ISSN No.: 2454- 2024 (online)

International Journal of Technical Research & Science

Digital Image Forgery and Techniques of Forgery Detection: A brief review

Amandeep Kaur*, Jyoti Rani**
Email id: cse2010.amandeep3@gmail.com
Dept. of Comp Sci. and Engg. , Giani Zail Singh PTU Campus Bathinda

Abstract-Digital images are all around us-from our mobile phones to the pages of online websites. Digital images are used in almost every field whether it is information forensic, journalism, criminal and forensic investigations or medical fields and many more. Because of the large availability and popularity of user-friendly image editing tools and software it become easy to alter the images but such modified images pose some serious dangers or problems in some fields where the genuineness of image has a prime important and in such fields it become very difficult to verify the authenticity and probity of digital images. Digital image forgery is the process of tampering contents of an image that is changing the meaning of image without leaving any detectable clues. In this paper, we present a review of various types of digital image forgery and forgery detection techniques.

Index Terms- Digital Image Forensics, Image Forgery, Forgery Detection

www.ijtrs.com

1. INTRODUCTION

Digital image forgery deals with digital image. The process of creating fake image has been tremendously simple with the introduction of powerful computer graphics editing software such as Adobe Photoshop, GIMP, and Corel Paint Shop, some of which are available for free. There are many cases of digital image forgery. All of these cases can be categorized into three major groups, based on the process involved in creating the fake image. The groups are Image Retouching, Image Splicing, and Copy-Move Attack, Morphing.

Image Retouching can be considered to be the less harmful kind of digital image forgery. Image retouching does not significantly change an image, but instead, enhances or reduces certain feature of an image. This technique is popular among magazine photo editors. It can be said that almost all magazine cover would employ this technique to enhance certain features of an image so that it is more attractive; ignoring the fact that such enhancement is ethically wrong. Fig. 1.1 shows an original image of lady's face whereas fig. 1.2 shows the same face with enhanced effects applied to it.

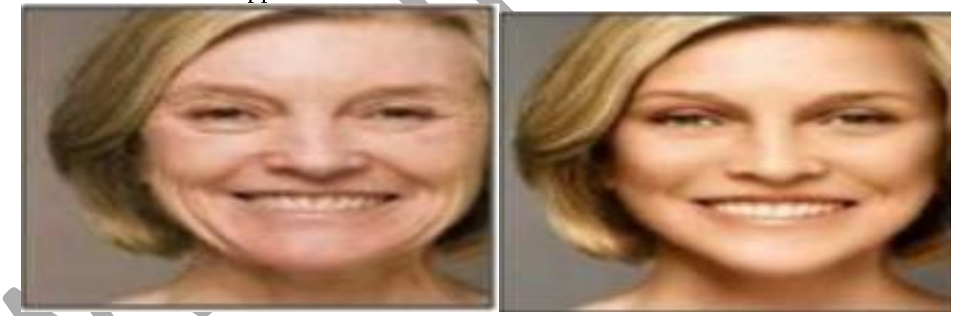

Fig. 1.1 (a) Original image **Fig. 1.1 (b) Enhanced image**

Image Splicing:

This technique is more aggressive than image retouching. Image Splicing is a technique that involves a composite of two or more images which are combined to create a fake image. Fig. 1.2 shows a base image. Fig. 1.3 shows shark inside sea. From Fig. 1.3 region occupied by shark is copied and it is pasted below the helicopter in the base image. This copy-paste operation from one image into another image forms a spliced image as shown in fig. 1.4.

