysis of pixels in an image block. The first three features are the average of red, green, and blue components respectively and the other four features are computed based on the division of that block into two parts in 4 directions: horizontal, vertical, and two diagonal directions. To obtain the correct matching, the main shift vector which has the highest frequency of occurrence is also defined. It gives low computational complexity and more robust against various post region duplication image processing graphics operations.

Li, Hancheng Zhu et al. [7] have used a vector with seven elements to describe the feature of each small blocks, a 9-dimensional vector is also introduced in to solve the problem with a fixed angle rotation on the copied regions. Elements of this vector are calculated based on the intensities from four equal-sized sub-blocks on each block. The first element is the average intensity, the next four elements are ratios of average intensities and the last four elements are differences of average intensities. A radix sort algorithm is applied to perform lexicographical sorting on these vectors and a forgery manipulation is also detected. The rotation with fixed angle can be detected but not with arbitrary angles by this methods.

HieuCuong Nguyen et al. [8] proposed Radon transformation to extract the features and use phase correlation to detect the pairs of matching vectors. The proposed method is well performed for the forged images which the rotation angle of the copied region is less than 4o, has Gaussian noise addition with a SNR greater than 35dB and smaller block size 8x8 pixels.

Preeti Yadav et al. [9] introduced an improved algorithm by applying DWT into an image to reduce the dimension representation. The feature vectors will be extracted from the small overlapping blocks of the compressed image and sorted lexicographically to find the duplicated blocks. The detection was carried out on the lowest level image representation and also proved best performance on small size copy move forgery, detected the multiple Copy-Move forgery with lower computational complexity.
Johnson et al. [10] proposed a method which describes how composites can be detected by estimating a camera's intrinsic parameters from the image of a person's eyes .In authentic images, the principal point is near the center of the image. When a person is translated in the image as part of creating a composite, the principal point is moved proportionally. The major sensitivity with this technique is in extracting the elliptical boundary of the eye. This process will be difficult for low-resolution images.

Riess and Angelopoulou et al. [11] introduced method which uses physics-based illumination cues to image forensics. They examined inconsistencies in secularities based on the dichromatic reflection model. Specularity segmentation on real-world images is challenging. Therefore, it requires manual annotation of specular highlights. A second drawback of this approach is that it relies on the presence of secularities on all regions of interest making them difficult to deploy in many real world scenarios.

TakaiNiinuma et al.[12] proposed a novel method for estimating parameters of light sources. Their key idea is in introducing the notion of difference sphere that are acquire by differencing two image regions of the reference spheres. They show that separate identification of multiple combined light sources is facilitated through an analysis of gray level contours on the difference sphere. In a forensic scenario, however, the conditions for image capturing cannot be controlled. Thus, one cannot assume to have such gray spheres placed in the scene under investigation.

Gholap and Bora [13], proposed a method, where color mismatches among objects are considered for forgery detection. In this method illuminate color is estimated in every specular highlight region. Then illuminantcolors were plotted in r-g plane by straight dichromatic lines. If these lines intersect points of different regions were not close to each other, it is considers as a forged image. This method performs well in images which contains specular highlight. It is also the method's limitation. i.e., secularities need to present in all region of interest.

Amerini, Irene, et al [14] proposed method is able to individuate if copy-move tampering has taken place and also to estimate the parameters of the transformation used. To support image forensics investigation SIFT (Scale Invariant Feature Transformation) is used. The presented techniques show effectiveness with respect to diverse operative scenarios such as composite processing & multiple cloning. Extensive experimental results are presented to confirm that the technique is able to precisely individuate the altered area & geometric transformation parameters.

Chun-Wei Wang et al [15] proposes a method for detecting copy-move forgery over images tampered by copy-move. To detect such forgeries, the given image is divided into overlapping blocks of equal size, feature for each block is then extracted and represented as a vector, all the extracted feature vectors are then sorted using the radix sort. The difference (shift vector) of the positions of every pair of adjacent feature vectors in the sorting list is computed. The accumulated number of each of the shift vectors is evaluated. A large accumulated number is considered as possible presence of a duplicated region, and thus all the feature vectors corresponding to the shift vectors with large accumulated numbers are detected, whose corresponding blocks are then marked to form a tentative detected result. Finally, the medium filtering and connected component analysis are performed on the tentative detected result to obtain the final result. Compared with other methods, employing the radix sort makes the detection much more efficient without degradation of detection quality.

III. EXPERIMENTAL RESULTS

In this experiment, we use an adaptive support vector machine for the classification .This system is implemented using Matlab 2014a.For the purpose of detecting forgery, a set of original and altered images are given as input to the classifier. The performance of this proposed is evaluated by comparing the results with existing forgery detection system.

1) ***Composite image forgery detection dataset:*** In order to carry out the process of forgery detection, a set of 200 images has been selected. Out of these, 100 original images are taken from Pinterest and the other 100 forged images are created using Photoshop. These images are further shown to 20 human observers with normal color vision. They are then asked to label these images as either genuine or fake. Based upon their decision, we evaluate the performance of our system.

