International Journal of Advance Research in Science and Engineering
Vol. No.4, Special Issue (01), September 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

# AN ENHANCEMENT OF COPY MOVE FORGERY DETECTION IN DIGITAL IMAGES USING HYBRID TECHNIQUE

**Naincy[1], Ashok Kumar Bathla[2]**

*[1]Research Scholar and [2]Assistant Professor*

*[1,2]Computer Engineering Department, YCOE, Punjabi University, Patiala, (India)*

## ABSTRACT

*Due to the technology advancement and availability of lots of sophisticated image editing tools, the digital images are losing authenticity. This has led to the proposal of different detection techniques to check whether the digital images are authentic or forged. Copy move forgery is a special type of forgery technique whose detection has become a widely used research topic under digital image forensics. In this paper an enhancement of copy move image forgery detection is done by implementing a hybrid of block based method DCT (Discrete Cosine Transform) and key-point based method SIFT (Scale-Invariant Feature Transform). The technique works by first applying DCT on an image and then SIFT on an resultant image obtained after applying DCT. Thus the features obtained using the hybrid technique DCT plus SIFT are found more robust against various types of attacks and show improvement in detection results also. The technique has shown quite significant results on multiple cloning, various attacks like against scaling, rotation, rotation plus scaling combined attack, noise, compression, blur and on real time images also.*

***Keywords: Forgery, Copy Move, Block Based, Key-Point Based, Discrete Wavelet Transform, Scale Invariant Features Transform.***

## I. INTRODUCTION

Now-a-days, digital images have acquired the reputation of being an important evidence. However, with the development of imaging technology and the accessibility of powerful affordable image editing tools like Photoshop, it is becoming easier to add, modify or remove important features from an image without leaving any visual traces. Any image manipulation can become a forgery, based upon the context in which it is used. Thus today digital images are losing authenticity and it is becoming difficult to distinguish between authentic and tampered images; which is an essential requirement in various areas like in legal cases, in electronic media, in medical profession, and in research works etc. Copy move is the most common technique used for creating digital image forgeries in which a part of an image is copied and pasted elsewhere in the same image. There have already been some efforts to address the problem of authenticating digital images and many copy move image forgery detection techniques have been proposed to do so but the work is still in its infancy stage.

### 1.1 Copy Move Image Forgery

Copy move image forgery is the most commonly used manipulations in which, part of image is copied and pasted to different locations in same image to either add or hide objects. Fig. 1 shows an example of copy move image forgery in which forged image is made by hiding persons shown in original image by pasting some other regions on them. It is also possible to do some post processing operations like scaling, rotation, noise addition, compression etc. on the copied part before pasting it to some other location to make its detection more difficult. As the copied region came from same image, thus no change occur in its properties like noise, texture, color etc. and hence makes the detection process difficult for humans [1]. The main focus of paper is on detection of this particular type of forgery.

The remaining contents of the paper are presented in following manner. Next section deals with types of copy move image forgery detection methods. Section 3 represents previous work related of copy move image forgery detection. Section 4 completely explains the methodology used for implementation of technique, section 5 deals with results and evaluation of performance parameter. In the end we have conclusion, future scope and references.

**a) Original image** **b) Forged image**

**Figure1:- An example of copy move image forgery [2]**

## II. COPY-MOVE IMAGE FORGERY DETECTION

Copy-Move forgery detection techniques can be broadly classified into two categories that are block based and key-point based methods as shown in Fig. 2. A brief discussion about these detection techniques is given as follows:

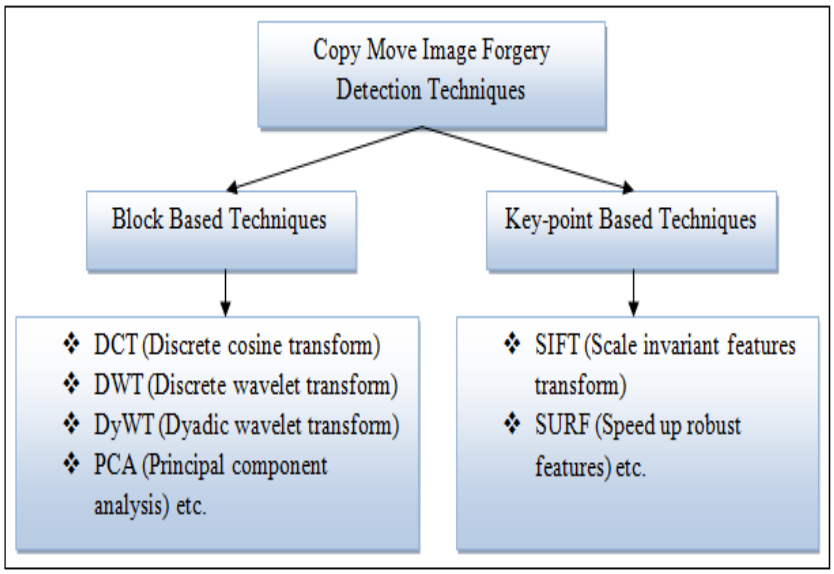


**Figure 2:- Copy move image forgery detection methods**

### 2.1 Block Based Methods

Block based methods come into existence due to various drawbacks of exhaustive search method like its high computational time. Block based method work by dividing the image into small overlapping or non-overlapping blocks by sliding a window of particular size over the image. Then the features for each block are calculated and their feature vectors are compared with each other which help in matching similar blocks. Thus it leads to detection of forged region. Block based methods are robust against various intermediate or post processing operations like compression, blurring, noise addition etc. But they are not efficient to detect forgery in regions having operations like scaling or rotations done over them. Some of commonly used block based methods are DCT, PCA, DWT, DyWT etc. [3][4].

### 2.2 Key-Point Based Methods

Key-point based forgery detection methods are proved great beneficial in dealing with the shortcomings of block based methods. These methods are proven robust against scaling and rotations attack. The key-point based methods start work by scanning the image. Then key-points are extracted from whole image and feature vectors are computed for these key-points. These feature vectors are placed in feature matrix where they are sorted lexicographically. Thus the similar feature vectors come closer and are suspected to be forged. Thus by following some threshold criteria forged regions are detected [5][6]. Major drawback that remains is the inability of key-point based methods in dealing with flat duplicate region detection [4]. Commonly used key-point based methods includes SIFT and SURF.

## III. RELATED WORK

**Fridrich et al. (2003) [7]** proposed the use of discrete cosine transform coefficients (DCT) as features and used block matching procedure for detection of copy move image forgery. The method is found robust against retouching and enhancement etc. **Pan et al. (2010) [2]** described a new region duplication detection method

based on SIFT that is found robust to distortions of the duplicated regions. The paper also highlights the drawbacks of SIFT, that this method is not suitable for detecting forgery in small region and can give false matching incase of intrinsically identical areas. **Amerini et al. (2010) [8]** proposed a technique to detect copy move image forgery in images using SIFT. The author has used agglomerative Hierarchical clustering to remove various false matches and Random Sample Consensus algorithm (RANSAC) to find geometric transformations that are used to create forgery. The method is also found robust on images having scaling or rotation attacks. **Kaur et al. (2013) [9]** gave an idea to combine block based method and key-point method and make a hybrid approach that is capable of detecting forgery in case of various editing operations. **Hashmi et al. (2014) [10]** proposed a method to deal with copy move image forgery by combining Dyadic Wavelet Transform (DyWT) and Scale Invariant Feature Transform (SIFT) to obtained more number of matching key-points and increase the detection efficiency. The method is found robust against various pre-processing attacks like scaling, rotation and noise addition also.

## IV. METHODOLOGY

In this dissertation work, a hybrid technique DCT (Discrete Cosine Transform) plus SIFT (Scale Invariant Features Transform) based on block based and key-point based methods for detection of copy move image forgery has been implemented. The algorithms to detect copy move image forgery using the above said technique as referred in figure 4.1 is briefly described as follows:

**Step 1: Take an image and apply Discrete Cosine Transform (DCT) on it**

First of all DCT (Discrete Cosine Transform) which is commonly known Block based method is applied on the test image. The purpose of applying DCT is to make it robust against various types of post processing operations like noise addition, blur addition and compression etc. on copied part due to its strong energy compaction property of DCT.

**Step 2: Key-point detection and feature extraction using SIFT**

Now we apply Scale Invariant Features Transform (SIFT) on resultant image obtained after applying Discrete Cosine Transform (DCT) to extract key-points from image. Along with each key-point, descriptor vector associated with it are also extracted.