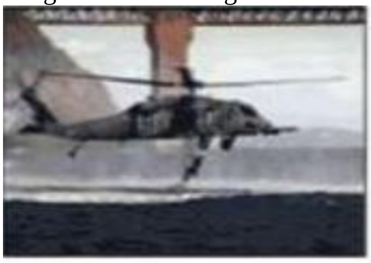

Fig. 1.2 Base Image

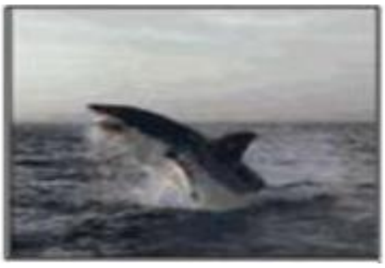

Fig. 1.3 Shark Image

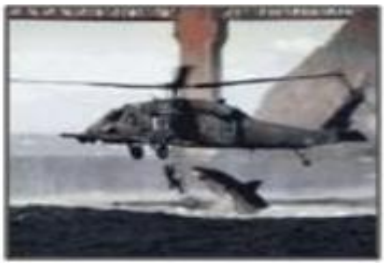

Fig1.4Base image with shark

Copy-move attack is more or less similar to Image Splicing in view of the fact that both techniques modify certain image region (of a base image), with another image. However, instead of having an external image as the source, copy-move attack uses portion of the original base image as its source. In other words, the source and the destination of the modified image originated from the same image. In a copy-move attack, parts of the original image is copied, moved to a desired location, and pasted. This is usually done in order to conceal certain details or to duplicate certain aspects of an image. Blurring is usually applied along the border of the modified region to reduce the effect of irregularities between the original and pasted region. Fig. 1.5 shows original image of a garden view. In Fig. 1.6 a region occupied by a deer is copied and pasted on the grass at front side in the same view.

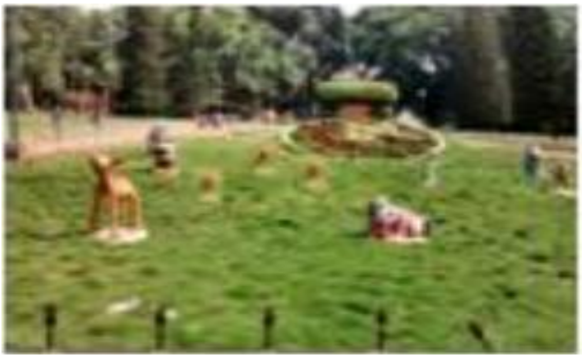

Fig. 1.5 Original Image

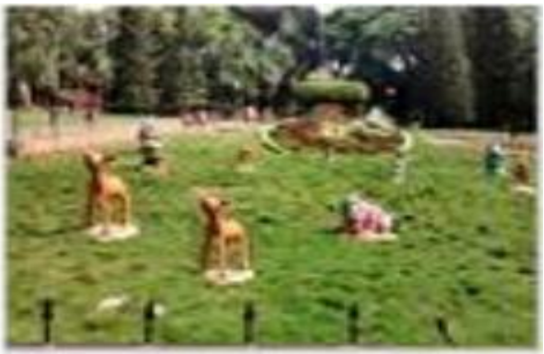

Fig. 1.6 Forged image

Morphing: It is a special effect in motion pictures and animations that changes one image or shape into another through a seamless transition. Most often it is used to depict one person turning into another through technological means or as part of a fantasy or surreal sequence.

