Volume 5 Issue I, January 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

# Improving Copy-Move Forgery Detection Time by Using DCT, Correlation and SOBEL Edge Detector

Harpreet Kaur[1], Sheenam Malhotra[2]
[1]M. Tech Student, [2]Assistant Professor
Department of Computer Science and Engineering, Sri Guru Granth Sahib World University Fatehgarh Sahib – India, 140406

***Abstract – Copy move image forgery is often used in which region of an image is copied and pasted at another location to hide an important scene, clone or duplicate the number of aspects in the same image. Block representing have been suggested to detect copy-move forgery but one of the major issues of this method is detection time. Image authentication technique is proposed which is based on DCT and Sobel operator to detect copy-move forgery with less detection time. Discrete cosine transform is used to compress an image and introduce blocking artifacts at the block boundaries which helps to detect forgery. The Compressed image is divided into 8*8 overlapping blocks and correlation is computed between blocks to extract the forged region. Edges of forged region are detected by Sobel edge detection. Proposed method improves the detection time, precision, recall, and accuracy. It is robust to rotation, scaling, blurring, noise, brightness, and multiple copy-move forged regions.Keywords – Image forgery, Copy-move, DCT, Compression, Blocking Artifact, Correlation, Edge Detection.***

## I. INTRODUCTION

Digital images are principal means of information exchange. Nowadays, images are used to strengthen the news in the newspapers, evidence in the court, legal documents and mostly in social networking sites etc [9]. But with the advancement and free availability of strong editing tools such as Adobe Photoshop, Corel draw, Gimp, and Paint.Net etc., tampered images are easily created due to which truthfulness of images are at big risk. Image forgery detection becomes an emerging and important research area. Image forensics techniques mainly divided into two parts. One is active and other is passive. The active approach requires watermark and a digital signature is embedded inside the image. Passive or blind forgery detection forensic technique detects the traces of tampering without any prior embedded watermark or digital signature [2]. Passive Approaches can be divided into five categories such as Pixel Based, format Based, camera Based, Physical Based, Geometry Based image forgery detection. Pixel based techniques are categorized as Copy-Move, Splicing, Re-sampling, Retouching [1]. In Copy move forgery, a region from an image is copied and pasted in the same image at another location to hide any important scene, duplicate the number of the objects to represent miss-information [3].

## II. RELATED WORK

Fattah, et al. [4] presented 2D-DWT method in which block matching is performed when all overlapping blocks are compared with selected candidate non-overlapping blocks to detect the forged region. Kumar, et al. [5] presented the fast DCT based copy-move forgery detection method which represents the features of overlapping blocks and matching is performed to detect the forgery by reducing the execution time of the algorithm. Cao, et al. [6] presented locality preserving projections method to detect the forgery from the images. LPP is used to reduce the size of a block and its dimensions. Hsu et al. [7] presented efficient histogram of orientated Gabor magnitude to extract features and identify forgery from the images having translation, rotation, JPEG compression, blurring, and brightness adjustment. Ustubioglu, et al. [8] presented the method in which the image is divided into overlapping blocks and LBP value is obtained from each block after that DCT is applied. LBP- DCT method lowers false negative values. Kumar, et al. [9] presented the novel method to detect the forgery on the basis of DCT coefficients. This method is efficient in the presence of contrast change. Huang [10] presented DCT to represent features and sorting is performed to detect the forgery in an image. Mahdian and Saic [11] presented method for detection of duplicate regions from images having noise and blurring but a major issue is execution time. Bacchuwar, et al. [12] presented jump patch block match algorithm for detection of copy-paste forgery but it takes a lot of detection time in minutes. Maind, et al. [13] presented DCT based method in which original and forged image is divided into overlapping blocks and features are extracted, sorted and matching is performed to detect duplicate regions but main drawback is high detection time, not robust to geometric transformations like scaling and accuracy of this method is less in case of blurring and noise.

Volume 5 Issue I, January 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

## III. PROPOSED METHODOLOGY

In Proposed methodology, copy-move forgery is detected by using discrete cosine transform. DCT is applied to an image for dimensionality reduction or compression. DCT is used due to its ability to represent most of the image details with fewer coefficients. DCT based image compression is also known JPEG compression which produces blocking artifact at the border of 8*8 blocks in the form of horizontal and vertical edges. These artifacts may be disturbed whenever forgery is performed in the image. Proposed method improves the performance by reducing the detection time and robust to many post-processing operations. Flowchart of copy-move forgery detection which describes the whole process of detection of duplicate regions from the forged image is shown in below Fig 1.