**Step 3: Key-point matching using g2NN (generalized 2 nearest neighbor)**

Now the key-points obtained are compared with each other with the help of their corresponding descriptors. For matching an approach called generalization of 2 nearest neighbor (2NN) that is generalized 2 nearest neighbor (g2NN) is used. Now according to 2NN, in high dimension feature space we compute the ratio between the Euclidean distance of the closest neighbor to that of the second-closest one. The ratio is then compared with a threshold value fixed to 0.6. For a given key-point let $D=\{d_1,d_2\ldots..d_{n-1}\}$ denotes the similarity vector which is basically the sorted Euclidean distances with respect to the other descriptors. Now if $d_1$ denotes the distance of closest neighbor and $d_2$ denotes the distance of second closest neighbor from some key-point. Then $d_1/d_2$ is compared with the fixed threshold value. The $d_1/d_2$ should be low in case of matching of similar key-points. Whereas it should be greater than threshold in case of random features. The generalization of 2NN means to continuously repeat the 2NN test until ratio of nearest neighbor and second nearest neighbor is greater than 0.5.

Thus it is able to detect multiple cloning also due to its repetition over 2NN test. If k is the value where we stop, then each key-point having Euclidean distance from $\{d_1, d_2 \ldots d_k\}$, where k lies between 1to n, is considered as a match for targeted key-point.

Now for further processing only matched key-points are taken and isolated ones are ignored. Now it may be possible that an image contain intrinsically identical areas. Due to which we can obtained various false matches. As this is the major issue that effect the detection results. Thus a methodology is used to reduce false matches and is explained as follows.

**Step 4: Apply hierarchical agglomerative clustering (HAC)**

Here we used the concept of hierarchical agglomerative clustering upon matched points to reduce false matching rate. The final merging situation in clustering is achieved with the help of threshold and some linkage method. The linkage method used here is known as ward linkage. Ward's linkage computes the increment or decrement in the error sum of squares (ESS) after merging the two clusters into a single cluster with respect to two individual clusters. In addition to this the value of threshold used to stop clustering procedure also plays an important role. It is basically based on inconsistency coefficient (IC). As the value of IC goes on increasing, the similarity among the objects connected by link goes on decreasing. Thus when the value of IC exceeds the threshold, the clustering is stopped. IC does not allow to join spatially far clusters as it takes into account an average distance among cluster. Now at the end of clustering procedure, that clusters are removed which does not contain more than 3 matched key-points.

An image is suspected to altered by copy-move attack if procedure obtained two or more clusters with at least three pair of matched points. This method adopted helps in reducing false matching rate to large extent. But still it contain false matches, thus the clusters are processed further as explained below.

**Step 6: Apply Random Sample Consensus algorithm (RANSAC) algorithm**

The matching points obtained after clustering still contain several mismatched points called outliers. Thus RANSAC (Random Sample Consensus algorithm) algorithm is used to remove these outliers. RANSAC (Random Sample Consensus) is applied to select a set of inliers that are compatible with a homography transform between the two clusters. RANSAC algorithm randomly selects set of 3 key-points from matched points of clusters and transform other matched key-points accordingly and compared there distance with respect to their corresponding matched ones. The points are said to be inliers if the distance is under certain threshold β otherwise they are marked as outliers. After fixed number of iterations, that set with higher number of inliers is chosen. Here test is repeated 1000 times with β equals to 0.05. If fewer than 3 points remain after discarding outliers, then the match is rejected.

**Step 7: Copy Move Image Forgery Detection**

Now an image is considered to forged by copy move attack if procedure obtained two or more clusters with at least three pair of matched points that links cluster with one another.

## V. RESULTS AND DISCUSSION

The research work is implemented using MATLAB R2013a programming tools on a PC with Windows 7 and the following features:

- ✓ Processor: Intel(R) Core(TM) 2 Duo CPU T6600 @ 2.20 GHz 2.20 GHz
- ✓ Installed Memory (RAM): 3.00 GB
- ✓ System Type: 64-bit operating system

### 5.1 Results and Discussion of Hybrid Technique DCT plus SIFT

First of all the implemented hybrid technique DCT plus SIFT is tested on a standard dataset known as MICC-F220 [10]. Along with some original images and planer forged images, the dataset also contain images having scaling, rotation and combined scaling and rotation attacks done on them. In the Fig. 3, first column represents original image, second column represents tampered image (having attack scaling, rotation and combined scaling plus rotation attack done on first, second and third image respectively) and third column represents the detection results using hybrid of DCT and SIFT. Results show that hybrid implemented is able to detect forgery efficiently, even if the copied part has done various above discussed attacks on it.

