Global Journal of Computer Science and Technology
Graphics & Vision
Volume 13 Issue 9 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Methodology for Evidence Reconstruction in Digital Image Forensics

By Kalpana Manudhane & Mr. M.M. Bartere
G.H. Riasoni College of Engineering & Management, India

Abstract- This paper reveals basics of Digital (Image) Forensics. The paper describes the ways to manipulate image, namely, copy-move forgery (copy region in image & paste into another region in same image), image splicing (copy region in image & paste into another image) and image retouching. The paper mainly focuses on copy move forgery detection methods that are classified mainly into two broad approaches – block-based and key-point. Methodology (generalized as well as approach specific) of copy move forgery detection is presented in detail. Copied region is not directly pasted but manipulated (scale, rotation, adding Gaussian noise or combining these transformations) before pasting. The method for detection should robust to these transformations. The paper also presents methodology for reconstruction (if possible) of forged image based on detection result.

Keywords: *digital forensics, copy-move forgery, keypoint, feature extraction, reconstruction.*

GJCST-F Classification: *I.4.0*

Strictly as per the compliance and regulations of:

Methodology for Evidence Reconstruction in Digital Image Forensics

Kalpana Manudhane [α] & Mr. M.M. Bartere [σ]

Abstract- This paper reveals basics of Digital (Image) Forensics. The paper describes the ways to manipulate image, namely, copy-move forgery (copy region in image & paste into another region in same image), image splicing (copy region in image & paste into another image) and image retouching. The paper mainly focuses on copy move forgery detection methods that are classified mainly into two broad approaches – block-based and key-point. Methodology (generalized as well as approach specific) of copy move forgery detection is presented in detail. Copied region is not directly pasted but manipulated (scale, rotation, adding Gaussian noise or combining these transformations) before pasting. The method for detection should robust to these transformations. The paper also presents methodology for reconstruction (if possible) of forged image based on detection result.

Keywords: digital forensics, copy-move forgery, keypoint, feature extraction, reconstruction.

I. Introduction

With the rapid development of computer networks, almost the daily work of all trades is more and more dependent on computer. As a result, high-tech crimes, commercial fraud and other phenomena involve computers. So, people pay more & more attention to digital forensics. Digital forensics is concerned with the use of digital information (image or document file) as source of evidence in investigations and legal proceedings. This paper focuses on image as evidence.

Digital image forensics has emerged as a new research field that aims to reveal tampering in digital images [1]. Tampering the image means illegally manipulating image with intent to damage.

From the early days an image has generally been accepted as a proof of occurrence of the depicted event. Use of digital image in almost all fields has become a common practice. The availability of low-cost hardware and software, make it easy to create, alter, and manipulate digital images As a result, we are rapidly reaching a situation where one can no longer take the integrity and authenticity of digital images for granted [2]. So, detecting forgery in digital images is an emerging research field. In the recent years large amount of digital image manipulation could be seen In magazine, fashion Industry, Scientific Journals, Court rooms, main media outlet and photo hoaxes we receive in our email.

Digital image forensics is called passive [3] if the forensic investigator cannot interfere with the image generation process. On the other hand, for Active approaches the generation process is purposely modified at an earlier stage to leave behind identifying traces. Typical instances of active approaches attach metadata to the image e. g., a cryptographic signature or a robust hash or embed a digital watermark directly into the image itself.

Digital image forensics is called blind [3] if the forensic investigator is confined to examine the final output of the generation process. In particular, knowledge neither of the original scene nor any intermediate result of the generation process is available at the time of analysis. Contrary, Non–blind forensic investigators have such a data available. Such data may be available from alternative sources (for instance, earlier versions of a processed image that have been published elsewhere). This paper focuses on passive–blind image forensics.

Digital Image Forensics can be subdivided into three branches as-1) image source identification; 2) Computer generated image recognition and 3) Image forgery detection. Further, digital image forgery categorized in three groups [4]- Copy-Move, Image splicing and Image retouching. Copy-Move forgery or Region-Duplication forgery is the most important type of forgery, in Copy-Move some part of the image copies and pastes into another part of the same image to create a new thing or to hide an important scene. Image splicing is the procedure of creating a fake image by cutting one part of an image and paste it to another image. Image Retouching doesn't obviously change the image, it just enhance some features of image. It is famous among magazine photo editors and most of magazine covers use this technique to change some features of an image but it is ethically wrong.