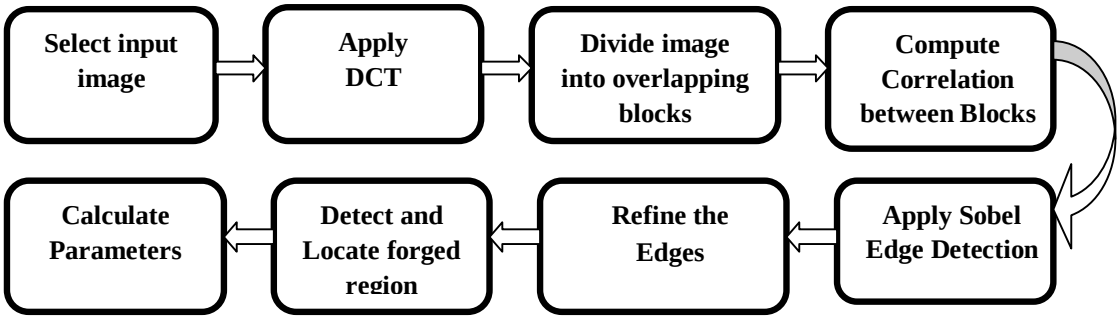



Fig. 1: Flow chart of proposed methodology

## IV. PROPOSED ALGORITHM

*A.* Start

*B.* Select forged image as input.

*C.* Apply image compression using DCT on the image. DCT will compress all rows and columns of image due to which blocking artifact is introduced in compressed image. DCT equation is given below:

$$y(k) = w(k) \sum_{n=1}^{N} x(n) \cos\left[\frac{\pi(2n-1)k-1}{2N}\right] \quad k = 1,2,\dots N \qquad Eq.(1)$$

Where $w(k) = \begin{Bmatrix} \sqrt{\frac{1}{N}} & if\ k = 1 \\ \sqrt{\frac{2}{N}} & 2 \le k \le N \end{Bmatrix}$, x, y is matrix of row or column, N is size of matrix.

After compression, images are reconstructed from its cosine transform using Inverse-DCT equation:

$$x(n) = \sum_{n=1}^{N} w(k)\, y(k) \cos\left[\frac{\pi(2n-1)k-1}{2N}\right] \quad n = 1,2,\dots N \qquad Eq.(2)$$

*D.* Divide compressed image into fixed size overlapping blocks of B*B pixels using equation:

$$N_{overlap} = (M - B + 1) * (N - B + 1) \qquad Eq.(3)$$

Where M*N is the size of image and B = 8.

*E.* Similarly, original image is selected and image compression using DCT will be applied to an image and divided it into overlapping blocks.

*F.* Compare the blocks of both original and forged image by computing the correlation coefficients between these blocks and blocking artifact region is detected. Correlation is calculated using below equation.

$$\frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{(\sum_m \sum_n (A_{mn} - \bar{A})^2)(\sum_m \sum_n (B_{mn} - \bar{B})^2)}} \qquad Eq.(4)$$

Where $\bar{A}$ & $\bar{B}$ are means of sets A & B, M*N is a size of A & B, m=1, 2, 3...M and n=1, 2, 3...N.

*G.* Convert image into black and white and use Sobel edge detector to detect or extract the edges of image by using below equation.

Volume 5 Issue I, January 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

$$G = \sqrt{G_x^2 + G_y^2} \ , \ G_x = \begin{bmatrix} -1 & 0 & +1 \\ -2 & 0 & +2 \\ -1 & 0 & +1 \end{bmatrix} and \ G_y = \begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ +1 & +2 & +1 \end{bmatrix} \quad Eq.(5)$$

Where G is gradient Magnitude, $G_x$ and $G_y$ are two images which at each point contain the horizontal and vertical derivative.

*H.* Refine the edges of detected region and remove the small connected components or objects that have fewer pixels from binary image using Morphological operations.

