*Research Article*

# Enhanced K-means Clustering Technique based Copy-Move Image Forgery Detection

**Tawheed Jan Shah[1], M. Tariq Banday[2]**

[1,2]Department of Electronics and Instrumentation Technology, University of Kashmir,
Srinagar, India
tawheedjan@gmail.com; sgrmtb@gmail.com

**Corresponding Author:**
Tawheed Jan Shah, Srinagar, India
Department of Electronics and Instrumentation Technology, University of Kashmir,
tawheedjan@gmail.com

**Article History**: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 23 May 2021

**ABSTRACT:**
Currently, different methods such as copy-move, image morphing, image splicing, image retouching, etc. are used to alter digital images. Among them, copy-move image forgery is one of the most familiar cyber-crimes and is affecting the world of digital images as this type of forgery is easy to create and one of the hardest forgeries to detect. This paper focusses on the detection of blind copy-move image forgery, which is frequently put into practice in the field of passive forensics to confirm the genuineness and integrity of digital images. In the proposed work, discrete wavelet transform is first applied on the input image. The resulting lowest frequency approximate sub-band is partitioned into small overlapping blocks having fixed size with a sliding factor of one pixel. The 2D discrete cosine transform is then computed for each fixed size block and is then stored as a one-row vector by using the zigzag scanning. The use of the hybrid transform together with fast k-means clustering technique helps to increase the processing speed and reduces the overall forgery detection time. The performance of the propounded system is assessed by using Matlab (R2016a) and then compared to the others works and is found to be satisfactory in terms of precision, recall, F1 Score, and forgery detection time.

**Keywords:** Image Forgery; Block Based Methods; DWT; Copy-Move Forgery; Image Forgery Detection

## 1. INTRODUCTION

In the present Savvy world, most of the information is conveyed to the receiver either through digital images or videos. However, these sources of information are easily forged or manipulated not only by the professionals but also by the novice persons by using different sophisticated and inexpensive image editing tools viz; PicMonkey, DxO PhotoLab 4, ACDSee Photo Studio Ultimate, ON1 Photo RAW, Adobe Photoshop, Adobe Lightroom, Corel PaintShop Pro, Pixlr Editor, Inkscape, etc. Consequently, there is a ubiquitous lack of trustworthiness of digital image credibility, primarily when it is used as evidence in a courtroom, but more in general, in the media and information world. Hence, the need of image forgery detection (IFD) in order to confirm the originality and integrity of digital images has become a topic of grave concern and is thus enticing the attention of research scientists in computer vision, digital investigation, digital image processing, image forensics, biomedical technology, etc.

The IFD techniques are broadly categorized into Non-Blind [1] and Blind forgery detection techniques [2] as shown in Figure: 1. The Non-Blind techniques are additionally classified into Digital Watermarking and Digital Signature. The digital watermarking is further sub-divided into fragile, semi-fragile, and robust watermarking while digital Signature is sub-divided into generic signature, robust signature, and distributed source coding. These techniques have solved the image authenticity problem to a more considerable extent, but their main drawback is that they require additional pre-processing which in turn needs special equipment such as development software's, high-cost cameras, etc. Also, the subsequent processing of the original image degrades its visual quality which limits its implementation in practice. On the contrary side, blind forgery detection techniques have gained much importance because they do not require any previous information about the image content and uses only the characteristics of the suspicious image received from the sender for accessing its authenticity and integrity. Thus, Blind Copy-Move forgery detection (CMFD) approaches are commonly adopted for detecting digital image forgery. Blind Copy-Move forgery detection techniques are commonly categorized into five types based on Pixel, Camera, Physics, Format and Geometry [3]. The brief description of each of the above-mentioned image forgery detection techniques is given in Figure 1.