The rest of paper is organized as follows. Section II reveals literature survey. In section III, the details of the block-based and keypoint-based method are presented with the general flowchart of the methods.

Section IV gives details to reconstruct image based on detection results. Section V gives details of comparison metrics and dataset. Section V describes factors to be considered to prove robustness of method. Proposed system & conclusion is presented at the end.

Author α: G.H. Riasoni College of Engineering & Management, Amravati, Maharashtra, India.
Author σ: G.H. Riasoni College of Engineering & Management, Amravati, Maharashtra, India.

II. Literature Survey

Detection of Copy-Move forgery is difficult as compared to other forgeries because the source and destination of forgery is same image, also the original image segment and the pasted one have same properties such as dynamic range, noise component and color palette.

The simplest way to detect a Copy-Move forgery is to use an exhaustive search. In this approach, the image and its circularly shifted version are overlaid looking for closely matching image block. This approach is simple and effective for small-sized images. However, this method is computationally expensive and even impractical for medium size image. Another technique for detecting forgery is based on autocorrelation. All Copy-Move forgery introduces a correlation between the original segment and the pasted one. Though this method does not have large computational complexity it often fails to detect forgery.

Basically, given an original image, there are two approaches for Copy move forgery detection (CMFD) - block-based and keypoint-based. Block-based method subdivide image into blocks, whereas keypoint-based method searches keypoints in image without dividing the image. Although a large number of CMFD methods have been proposed, most techniques follow a common pipeline, as shown in Fig.1. According to approach selected, each phase has different working methodology. Let us see these phases in brief [5]

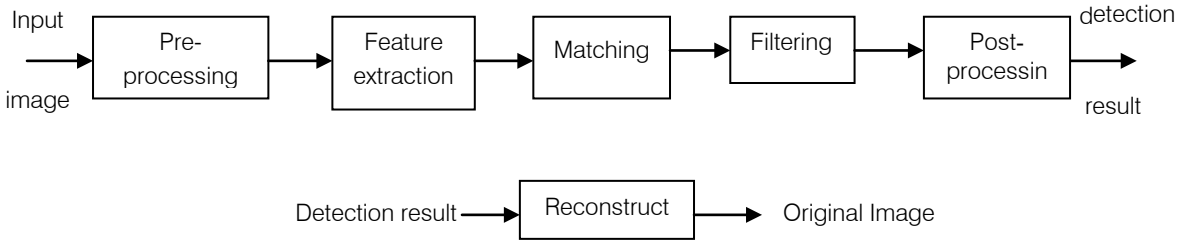

Figure 1 : Common processing pipeline for detection of copy-move forgery & image reconstruction

Most methods operate on grayscale images. So, preprocessing involves color image to be converted to grayscale image. In feature extraction, a feature vector is computed for block or keypoint. Similar feature vectors are subsequently determined in matching step.

High similarity between two feature descriptors is interpreted as an indication for a duplicated region.

Filtering schemes have been introduced in order to reduce the probability of false matches. For instance, neighboring pixels often have similar intensities, which can lead to false forgery detection.

Different distance criteria were also proposed in order to filter out weak matches. The goal of this last phase i.e. post-processing is to preserve matches that exhibit a common behavior. A set of matches that originate from the copy-move action are expected to be spatially close to each other in both the source and the target blocks or keypoints. Furthermore, these matches should exhibit similar amounts of translation, scaling and rotation. In reconstruction, we try to recover original image if possible.