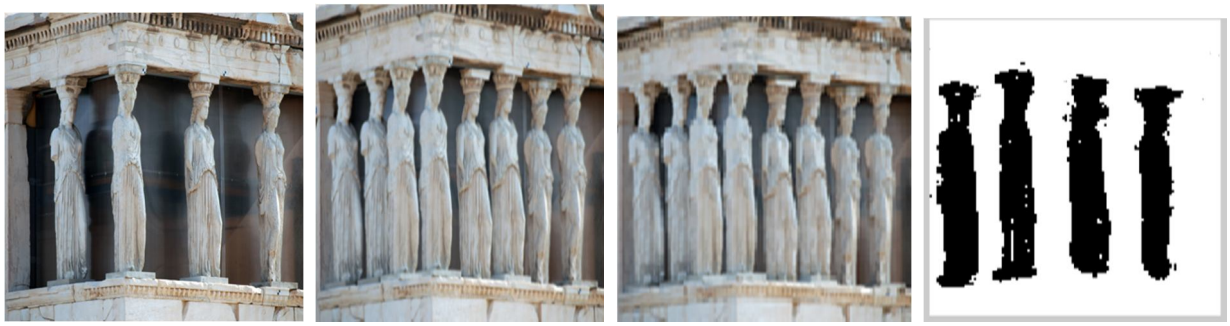
*I.* Locate the copy-move tampered area and highlight the detected region or pixels with yellow color.

*J.* Calculate the parameters such as detection time, precision, recall and accuracy.

*K.* End.

## V. RESULT AND DISCUSSION

This proposed approach is performed on a personal computer with 2.40GHz CPU, 2GB memory and by using MATLAB 2010b software. To compare the proposed algorithm with existing method, a dataset of 200 images is prepared from available datasets [13] [14] [15] in which 100 are original and 100 are forged images. Copy move forgery detection results are shown in the Fig 2. Here Fig 2(a) is the original image, Fig 2(b) is the forged image in which multiple tampering is performed, Fig 2(c) is the compressed image after DCT compression by using Eq. (1) and inverse discrete cosine transform is applied using Eq. (2). Then image is divided into overlapping blocks and correlation is computed using Eq. (3) and Eq. (4) and Block Artifact Region Detected image is shown in Fig 2(d). Apply Sobel edge detector by using Eq. (5) as shown in Fig 2(e) and Fig 2(f) shows edge refinement image by using Morphological operations. After applying all the equations the detection result in the form of binary mask is shown in Fig 2(g). Visual representation of detected forged region has highlighted with yellow color shown in Fig 2(h).



(a) Original image (b) Forged image (c) Compressed image (d) Block Artifact detection

(e) Edge detection (f) Edge refinement (g) Binary Mask (h) Detection Result

Fig 2 Copy-move forgery detection Result of proposed method on images.

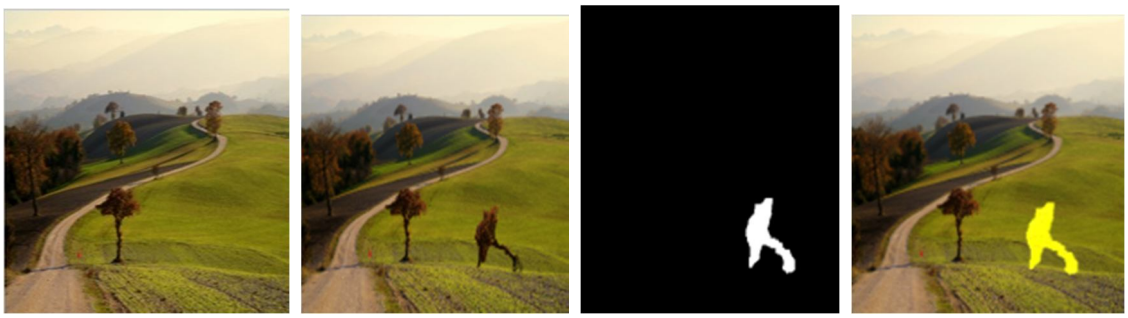
Some of the images used to evaluate the result of proposed method is shown below in which (a) is original, (b) is forged image, (c) & (d) are detection results. Fig 3.1 shows an example of copy-move forgery without any transformation (a) original image with one tower, (b) forged image with two towers in which right tower is duplicate of left one, (c) is binary mask & (d) is detection result.

Volume 5 Issue I, January 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

(a) (b) (c) (d)

Fig 3.1 Example of simple copy-move forgery (a) original image (b) forged image (c) binary mask & (d) detection result.