2) ***Performance evaluation:*** Based upon human decision, we check the effectiveness of our system. Here we calculate the true positive rate(TPR) and false positive rate(FPR) for better accuracy.

$$\text{TPR}= \frac{Number\ of\ images\ labelled\ as\ forged\ which\ are\ actually\ forged}{Total\ number\ of\ forged\ images}$$

$$\text{FPR}=\frac{Number\ of\ images\ labelled\ as\ forged\ which\ are\ authentic}{Total\ number\ of\ authentic\ images}$$

We train our system with the help of adaptive SVM. In order to detect the forgery based on color luminance, HOG, SASI and LBP feature extractors are used for extracting illuminate features of an image. With the help of these features, we train the adaptive SVM to detect the forgeries present in digital images. Adaptive SVM is then used to classify the various images as original or altered. The major advantage of adaptive SVM is its ability to adapt one or more existing classifiers for our primary dataset. We calculate the performance of proposed algorithm based on the accuracy in results with respect to existing system. It has been found that the existing system [6] for forgery detection performs well by yielding detection rates of 86% on a standard dataset. In existing system, they used SVM meta-fusion classifier in order to distinguish the original and altered images. However, by using an adaptive SVM for classification, the accuracy of system is increased by 98.7%.Also this work is fully automated and there is no need of human expertise. Thus our method firmly describes the authenticity of a given image.

Table 1. Comparison of forgery detection techniques

S. no.	Method Used	Precision
1.	Existing System	82%
2.	Proposed system	85.831 %

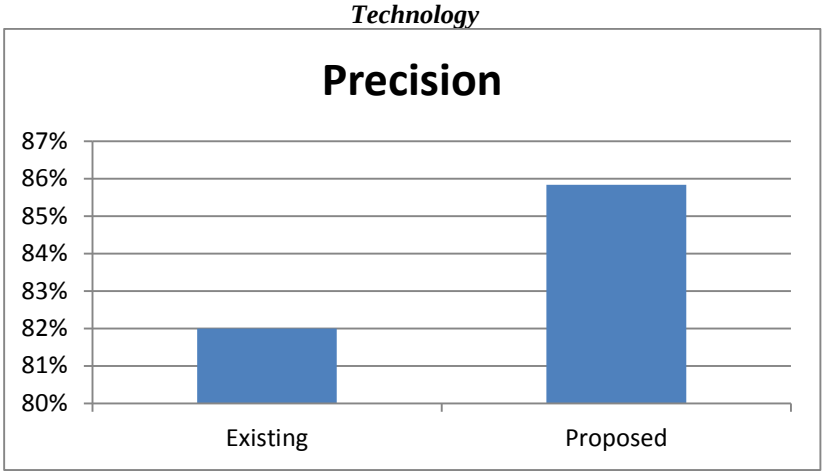

Figure 5.1 Comparison of forgery detection techniques (a)

Table 2. Comparison of forgery detection techniques

S. no.	Method Used	Recall
1.	Existing System	84.89%
2.	Proposed system	97.89%

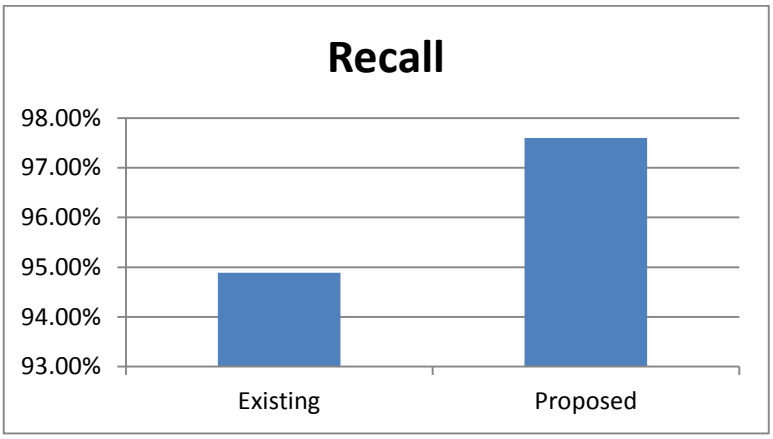

Figure 5.2 Comparison of forgery detection techniques (b)

Table 3. Comparison of forgery detection techniques

S. no.	Method Used	Accuracy
1.	Existing System	86%
2.	Proposed system	98.7%

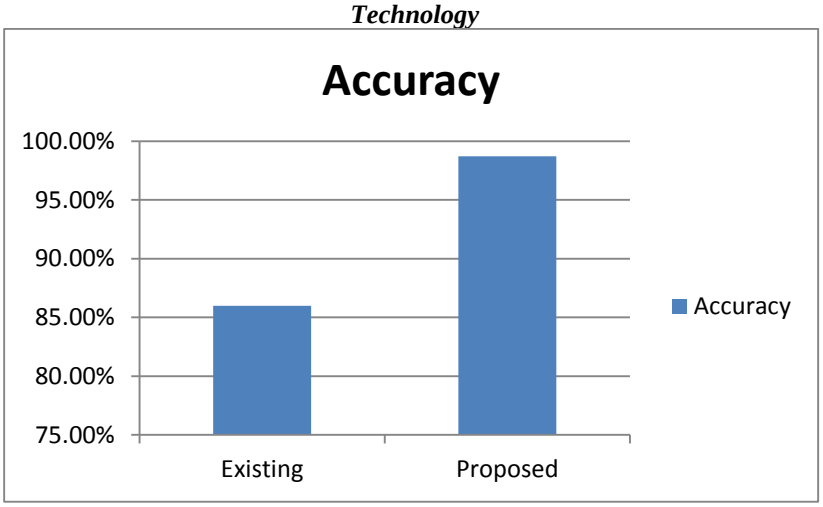

Figure 5.3 Comparison of forgery detection techniques (c)