Literature survey of CMFD methods is as follows-

Fridrich et al. (2003) [6] is the first to propose CMFD method. In this method, image is divided into overlapping small blocks. Then he used of discrete cosine transform (DCT) as block feature, this method is not robust to transformation. B. Mahdian and S. Saic (2007)[7] used blur invariant moments as block feature. S. Ryu, M. Lee and H. Lee (2010) [8] use of magnitude of zernike moments as a feature of block. The method is invariant to rotation but still weak for scale & other affine transformation. Somayeh Sadeghi et al. (2012) [4] had used Fourier transform as block feature, though computation time is improved, the method is not so much accurate. Other block-based methods are based on-DWT (Discrete Wavelet Transform), PCA (Principle Component Analysis), Hu moment, SVD (Singular Value Decomposition) and KPCA (kernel-PCA) etc. These block-based methods accurately detect forged region, but require more computation time and memory.

B. L. Shivakumar and S. Baboo (2011) [9] uses SURF (Speeded Up Robust Features) as keypoint feature. The method detects forgery with minimum false match for images with high resolution. But it failed to detect small copied regions. I. Amerini et al.(2011) [10] presented a new technique based on Scale invariant Feature Transform (SIFT) [11] features to detect and localize copy-move forgeries. G2NN method is used for keypoint matching and clustering is used to detect forgery. The method also deals with multiple cloning.

The method also determines geometric transformation. Xunyu Pan(2011) [1][12], in his dissertation, detect region duplication by using Scale invariant feature transform(SIFT) method to extract keypoint and Best-bin-first algorithm for keypoint matching. His method also deals with geometric transformation. These keypoint based methods show good performance with very less computation time and minimum memory requirement.

So, it can be concluded that though block-based methods improve detection result, keypoint based methods are more efficient if we consider factors

of computation time and memory requirement. They are reliable and give good performance in case of affine transformation such as large scaling and rotation as compared to block-based methods. However, keypoint based methods are sensitive to low-contrast and repetitive image contents.

III. Approaches to CMFD

As it is cleared that there are basically 2 approaches to CMFD, namely, block-based and key-point based, let us see methodology in depth for each.

a) Block-based approach

Firstly, image is subdivided into overlapping or non-overlapping blocks. For detecting forged area, the characteristics of each block of the image calculated and compared with each other.

Fig.2 shows the general procedures of detecting block-based copy-move forgery.

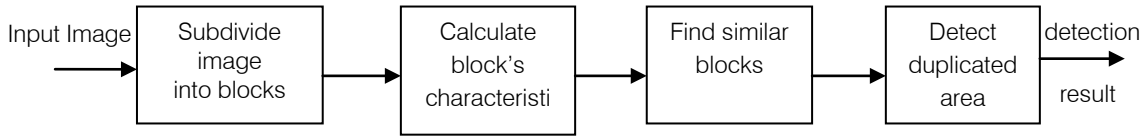

Figure 2 : Block-based CMFD procedure

Extracting image features or characteristics can be done by different technique as discussed in Literature survey such as frequency based approaches(DCT, DWT, FT, etc), moment-based approaches (blur, Zernike), dimension-reduction techniques(PCA, SVD, KPCA).

Similar blocks are identified by lexicographic sorting. In lexicographic sorting a matrix of feature vectors is built so that every feature vector becomes a row in the matrix. This matrix is then row-wise sorted. Thus, the most similar features appear in consecutive rows. Similarity criteria may be Euclidian distance, correlation etc.

The block size also affects performance of algorithm. If it is very large then can not locate small copied regions. If it is too small, more computation time and memory will be required. 16×16 will be choice of most researchers.

b) Keypoint-based approach

The first step in keypoint-based method is to find image keypoints and collect image features at the detected keypoints. Keypoints[1] are locations that carry distinct information of the image content. Each keypoint is characterized by a feature vector that consists of a set of image statistics collected at the local neighborhood of the corresponding keypoint. Fig.3 shows the general procedures of detecting keypoint-based copy-move forgery [10].

Figure 3 : keypoint-based CMFD procedure

c) Keypoint extraction methods

SIFT (Scale Invariant Feature Transform) is one of the methods to extract keypoint. SIFT keypoints are found by searching for locations that are stable local extrema in the scale space[11]. Scale space is obtained by Gaussian and difference of Gaussian. At each keypoint, a 128 dimensional feature vector is generated from the histograms of local gradients in its neighborhood. To ensure that the obtained feature vector is invariant to rotation and scaling, the size of the neighborhood is determined by the dominant scale of the keypoint, and all gradients within are aligned with the keypoint's dominant orientation. Furthermore, the obtained histograms are normalized to unit length, which renders the feature vector invariant to local illumination changes.