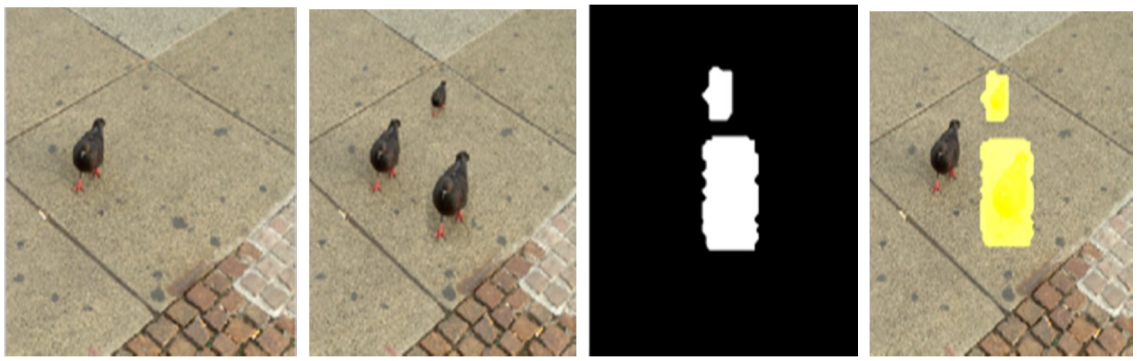
Below Fig 3.2 shows an example of tree image having copy-move forgery with geometric transformation such as rotation. Here (a) is original image, tree from original image is copied and pasted after rotation in the right of same image called forged or tampered image such as (b) , (c) binary detection mask in the form of black and white where white is forged region and (d) is detection result.



(a) (b) (c)

Fig 3.2 Copy-move with rotation (a) original image (b) forged image (c) binary mask & (d) detection Results.

Below Fig 3.3 shows image (b) having forged bird which is copied and pasted after Geometric transformation such as scaling and more than one time bird is pasted to represent the example of multiple forgery.



(a) (b) (c) (d)

Fig 3.3 Copy-move with Scaling (a) original image (b) forged image (c) binary mask & (d) detection Results.

Performance of proposed method is evaluated and comapred with block representing method by calculating the detection time, Precision, Recall, and Accuracy. Performance Parameters are shown below:

*A. Detection Time*

The detection time of Block Representing Method is compared with the proposed method and result shows that proposed method is computationally much faster than existing method. Detection time of proposed method is between 3 sec to 8 sec but block representing method requires detection time between 45 sec to 340 sec. Existing method is based on DCT feature extraction, sorting and matching which consume large time but proposed method is based on DCT compression, correlation, Edge detection due to which it require less time to detect the forgery. Comparison of detection time is shown below in Table 1.

Volume 5 Issue I, January 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

TABLE 1: DETECTION TIME OF PROPOSED AND EXISTING METHOD

| Images | Size of Image | Proposed method (in sec) | Block representing method (in sec) |
|---|---|---|---|
| Image 1 | 240*161 | 3.464 | 47.05 |
| Image 2 | 240*161 | 3.498 | 49.39 |
| Image 3 | 240*161 | 3.545 | 52.87 |
| Image 4 | 240*161 | 4.633 | 60.19 |
| Image 5 | 240*161 | 4.898 | 63.70 |
| Image 6 | 240*161 | 4.011 | 60.69 |
| Image 7 | 240*161 | 3.132 | 97.86 |
| Image 8 | 235*235 | 5.577 | 148.93 |
| Image 9 | 235*235 | 5.992 | 212.80 |
| Image 10 | 235*235 | 5.972 | 243.71 |
| Image 11 | 235*235 | 5.218 | 279.39 |
| Image 12 | 335*335 | 6.991 | 305.04 |
| Image 13 | 335*335 | 6.899 | 338.95 |
| Image 14 | 335*335 | 7.021 | 322.68 |
| Image 15 | 335*335 | 7.243 | 339.71 |

Graph representation of Detection time between two methods is shown below in Fig 4. Experiment results show that detection time of proposed method is very less as compared to block representing method.