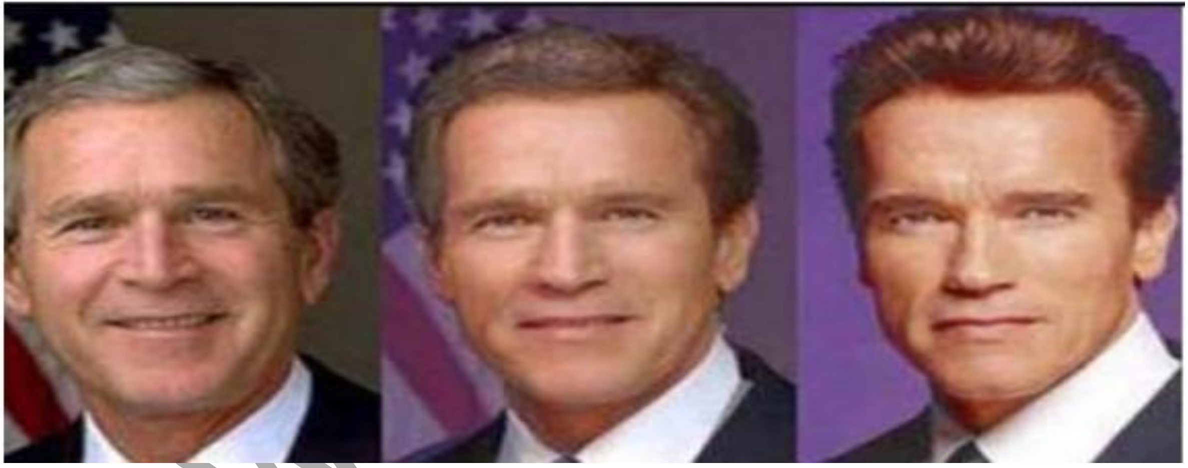

Fig. 1.7 (a) Original **Fig. 1.7 (b) Forged** **Fig. 1.7 (c) Original**

2. DIGITAL IMAGE FORENSICS

Digital Image Forensics is a quite recent discipline; nonetheless, it is tightly connected with a number of different research fields. DIF inherits its goals and attitude from classical (analog) forensic science and from the more recent field of computer forensics. Forensic disciplines in general aim at exposing evidence of crimes; to do so, they have to deal with the burglars' ability in either hiding or possibly counterfeiting their traces. In digital imaging both the acquisition process and the tampering techniques are likely to leave subtle traces. The task of forensics experts is to expose these traces by exploiting existing knowledge on digital imaging mechanisms, being aided by consolidated results in multimedia security research.

2.1 Applications of Digital Image Forensics

Digital forensics is commonly used in both criminal law and private investigation, Forensic analysis the images on online social networks, Used for detecting tampered or forged image, Image forgery detection system is needed in many fields for protecting copyright and preventing forgery or alteration of images. It is applied in areas such as journalism, scientific publications, digital forensic science, multimedia security, surveillance systems etc.

The copy-move forgery is one of the difficult forgeries to detect in image processing. It is common image tampering technique used now a day. In this some part of the image needs to be covered to add or remove information of an image.

2.2 Approaches to detect Digital Image Forgery

There are two approaches for detecting digital image forgery. One is active approach and the other is passive approach.

2.3 Active Approach

An active detection method which consists of adding image details in order to describe digital tampering such as name, date, signature, etc. It requires a special hardware implementation to mark the authentication of the digital image.

2.4 Passive Approach

Passive method detects the duplicated objects in forged images without need of original image watermark and depends on traces left on the image by different processing steps during image manipulation. Passive approach also determines the amount and the location of forgery in the image.