IV. CONCLUSIONS

An efficient method for detecting digital image forgeries is presented in this paper which is based on the concept of illumination inconsistencies. As we know that illumination inconsistencies present in the scene provide significant cues for detecting false image. Here the focus is to create an illuminated map from given images. These maps are then used to extract various edge based and texture based features. These features are further processed in training and testing phase of classifier. An adaptive support vector machine is used to classify whether the given image as genuine or forged. We can assume that our approach towards forgery detection, in addition to various forensic tools, may be effective in determining tampering detection.

ACKNOWLEDGMENT

Every success stands as a testimony not only to the hardship but also to hearts behind it. Likewise, the present work has been undertaken and completed with direct and indirect help from many people and I would like to acknowledge all of them for the same.

REFERENCES

1) Luo, Weiqi, Jiwu Huang, and GuopingQiu. "Robust detection of region-duplication forgery in digital image." *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on*. Vol. 4. IEEE, 2006.
2) Mahdian, Babak, and Stanislav Saic. "A bibliography on blind methods for identifying image forgery." *Signal Processing: Image Communication* 25.6 (2010): 389-399.
3) S.Shaid. "Types of Image Forgery." Internet: http://csc.fsksm.utm.my/syed/research/image-forensics/11-types-of-imageforgery.html, Feb.08, 2010 12:17 [Dec. 4, 2012].
4) Z. He, W. Sun, W. Lu, and H. Lu. "Digital image splicing detection based on approximate run length," Pattern Recogn .Lett., vol. 32, pp. 1591-1597, 2011.
5) B. L. Shivakumar and Lt. Dr. Santhosh. "Detecting copy-move forgery in Digital images: A survey and analysis of current methods," Global Journal of Computer Science and Technology, vol. 10, no. 7, 2010.
6) WeiqiLuo,Jiwu Huang, GuopingQiu, "Robust Detection of Region- Duplication Forgery in Digital Image", 18th IEEE International Conference on Pattern Recognition, Hong Kong, p. 746 – 749, 2006.
7) Leida Li, Shushang Li, Hancheng Zhu, "An efficient scheme for detecting Copy-Move forged images by local binary patterns", Journal of Information Hiding and Multimedia Signal Processing, Vol. 4, No. 1, pp. 46-56, January 2013.
8) HieuCuong Nguyen and Stefan Katzenbeisser, "Detection of Copy- Move forgery in digital images using Radon transformation and phase correlation", IEEE Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Piraeu, 2012.
9) Preeti Yadav, Yogesh Rathore, "Detection of Copy-Move Forgery of Images Using Discrete Wavelet Transform", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 04 April 2012.
10) M. K. Johnson and H. Farid, "Detecting photographic composites of people,"in Proc. 6th Int. Workshop on Digital Watermarking, Guangzhou, China, 2007.
11) C. Riess and E. Angelopoulou. Physics-Based Illuminant Color Estimation as an Image Semantics Clue. In: Proceedings of the 16th IEEE International Conference on Image Processing(Page: 689 Year of Publication: 2009 ISBN: 978-1-4244-5653-6).

12) T. Takai, K. Niinuma, Difference Sphere: An Approach To Near Light Source Estimation Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition,(Page: 98 Year of Publication: 2004 ISBN: 0-7695-2158-4) .
13) S. Gholap and P. K. Bora, Illuminant colour based image forensics, in Proc. IEEE Region 10 Conf. 2008, pp. 1– 5. [9] C. Riess and E. Angelopoulou, Scene illumination as an indicator of image manipulation,Inf. Hiding, vol. 6387, pp. 66– 80, 2010.
14) Amerini, Irene, et al. "A sift-based forensic method for copy–move attack detection and transformation recovery." *Information Forensics and Security, IEEE Transactions on* 6.3 (2011): 1099-1110.
15) Lin, Hwei-Jen, Chun-Wei Wang, and Yang-Ta Kao. "Fast copy-move forgery detection." *WSEAS Transactions on Signal Processing* 5, no. 5 (2009): 188-197.
16) Deshpande, Pradyumna, and PrashastiKanikar. "Pixel Based Digital Image Forgery Detection Techniques." *International Journal of Engineering Research and Applications (IJERA)* 2.3 (2012): 539-54.
17) Reshma, P. D., and C. Arunvinodh. "Image forgery detection using SVM classifier." *Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on*. IEEE, 2015.