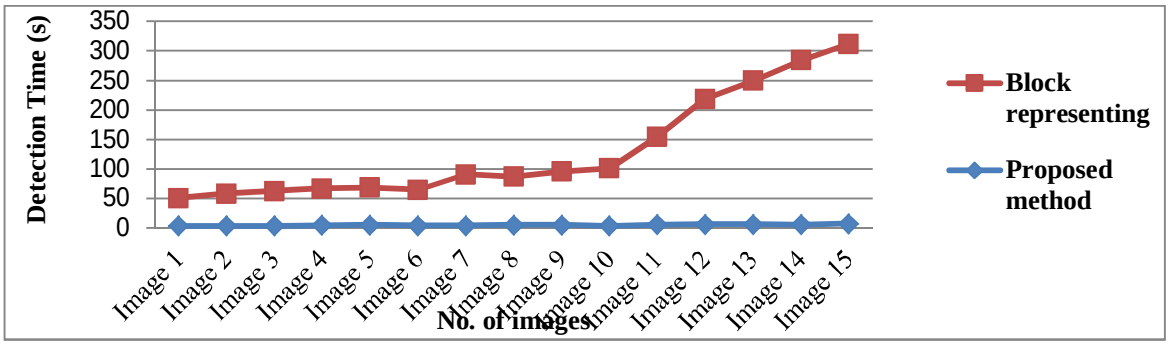



Fig 4: Detection Time between two methods.

For evaluation of the results, comparison between proposed and existing method on the basis of performance parameters shown below in Table 2. TP (True Positive) is number of forged images that have been correctly detected as forged. FP (False Positive) is number of forged images that have been falsely detected as forged. FN (False Negative) is number of images that have been falsely missed but they are forged. TN (True Negative) is number of original images correctly detected that have been correctly detected as not-forged.

TABLE 2: COMPARISON OF PERFORMANCE MEASURES BETWEEN TWO METHODS.

| METHODS | TP | FP | TN | FN |
|---|---|---|---|---|
| Block Representing | 75 | 25 | 98 | 2 |
| Proposed Method | 95 | 4 | 100 | 1 |

*B. Precision Rate*

A precision rate is the ratio of no. of correctly detected images to the sum of correctly detected images plus false positive. It is also

Volume 5 Issue I, January 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

called positive predictive rate. If value of precision is high it indicates less false positive. Mathematically,

$$Precision\ Rate\ = \frac{TP}{TP+FP} \times 100 \quad \text{Eq. (6)}$$

*C. Recall Rate*

A recall rate is the ratio of correctly detected images to the sum of correctly detected images plus false negative. If value of recall is high it indicates less false negative. The recall is also called as true positive rate or sensitivity. Mathematically,

$$Recall\ Rate\ = \frac{TP}{TP+FN} \times 100 \quad \text{Eq. (7)}$$

*D. Accuracy*

Accuracy is used to calculate the proportion of true positive and true negative in all evaluated cases. Accuracy of proposed method is much better than existing block representing method. Accuracy is calculated by using below formula:

$$Accuracy\ = \frac{TP+TN}{TP+TN+FP+FN} \quad \text{Eq. (8)}$$

Comparison of precision, recall and accuracy is shown below in Table 3. Results show that proposed method outperforms the exiting method and detect forgery with high accuracy.

TABLE 3: COMPARISON OF PRECISION, RECALL AND ACCURACY BETWEEN TWO METHODS.

| Parameters | Block Representing method | Proposed Method |
|---|---|---|
| Precision | 74.25% | 95.95% |
| Recall | 91.46% | 98.95% |
| Accuracy | 86.00% | 97.50% |

Graph representation of comparison between precision, recall and accuracy of proposed method and existing method is shown below in Fig 5.

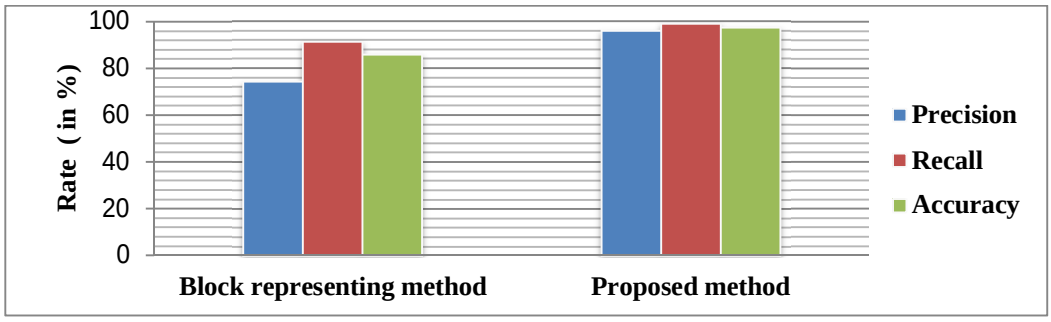



Fig 5: Precision, recall and accuracy results comparison between two methods.