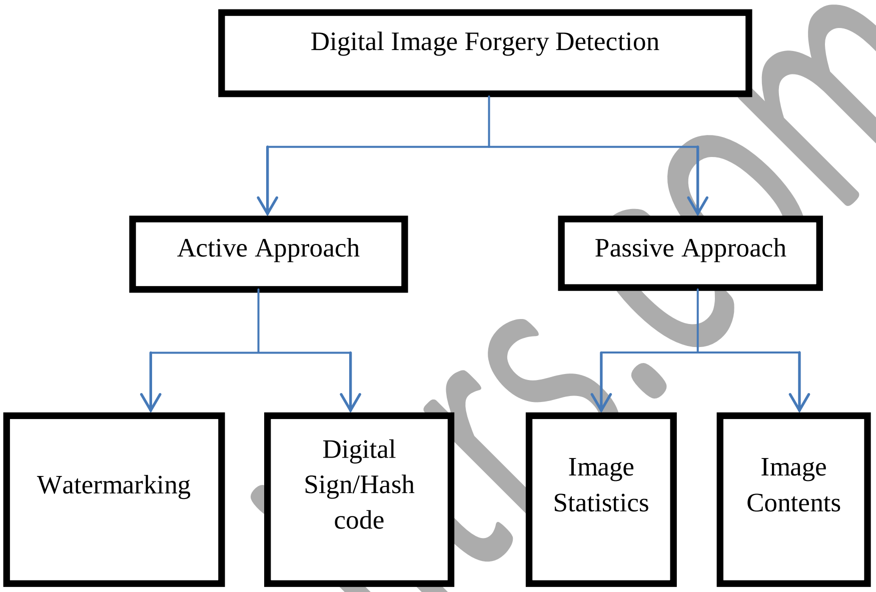

Fig. 2.1 Image Forgery Detection Approaches

3. LITERATURE SURVEY

I Amerini, et al. (2014) proposed a system which could evaluate the effectiveness of the attacking methods from the side of perceptual image quality; a new version of a SIFT key point removal method based on a perceptual metric. The author explained the criterion for the choice of the quality metric q(·) and then a comparison between the proposed system and Counter-forensics of SIFT-based copy-move detection by means of key point classification , both in terms of key point removal and in terms of final perceptual quality, is presented. Author has demonstrated that the proposed method obtains the lowest possible impact on visual quality with respect to the methods presented so far still achieving to remove a relevant number of key points.

Tu K. Huynh, et al.(2015) presented a survey on Image Forgery Detection (IFD) techniques applied for both Copy-Move and spliced images. The author has classified the algorithms on the basis of processing input images with or without transformation before extracting the image features for the copy- move images. For the spliced images, groups of detection techniques are based on image features or camera features. Reducing the complexity, increasing the detection rates, researching faster algorithms or building the large database to test is concluded.

Sushama Kishor Bhandare, et al.(2015) presented a review of the forensic methods for detecting globally and locally applied contrast enhancement, cut-and-paste forgery, histogram equalization, and noise in the digital image .Author has concluded that the techniques that are robust against the post processing operations and anti forensic techniques need to be developed.

Nandini Singhal, et al. (2015) presented a review of techniques for pixel based forgery detection. Two techniques presented in the paper are copy-move or cloning and fast-copy move detection. In copy-move or cloning technique a part of the image is copied and pasted into another part of the image which has limitation of only shifting of copied regions. In order to overcome this limitation another technique fast-

www.ijtrs.com

copy move detection having complex but precise results is discussed. But its main disadvantage is that it is not able to detect for very small region. Author has discussed a special type of forgery detection which can detect the duplicated regions accurately and quickly.

Harpreet Kaur, et al. (2015) presented different techniques to detect copy move forgery using block based method. Author has presented limitations of different techniques used for passive method to detect copy move forgery. Author has concluded that the comparative work can be extended by proposing a novel technique with which the existing limitations can be overcome.

Mohammad Farukh Hashmi, et al. (2015) presented an approach for image forgery authentication. Author has stated that a non morphed and non forged image shows homogeneity in non spectral domain. This homogeneity is lost when any forgery or morphing is applied on the images. Author proposed a system by applying a set of transform on the images. DCT statistics, LBP features with curvelet statistics and Gabor transform of the images has been combined to represent an image in the transformed domain. CASIA image dataset with seven thousand authentic and same numbers of tempered images is used to verify the technique. Dataset is divided into two equal halves to perform training and testing. Transformed images are used to train Hidden Markov model as HMM can extract probabilistic state information from a large statistical model. Test images are tested in transformed domain by HMM with log likelihood estimator. In case HMM returns an indeterminist result or multiple subset of result, the transformed test image was tested with two class SVM classifier with RBF kernel. The system shows the accuracy of over 89% for 500 test instances. Sensitivity and Specificity were found to be 90% and 88% respectively.

Snigdha K. Mankar, et al. (2015) studied various techniques like the SVM classifier, Pixel-based and partition-based to detect forgery of images. Author has concluded that multimedia authentication techniques have emerged to verify content integrity and prevent forgery of images.

Jessica Fridrich, et al proposed a system to detect malicious manipulation with digital images. The proposed system, implemented in C, may successfully detect the forged part even when the copied area is enhanced/ retouched to merge it with the background and when the forged image is saved in a lossy format, such as JPEG. The performance of the proposed method is demonstrated on several forged images.