Another method proposed by Herbert Bay et. al. for fast detectors and descriptors, called SURF (Speeded Up Robust Features). SURF's detector and descriptor is said to be faster and at same time robust to noise, detection displacements and geometric and photometric deformations.

d) Keypoint matching methods

Given a test image, a set of keypoints X={x1,….,xn} with their corresponding SIFT descriptors {f1,….,fn} are extracted. Best-Bin-First search method derived from the kd-tree algorithm (bins in feature space are searched in the order of their closest distance from the query location) used to get approximate nearest neighbors. Matching with a kd-tree yields a relatively efficient nearest neighbor search. The Euclidean

distance is used as a similarity measure. It has been shown that the use of kd-tree matching leads, in general, to better results than lexicographic sorting, but the memory requirements are significantly higher.

Another is the 2NN algorithm. For the sake of clarity let D={d1, d2, ,….,dn-1} gives sorted Euclidean distance of a keypoint with respect to other keypoint descriptors. The keypoint is matched only if following condition is satisfied

$$d_1/d_2 < T \quad where\ T \in (0,1) \qquad (1)$$

That's why this procedure is called as 2NN test. Drawback of this method is cannot handle multiple keypoint matching. So, Amerini et. al. [10] proposed generalized 2NN test (called as g2NN) starts from the high dimensional feature space such as that of SIFT features. The generalization consists of iterating the 2NN test between d_*i*/d_(i+1) until this ratio is greater than T (in their experiments this value is set to 0.5). Finally, by iterating over each keypoints, we can obtain the set of matched points. All the matched keypoints are retained, but isolated ones are discarded. But it can be possible that images that legitimately contain areas with very similar texture yield matched keypoints that might give false indicator.

IV. Clustering

Cluster is a collection of data objects such as objects that are similar to one another will be placed within the same cluster and dissimilar objects to the clusters. Clustering problem is to find similarities between data according to the characteristics found in the data and group similar data objects into clusters.

There are various approaches to clustering discussed in brief as follows-

Cluster analysis[13] try to subdivide a data set X into C subsets (clusters) which are pair wise disjoint, all non-empty and reproduce X via union. These clusters are termed as hard clusters (non-fuzzy). Whereas fuzzy clusters allow one piece of data to belongs to two or more clusters. C-means clustering is fuzzy based while k-means is hard clustering. Hierarchical clustering [10] creates a hierarchy of clusters which may be represented by a tree structure. The algorithm starts by assigning each keypoint to a cluster; then it computes all the reciprocal spatial distances among clusters, finds the closest pair of clusters, and finally merges them into a single cluster.

Other major clustering approaches are partitioning, Density-based, grid-based, model-based, frequent-pattern-based and constraint-based. Swarm optimization based approaches such Particle swarm optimization and Ant colony optimization can also be successfully applied to clustering [14].

a) Comparison between Block-based and Keypoint based approach

Comparison in simple terms is represented in following table-

	Block-based approach	Keypoint based approach
1	Subdivide image into blocks for feature extraction	Without dividing image determine keypoints for feature extraction
2	Feature vector matching is done mostly by lexicographic sorting	Feature vector matching is done by 2NN, g2NN, best-bin-first algorithm
3	Cannot detect large transformations	Can detect large transformations
4	More memory required and consequently more computation time	Less memory and computation time as keypoints are less in number
5	More accurately detect duplication	Some what less accurate

V. Image Reconstruction

After detection of forgery, next step is to try to reconstruct image to original. If forgery is done for highlight something and background is simple then it can be reconstructed easily by region growing. But if forgery is to hide something underlying then it is not possible to reconstruct it. Further more detection method is not able to distinguish original and copied region. It just claims that two regions are identical to each other. If we assume that copied region is one on which some transformations are performed. But in that case it will confuse in situation in which there is plain copy-move (without any transformation). In that case we will assume first region encountered is original and second is duplicated. Let us see region growing in brief.

a) Region Growing

As name suggests, region growing is a procedure that group pixels or sub-regions into larger regions based on predefined criteria for growth [15]. The basic idea is to start with a set of seed points and from these grow regions by appending to each seed those neighboring pixels that have predefined properties

similar to the seed (such as specific intensity range or color). Following are the problems in region growing where decision is needed to be taken.