**Figure 3:- Results of Hybrid DCT plus SIFT on Some Forged Images of Dataset MICC-F220.**

In addition to this, the effectiveness of the method has been tested against noise, blur, compression and multiple cloning by creating forged images with such attacks. For this, the forged images are created by copy-move operation on any of the authentic image from the dataset MICC-F220. The copied region is post-operated by Gaussian noise, blur or compression. For multiple cloning, the copied part is copied multiple times. Along with these, some real time images are taken and forged for checking the robustness of this research work on these also. So an additional dataset of 25 images is created, containing 5 images each for checking robustness against noise, blur, compression, multiple cloning and real time data as illustrated in table 1 also.

**Table 1:- Tests performed on additional dataset**

| Sr. no. | Operation | Value |
|---|---|---|
| 1. | Noise addition | Zero mean and 0.02 variance |
| 2. | Blur addition | Standard deviation 1.0 |
| 3. | Compression | Bit per-pixel (BPP) ratio 0.8 |
| 4. | Multiple cloning | ---- |
| 5. | Real time images | Camera resolution 12.3 Megapixels |

**Figure 4:- Results of hybrid DCT plus SIFT on some forged images of additional dataset**

In the Fig. 4, first column represents original image, second column represents tampered image (having operation of noise addition, blur addition, compression, multiple cloning and real time images shown on first, second, third, fourth and fifth image respectively) and third column represents the detection results using hybrid of DCT and SIFT. Results show that hybrid implemented is able to detect forgery efficiently on all above discussed operations also.

### 5.2 Evaluation of Performance Parameters and Comparative Analysis

In this subsection, the hybrid of DCT and SIFT presented in the dissertation work has been compared with an existing hybrid technique DyWT plus SIFT [10] using standard dataset MICC-F220. The performance of both the hybrid techniques is evaluated on the basis of parameters like: precision, recall, False Positive Rate (FPR) and accuracy. Table 2 represents values of terminology used to calculate evaluation parameters and table 3 represents the comparative analysis of both the above said techniques.

**Table 2: Values of Terminology Used to Calculate Evaluation Parameters**

| TP | TN | FP | FN |
|---|---|---|---|
| 87 | 103 | 7 | 23 |

From the above mentioned measures we calculated accuracy, precision, TPR (True positive rate) and FPR (False positive rate) which are defined as:

- ✓ **Accuracy** = $\frac{TP+TN}{TP+TN+FP+FN}$
- ✓ **Precision** = $\frac{TP}{TP+FP}$
- ✓ **TPR or Recall** = $\frac{TP}{TP+FN}$
- ✓ **FPR** = $\frac{FP}{TN+FP}$

**Table 3:- Comparative Analysis of Hybrid DCT Plus SIFT with Existing Technique**

| Method | Precision (%) | Recall (%) | FPR (%) | Accuracy (%) |
|---|---|---|---|---|
| Hashmi et al.[10] | 88 | 80 | 10 | 85 |
| DCT plus SIFT | 92.55 | 79.09 | 6.36 | 86.36 |

So, from table 3, it can be concluded that the hybrid of DCT and SIFT succeeded in achieving high values of precision and accuracy. Moreover, the False Positive Rate (FPR) was also improved significantly using this hybrid of DCT and SIFT as compared to the existing technique [10]. The hybrid of DCT and SIFT is also able to manage satisfactory value of recall also.

Graphical representation of above shown comparison between hybrid of DCT and SIFT with existing technique DyWT plus SIFT [10] has been presented in Fig. 5.