4. COPY-MOVE FORGERY DETECTION TECHNIQUES

A number of techniques are available to detect copy-move forgery which can be classified into two main categories such as block-based and key point-based methods.

4.1 Blocks-based methods

In block-based methods, the image will be divided into overlapping blocks of specified size and a feature vector will be computed for these blocks. Similar feature vectors are then matched to find the forged regions. For e.g. DCT, DWT, PCA, KPCA etc.

4.2 Features matching-based methods

In this category, feature vectors are computed for regions with high entropy. There is no subdivision into blocks. The feature vectors are matched to find the copied blocks. The well-known key-point detectors are Harris, SIFT, SURF and FAST. For instance, the Scale Invariant Features Transform (SIFT), which is invariant to illumination, scaling, rotation and JPEG compression.

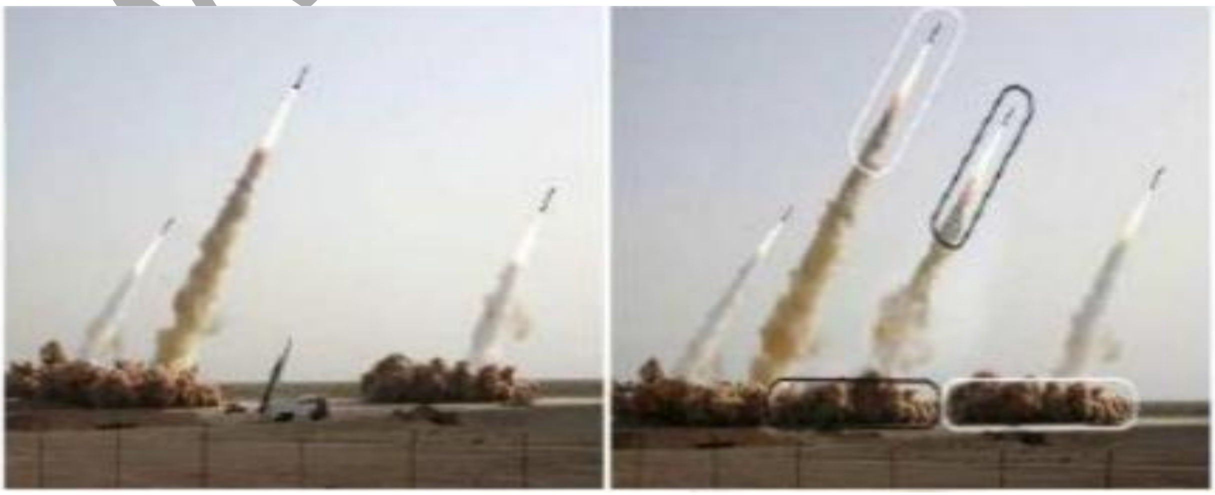

Fig. 4.1 Example of copy-move attack on images

www.ijtrs.com

General process of image forgery detection includes the following steps:

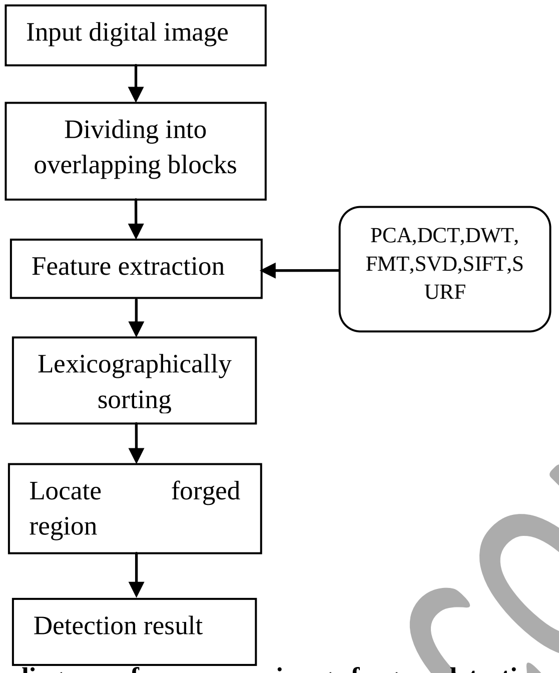
Input digital image
Dividing into overlapping blocks
Feature extraction
PCA,DCT,DWT, FMT,SVD,SIFT,SURF
Lexicographically sorting
Locate forged region
Detection result