- Selecting a set of one or more starting points many times can be based on the nature of problem. When the prior information is not available, set of properties at every pixel is needed to be computed, so that can be used to assign pixels to regions during growing process. If these computation results in clusters, then pixels whose properties place them near the centroid of these clusters can be used as seeds.
- Selection of similarity criteria depends on problem under consideration and type of image data available.
- Formulation of stopping rule is another problem. The growing process should stop when no more pixels satisfy criteria for inclusion in that region. Additional criteria to increase power of algorithm are- size, likeliness between candidate pixel, shape of region being grown, pixels grown so far etc..

VI. Comparison Metrics & Dataset

There should be a criteria on basis of which various methods can be compared. Measures for checking performance of method are mainly Precision, p, and Recall, r [5]. They are defined as:

$$p = \frac{T_P}{T_P + F_p} \qquad r = \frac{T_P}{T_P + F_n} \tag{2}$$

Where, T_P = number of correctly detected forged images,

F_p = number of images that have been erroneously detected as forged,

and F_n = number of falsely missed forged images.

Here, precision denotes the probability that a detected forgery is truly a forgery; while recall shows the probability that a forged image is detected. Recall is often also called true positive rate. Score F1 is a measure which combines precision and recall in single value given as follows-

$$F_1 = 2 \cdot \frac{p \cdot r}{p + r} \tag{3}$$

Along with this traditional measures such as memory requirement and computation time are also significantly considered.

Now, question arises – on which images we can test our method? Amerini et al. have published two ground truth databases for CMFD, namely, MICC F220 and MICC F2000 consists of 220 and 2000 images respectively. Half of images are tampered. The image size is 2048×1536 pixels. Type of processing is limited to rotation and scaling. Also original image is not available. Fig. shows some of images of dataset MICC-F8multi.

Figure 4 : Forged images of dataset MICC-F8multi

Another one is a project1ims set of 5 object images (named [name].pgm, where [name] = {book1, book2, kit, ball, juice} is the object shown), and two sets of 10 cluttered scene images. One set is the training set and the images are named Img0[i].pgm, where i=1...10.

The other set is the test set, and the images are named TestImg0[i].pgm, where i=1...10. Every image (in training and test sets) contains 0-5 of the objects represented in the object images. Each object is contained in exactly five images in each set (training and test), and is not present in the other five. There is a file gt.txt, which contains the ground truth for the cluttered images - it shows which of the five objects are present in each images. Steps to analyze method is as follows-

1. By looking through the images and comparing to the ground truth, make sure that how the two are related.
2. Using the method to be analyzed, compute the number of matches between each object image and each training image. You should compute a 5x10 matrix of integers.
3. Design a simple classifier for each object separately (based only on the training data) that tells whether the object is present in an image by thresholding the number of matches.
4. Evaluate your classifier on each image in the training set. Note: Designing a classifier means coming up with a method for computing a threshold based only on the training data, which will eventually work well on test data. An example of such a method is to set the threshold to the largest number of matches for an image that did not contain the object. Another is to set the threshold to the smallest number of matches for an image that did contain the object.
5. Now compute the number of matches between the each object image and each test image. Again, you should compute a 5x10 matrix of integers. Using your classifiers, classify each test image now as either containing each object or not.
6. Compare your classifications to the ground truth. You should compute the number of misses (number of images that contained the object that were classified as not containing the object) and the number of false positives (number of images that do not contain the object that were classified as containing the object). Ideally, you want zero in both.