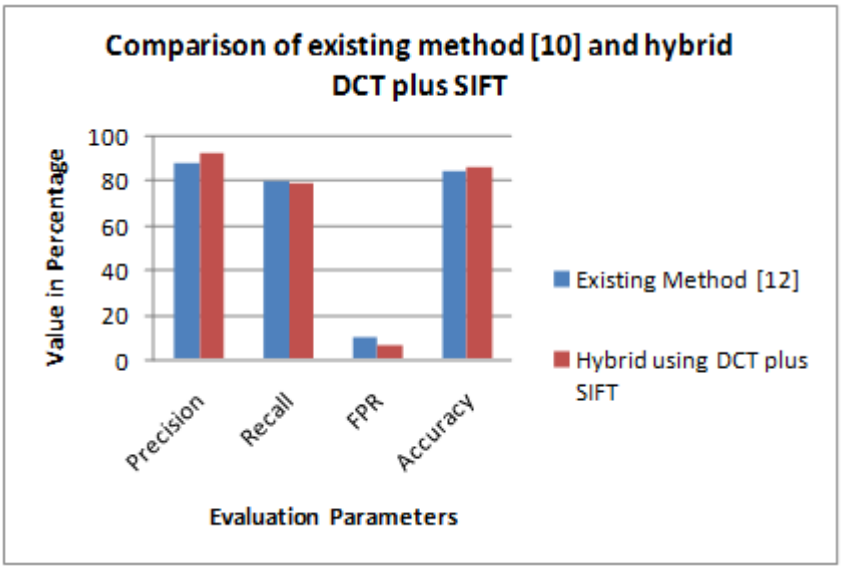


**Figure 5:- Graphical Representation of Performance Measures**

## VI. CONCLUSION AND FUTURE WORK

It is confirmed from literature that none of the existing technique is good enough to detect copy move image forgery and still the large number of issues are present in this field. Thus in this dissertation work a hybrid of DCT and SIFT for copy move image forgery detection is implemented with an aim of resolving some of the issues and detect copy move image forgery with good results. The technique implemented has shown its robustness against various types of attacks like noise addition, blur addition, compression, scaling, rotation, compression and combination of rotation plus scaling. The technique has shown quite good results on multiple cloning and on real time images also. The technique DCT plus SIFT has shown remarkable improvement in precision, FPR and

accuracy as compared to existing technique DyWT plus SIFT [10]. The technique has shown satisfactory results of recall also.

As the technique implemented is basically developed for detection of copy move image forgeries in digital images only. Thus, the work can be extended to detect copy move forgeries in videos also. Secondly, work can be extended to detect copy move image forgeries in flat and small regions also.

## REFERENCES

[1] Qureshi M. A., Deriche M., "A Review on Copy Move Image Forgery Detection Techniques", IEEE 11th International Multi Conference on System, Signal and Devices, Barcelona, pp. 1-5, 2014.

[2] Pan X., Lyu S., "Region Duplication Detection using Image Feature Matching", IEEE Transactions on Information Forensics and Security, vol. 5, no. 4, pp. 857-867, 2010.

[3] Hashmi M. F., Hambarde A. R., Keskar A. G., "Copy Move Forgery Detection using DWT and SIFT Features", IEEE 13th International Conference on Intelligent Systems Design and Applications (ISDA), Bangi, pp. 188 – 193, 2013.

[4] Saleem M., Altaf M. Q., Chaudry Q., "A Comparative Analysis on Pixel based Blind Cloning Techniques", IEEE International Conference on Control System, Computing and Engineering, Penang , pp. 130-135, 2014.

[5] Amerini I., Ballan L., Caldelli R., Bimbo A. D., Serra G., "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.

[6] Lowe, David G., "Distinctive Image Features from Scale-Invariant Key Points", International Journal of Computer Vision, vol. 60, no. 2, pp. 91-110, 2004.

[7] Fridrich J., Soukal D., Lukas J., "Detection of copy-move forgery in digital images", Proceedings of Digital Forensic Research Workshop, Citeseer, 2003.

[8] Amerini I., Ballan L., Caldelli R., Bimbo A. D, Serra G., "Geometric Tampering Estimation by Means of a Sift-Based Forensic Analysis", IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP), Dallas, pp. 1702- 1705, 2010.

[9] Kaur A., Sharma R., "Optimization of Copy-Move Forgery Detection Technique", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 4, pp. 576-578, 2013.

[10] Hashmi M. F., Anand V., Keskar A. G., "Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform", ELSEVIER, AASRI Conference on Circuit and Signal Processing, pp. 84-91, 2014.