Fig. 4.2 Block diagram of copy-move image forgery detection system

PCA: Principal Component analysis, DCT: Discrete Cosine transform, DWT: Discrete Wavelet transform, SVD: Singular Value decomposition, SIFT: Scale Invariant Feature transform, SURF: Speeded up Robust features.

Principle Component Analysis (PCA) is a candidate to extract the image features [9]. In the Dartmouth Computer Science Technical Report of 2004, Alin C Popescu and Hany Farid used PCA to automatically detect duplicated regions in a digital image. The technique works by first applying a principal component analysis to small fixed-size image blocks to yield a reduced dimension representation. The representation is robust to minor variations in the image due to additive noise or lossy compression. Duplicated regions are then detected by lexicographically sorting all of the image blocks. The efficiency of the proposed technique on credible forgeries, and its robustness and sensitivity to additive noise and lossy JPEG compression has been shown by the author.
The procedure to produce each feature vector is called principle component analysis in which values are obtained by using the theorems of covariance matrix, eigenvectors and linear basis for each image block with the initial conditions of zero-mean. Then a matrix S of block vectors quantized according to number of quantization bins to reduce the mirror variations created. These quantization coefficients are then sorted lexicographically and the duplicated regions has been detected by considering the offset of all pairs whose distances in S less than a specific threshold. To obtain the efficient results, a duplication map is defined by producing a zero image of the same size as original and assigning all pixels in a duplicated region to a unique grayscale value. With the dimension of the PCA reduced representation and total number of image pixels are N_t and N respectively, the algorithm has complexity of O(N_tNLogN).

4.3. DCT, DWT

Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are popular techniques to transform an input image to the frequency domain before extracting the image features.
Jessica Fridrich, et.al [8] used quantized Discrete Cosine Transform (DCT).The feature vectors are vectors of quantized DCT coefficients. The quality factor in JPEG compression determines the quantization step for DCT transform coefficients which is called the user-specified parameter Q. The mutual positions are considered in case of too many matching blocks having the same shift vector to define a specific block pair. For the color images, the algorithm requires a color to grayscale conversion. It takes MNlog2(MN) steps in exact match.
Discrete Wavelet Transform (DWT) is always the potential candidate for research on CMFD. In fact, many proposed algorithms to detect Copy-Move regions using DWT coefficients. Nandini Singhal, et. al [4] proposed a system using DWT to detect pixel-based forgery. A forged image is taken as an input image. DWT is applied to the input image to yield LL1 sub-band. The LL1 sub-band is divided into sub-images. Then phase correlation is calculated. The offset between the copy-move regions is also calculated. The copy-move region is

www.ijtrs.com

found out by pixel matching. Then MMO (Mathematical Morphological Operations) is applied to detect the result.

4.4 SIFT, SURF

Scale Invariant Features Transform (SIFT)presents a method for extracting distinctive invariant features from images that can be used to perform reliable matching between different views of an object or scene in given image. The features are invariant to different scale and rotation, and provide robust matching across a large range of affine transformation, distortion, change in 3D viewpoint, addition of noise, and change in illumination. The features are highly distinctive and a single feature can be correctly matched with high probability against a large database of features of image and video. SURF is a scale and rotation invariant interest point detector and descriptor. It can be computed and compared much faster than other image features like SIFT and HOG.