VII. Robustness of Method

Method for CMFD should able to detect forgery invariant to rotation, (up and down) scaling, noise added to copied region before pasting it. Also method is expected to detect combinations of these manipulations. Method should detect multiple copies of the same region. Also, the method be able to detect multiple forgeries i.e. more than one region copied and pasted. Let us consider these factors one by one.

a) Scale and rotation invariance

If copied region is up-scaled or down-scaled then pasted, method should detect it accurately. Bayram et. al.[16] suggested a method by applying Fourier Mellin Transform (FMT) on the image block. The authors showed that their technique was robust to compression up to JPEG quality level 20 and rotation with 10 degree and scaling by 10%.

Hwei-Jen Lin et. al. [17] proposed a method in which each block B of size 16x16 by a 9-dimensional feature vector. The feature vector extracted stored in floating numbers is converted into integer values for fast processing and then sorted using the radix sort, which makes the detection more efficient without degradation of detection quality. The difference (shift vector) of the positions of every pair of adjacent feature vectors in the sorted list was computed and then evaluated and the large accumulated number was considered as possible presence of a duplicated region. The scheme performed well when the degree of rotation was 90, 180 and 270 degree. The figure 5 [2] shows duplicated region with and without rotation.

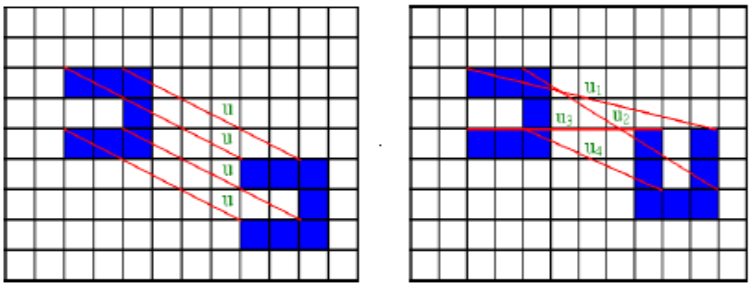

Figure 5 : (a) Duplicated regions form several identical shift vector u. (b) Duplicated region from several (different) shift vector(u1 u4) , rotated through 90 degree.

We already seen than the method scale invariant features transform (SIFT) is more robust for scaling and Zernike moments based method is robust to rotation.

b) Robustness to Gaussian noise

Copied region is not just pasted but often some noise is added to it before pasting. Gaussian noise [15]

represents statistical noise having probability distribution function equal to normal distribution. Gaussian noise model is frequently used in image processing.

Irrespective of noise added either in small or large in mount, method should choose to leave the ground truth clean [5].

c) Robustness to combined transformation

The method is robust if it can detect combined transformation consisting of rotation, scale and Gaussian noise.

d) Detection of multiple copies of same region

This factor depends on algorithm used for keypoint/block feature vector matching. 2NN algorithm is not able to detect multiple copies while g2NN is able to detect.

e) Robustness to multiple copy-move

The method should detect multiple forgeries of copy-move with accuracy. Note that performance of method should not become less for one factor when trying to attempt to improve another factor.

f) Complexity of algorithm

Though lot of work is done in the field of copy move forgery detection, methods are very complex. If we want to achieve above factors, complexity further increases. Some simplification in current approaches or different way of approaching the problem is needed.

VIII. Proposed System

We will try to implement keypoint-based Scale Invariant Feature Transform (SIFT) algorithm for keypoint and feature extraction; generalized 2NN (g2NN) algorithm for keypoint feature matching; fuzzy c-means clustering for forged region detection. Hope so, almost all types of transformations being detected. We will also try to reconstruct original image whenever possible using region growing algorithm.

IX. Conclusion

This paper gives basic of Digital (Image) Forensics. The paper also put light on the ways to image manipulation, namely, copy-move forgery, image splicing and image retouching. The literature survey is presented for copy move forgery detection methods that are classified mainly into two broad approaches- block-based and key-point. Methodology (generalized as well as approach specific) of copy move forgery detection is presented in detail. Many authors have proposed good methods with lot of experiments. Some authors also provided dataset for experimental testing. Though lot of work had been done in the field of copy move forgery detection, methods are very complex. If we want to achieve robust method against all manipulations complexity further increases. Some simplification in current approaches or different way of approaching the problem is needed. Accuracy is also needed to be improved. This paper make familiar to new researchers in this field with current methodology and robustness requirement for the methods to be proposed.