## VI. CONCLUSION AND FUTURE SCOPE

The Proposed copy moves forgery detection method is based on DCT for dimensionality reduction or compression, a correlation for similarity measure and extracting a tampered region. Sobel edge detection is used to detect the edges of forged region. The main advantage of proposed method is its lower computational time and robust to various attacks such as rotation, scaling, brightness, blur, noise. It quickly and accurately detects the location of single or multiple, small or large forged regions of regular or irregular shapes. Compared with a block representing a method, the detection time of proposed method is very less. Precision, recall, and accuracy is also higher than existing block representing method. Robustness against post-processing operations such as flipping and more than one type of forgery is detected with a single method may be studied further in future.

## REFERENCES

[1] G. K. Birajdar, V. H. Mankar, "Digital Image Forgery Detection Using Passive Techniques: A Survey," Digital Investigation, ELSEVIER, Vol. 10, Issue 3, pp: 1-20, May 2013.
[2] M. A. Qureshi, M. Deriche, "A bibliography of pixel-based blind image forgery detection techniques," Signal processing: Image communication, ELSEVIER, Vol. 39, pp: 46-74, Aug 2015.
[3] S. A. Fattah, M. I. Ullah, M. Ahmed, C. Shahnaz, "A Scheme for Copy Move Forgery in Digital Images based on 2D-DWT," IEEE, pp: 801-804, Oct 2014.
[4] S. Kumar, J. Desai, S. Mukherjee, "A fast DCT based method for copy move forgery detection," Second international conference on image processing, IEEE,

pp: 649-654, May 2013.
[5] G. Cao, Y. Chen, G. Zong, "Detection of Copy Move Forgery in Digital Image using Locality Preserving Projections," International Conference on Image and Signal Processing, IEEE, Oct 2015.
[6] C. Hsu, J. Lee, W. Chen, "An Efficient Detection algorithm for Copy-Move Forgery," 10th Asia Joint Conference on Information Security IEEE, pp: 33-36, May 2015.
[7] B. Ustubioglu, G. Ulutas, V, Nabiyev, "LBP-DCT Based Copy Move Forgery Detection Algorithm," Springer International Publishing, Information Sciences and Systems, pp: 127-136, Dec 2015.
[8] S. Kumar, J. Desai, S. Mukherjee, "Copy Move Forgery Detection in Contrast Variant Environment using Binary DCT Vectors," I.J. Image, Graphics and Signal Processing, pp: 38-44, May 2015.
[9] Y. Huang, W. Lu, W. Sun, D. Long, "Improved DCT-based detection of copy-move forgery in images," Forensic Science International, pp: 178–184, July 2013.
[10] K. S. Bacchuwar, Aakashdeep, K. R. Ramakrishnan "A Jump Patch-Block Match Algorithm for Multiple Forgery Detection," IEEE, pp: 723-728, March 2013.
[11] B. Mahdian , S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants," Forensic Science International 171, pp:180–189, Sep 2007.
[12] R. A. Maind, A. Khade, "Image copy move forgery detection using block representing method," International Journal of Soft Computing and Engineering," Vol. 4, Issue 2, pp: 49-53, May 2014.
[13] D. Tralic, I. Zupancic, S. Grgic, M. Grgic, "CoMoFoD - New Database for Copy-Move Forgery Detection," in Proc. 55th International Symposium ELMAR, ISSN 1334-2630, pp: 49-54, Sep 2013.
[14] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, G. Serra. "A SIFT-based forensic method for copy-move attack detection and transformation recovery," IEEE Transactions on Information Forensics and Security, Vol. 6, Issue 3, pp: 1099-1110, 2011.
[15] V. Christlein, C. Riess, J. Jordan, C. Riess, E. Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches," IEEE Transactions on Information Forensics and Security, Vol. 7, No. 6, pp: 1841-1854, Aug, 2012.