When some object is copy-moved with the help of geometrical and illumination transform, it becomes difficult to detect that object. Speed up Robust Feature (SURF) and Scale Invariant Feature Transform (SIFT) are invariant with respect to geometrical and illumination transform. Ramesh Chand Pandey, et. Al (2014) [10] proposed a method to detect copy move forgery in an image based on passive forensic scheme. The proposed method used SURF and SIFT, which make it very fast and robust in detecting copy-moved regions. To achieve very fast speed in copy-move forgery detection, SURF image features are used to find the image key-points (interest points) and extract their64 dimensional descriptor which is used for rapid matching. The purposed system reads an image. Image key-points / interest points are detected via SURF key-point detector. The descriptors for the key-points are computed using SURF key-point descriptor. The best ten matches are identified for every key-point. g2NN matching (g2NN-generalized 2 nearest neighbor) is applied. The dynamic thresholding step is performed. The matched key-point are joined using a line to represent the copied region.

CONCLUSION

The paper surveys the different types of digital image forgery, approaches to detect digital forgery. Specifically pixel-based forgery detection techniques are discussed. All the methods and approaches discussed in this paper are able to detect forgery. But some algorithms are not effective in terms of detecting actual forged region. On the other hand some algorithms have a very high time complexity. So, there is a need to develop efficient and accurate image forgery detection algorithm, either by combining the existing techniques or by developing new techniques.

REFERENCES

[1] I Amerini, F. Battisti, R. Caldelli, M. Carli, A. Costanzo, “Exploiting Perceptual Quality Issues In Countering SIFT-Based Forensic Methods”, IEEE International Conference on Acoustic, Speech and Signal Processing (ICASSP), p. 2664-2668, 2014.

[2] Tu K. Huynh, Thuong Le-Tien, KhoaV.Huynh, SyC.Nguyen, “A Survey on Image Forgery Detection Techniques”,The 2015 IEEE RIVF International Conference on Computing & Communication Technologies Research, Innovation, and Vision for Future (RIVF), p. 71-76, 2015.

[3] Sushama Kishor Bhandare, Nitin Krishnarao Bhil, “Digital Image Forensic”, International Journal of Advance Research in Computer Science and Software Engineering, p. 839-842, 2015.

[4] Nandini Singhal, Savita Gandhani, “Analysis of Copy-move Forgery Image Forensics: A Review”, International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.8, No.7, pp.265-272, 2015.

[5] HarpreetKaur, KamaljitKaur, “A Brief Survey of Different Techniques for Detecting Copy-Move Forgery”, International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 4, p. 875-882, 2015

[6] Mohammad FarukhHashmi, Avinash G. Keskar, “Image Forgery Authentication and Classification using Hybridization of HMM and SVM Classifier”, International Journal of Security and Its Applications Vol. 9, No. 4, pp. 125-140, 2015.

[7] Snigdha K. Mankar, Prof. Dr. Ajay A. Gurjar, “Image Forgery Types and Their Detection: A Review”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, April 2015.

[8] Jessica Fridrich, David Soukal, and Jan Lukáš, “Detection of Copy Move Forgery in Digital Images”, Digital Forensic Research Workshop, Cleveland, Ohio, USA, 2003

[9] Alin C Popescu and HanyFarid, “Exposing Digital Forgeries by Detecting Duplicated Image Regions”, Dartmouth Computer Science Technical Report TR2004-515, USA, August 2004.

www.ijtrs.com

[10] Ramesh Chand Pandey, Sanjay Kumar Singh, K. K. Shukla and RishabhAgrawal, "Fast and Robust Passive Copy-Move Forgery Detection Using SURF and SIFT Image Features".

[11] MohdDilshad Ansari, S. P. Ghrera and VipinTyagi, "Pixel-Based Image Forgery Detection: A Review", IETE Journal of Education, 55:1, 40-46, 2014.

[12] Andrea Costanzo, Irene Amerini, Roberto Caldelli and Mauro Barni, "Forensic Analysis of SIFT Keypoint Removal and Injection", IEEE Transactions on Information Forensics and Security, VOL. 9, NO. 9, september 2014

www.ijtrs.com