References Références Referencias

1. Xunyu Pan, "Digital Forensics Using Local Signal Statistics", A Dissertation, 2011.
2. B.L.Shivakumar1 Lt. Dr. S.Santhosh Baboo," Detecting Copy-Move Forgery in Digital Images: A Survey and Analysis of Current Methods", Global Journal of Computer Science and Technology Vol. 10 Issue 7 Ver. 1.0, pp.61-65, 2010.
3. Matthias Kirchner, "Notes on Digital Image Forensics & counter forensics", pp.1-97, 2012.
4. Somayeh Sadeghi, Hamid A. Jalab, and Sajjad Dadkhah," Efficient Copy-Move Forgery Detection for Digital Images", World Academy of Science, Engineering and Technology, pp. 755-758, 2012.
5. Vincent Christlein, Christian Riess, Johannes Jordan, Corinna Riess, and Elli Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches", ieee Transactions On Information Forensics And Security, pp. 1-26, 2012.
6. Fridrich, D. Soukal, and J. Lukas, "Detection of copy-move forgery in digital images," in Proceedings of Digital Forensic Research Workshop, Aug. 2003.
7. B. Mahdian and S. Saic, "Detection of Copy-Move Forgery using a Method Based on Blur Moment nvariants," Forensic Science International, vol. 171, no. 2, pp. 180–189, 2007.
8. S. Ryu, M. Lee, and H. Lee, "Detection of Copy-Rotate-Move Forgery using Zernike Moments," in Information Hiding Conference, pp. 51–65, Jun. 2010.
9. B. L. Shivakumar and S. Baboo, "Detection of Region Duplication Forgery in Digital Images Using SURF," International Journal of Computer Science Issues, vol. 8, no. 4, pp. 199–205, 2011.
10. I.Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, and G. Serra, "A SIFT-based Forensic Method for Copy-Move Attack Detection and Transformation Recovery," IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 1099–1110, 2011.
11. DAVID G. LOWE, "Distinctive Image Features from Scale-Invariant Keypoints", International Journal of Computer Vision 60(2), pp.91–110, 2004.
12. Xunyu Pan and Siwei Lyu, "Detecting Image Region Duplication using SIFT features", pp.1-4, 2011.
13. James C. Bezdek, Robert Ehrlich, William Full, "FCM: The Fuzzy c-means clustering algorithm", Computers and Geosciences, vol.10, pp.191-203, 1984.

14. Ajith Abraham, Swagatam Das, and Sandip Roy ,"Swarm Intelligence Algorithms for Data Clustering", pp.279-312.
15. Rafael C. Gonzalez, Richard E. Woods, "Digital Image Processing", Book, 2009.
16. Sevinc Bayram, Taha Sencar, and Nasir Memon, "An efficient and robust method for detecting copy-move forgery," in Proceedings of ICASSP 2009, 2009.
17. Hwei-Jen Lin, Chun-Wei Wang, Yang-Ta Kao, "Fast Copy-Move Forgery Detection", in WSEAS Transaction on Signal Processing, Vol 5(5), pp. 188-197, May 2009.
18. M. Barni, A.Costanzo , "A fuzzy approach to deal with uncertainty in image forensics", Signal Processing: Image Communication 27, pp.998–1010, 2012.
19. Deguang Wang, Baochang Han, Ming Huang,"Application of Fuzzy C-Means Clustering Algorithm Based on Particle Swarm Optimization in Computer Forensics", International Conference on Applied Physics and Industrial Engineering, pp.1186 – 1191, 2012.
20. Gonzalo Vaca-castano, "Satlab tutorial session-2", http://www.aishack.in/2010/05/sift-scale-invariant-feature- transform", 2010.
21. Hany Farid, "Image forgery detection A survey", ieee signal processing magazine, pp. 16-25, 2009.