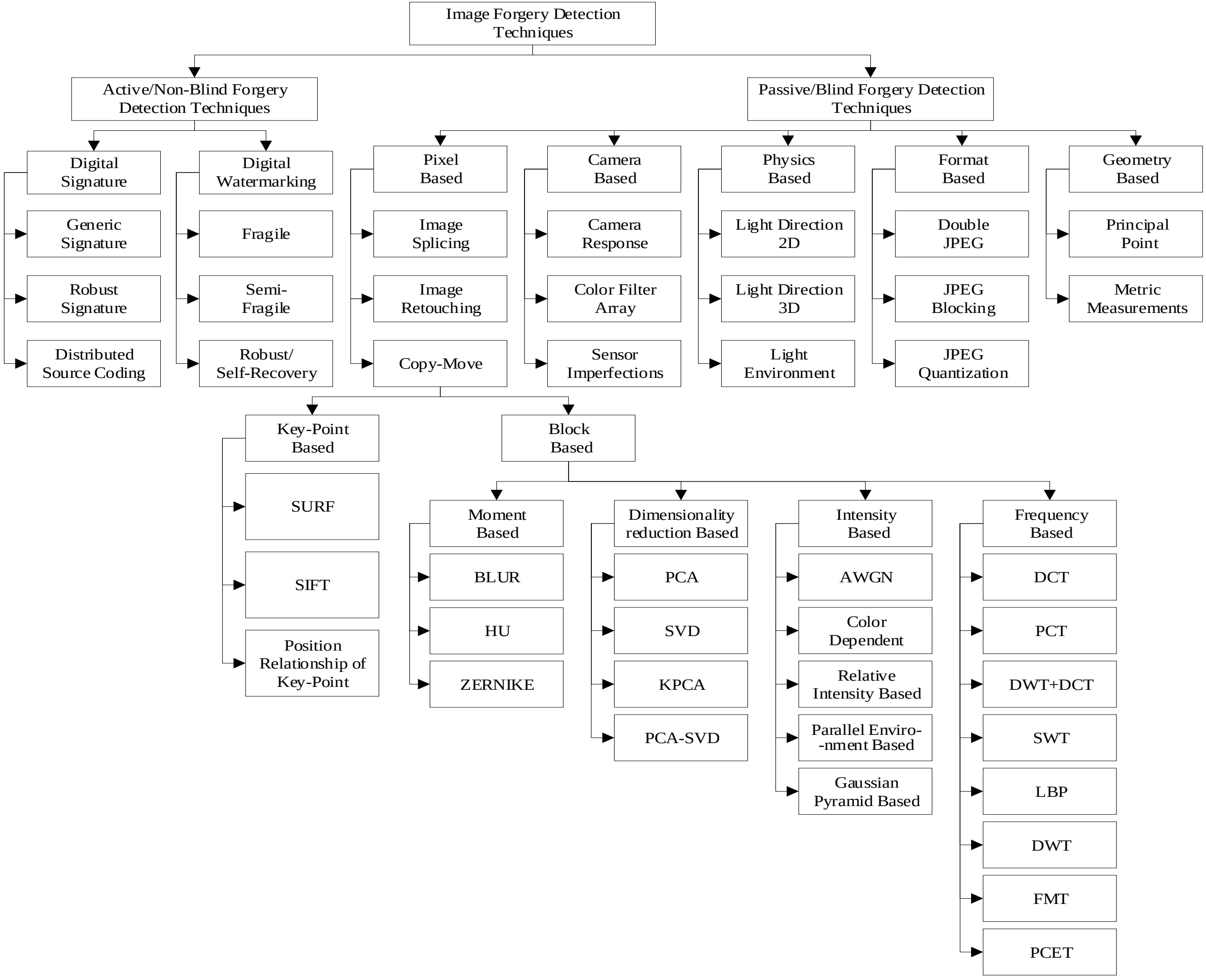

Figure 1. Classification of Image Forgery Detection Techniques

### 1.1. Geometry-Based Techniques

When the unforged image is manipulated by using different processes such as shifting of an object or region in the image, translation or combining the existing image with another image then the position of the principal point (i.e. the point where a principal plane intersects the axis) changes which otherwise, always lies close to the centre of the image. The geometric based techniques utilize different available image features such as dimension, position of objects related to the camera,etc. to detect the forgery.

### 1.2. Format-Based Techniques

This forgery detection technique is based on the image format and the most common image formats used today is the lossy JPEG compression. In JPEG compression, the image is first represented as a Discrete Cosine Transform (DCT) blocks. The resulting coefficients from DCT are then quantized in order to achieve compression. The DCT blocking and the quantization process introduces certain artifacts in the suspicious image, which are finally exploited to identify the forgery. Format based techniques are divided into three types viz; Double compression, JPEG Blocking, and JPEG Quantization as shown in Figure 1.

### 1.3. Physics-Based Techniques

Digital Images are usually captured in different conditions, i.e., different lighting or brightness, shadows, reflections etc. When such images are composited to acquire the manipulated image, it becomes tough for the forgers to match the brightness of the individual images. Such light variations, reflections etc within the images can be used for detecting the traces of forgery.

### 1.4. Camera-Based Techniques

Nowadays, most of the images are acquired by using different high resolution and low-cost digital cameras such as Canon, Nikon, Sony, Olympus, etc. rather than typical film cameras. Since these cameras are not perfect imaging systems because various artifacts are present regarding each step of the imaging process in them. The artifacts can be used to associate an image with a specific camera and hence makes the forgery detection possible.

### 1.5. Pixel-Based Techniques

These techniques identify the image forgery either directly or indirectly by accentuating on the pixel related characteristics or statistical changes of the suspected image. Pixel-based IFD techniques are broadly classified into Photomontage or Image Splicing, Image Retouching, and Image Cloning or Copy-move forgery. In image splicing, the regions from two or more unlike images are merged to generate a significantly different image from the original. Image splicing is further divided into two types: Boundary based and Region based [4]. Image retouching involves scaling, rotating, skewing, flipping or stretching the portions of the image in order to create a realistic match or high quality forged image. While retouching an image, specific periodic correlations are introduced in its samples. Those samples are then used to detect the digital image forgery. This type of forgery is less harmful as compared to the others. In the third type of forgery, copied region belongs to the same image. Among these three types of forgeries, copy-move forgery (CMF) is the most popular because it requires only one image. CMF and Image splicing are usually accompanied by different types of operations viz; JPEG compression, adding noise, and image blurring or geometrical operations viz; rotation, shifting and scaling, thereby, making the forgery detection difficult. The part of the image manipulated by CMF is almost imperceptible to the human visual system and thus, detecting evidence of such incident is a serious issue in image forensics. However, the computational complexity is the major issue in case of copy-move forgery detection based on exhaustive search methods.

CMFD techniques are generally classified into block-based [5] and Key-point based methods [6]. Key-point based methods are based on recognizing and selecting the high entropy image portions instead of sub-dividing the image into blocks as in case of block based methods. The features are then extracted for each key-point and later matched to identify the duplicated region. The popular key-point based methods encompasses Scale Invariant Feature Transform (SIFT) [6], Speeded-up Robust Features (SURF) [7] and Position Relationship of Key-points [8]. Key-point based methods cannot detect the CM forgery sufficiently, when the copy and pasted region is smooth area because key-point features cannot be extracted from them. Further, these methods are not robust to geometric transformation such as scaling, rotation etc. which restricts their use for detecting post-processed duplicated regions. On the other hand, Block-based methods detect the forgery more accurately. The general and straightforward process of Block based CMFD is shown in Figure: 2.

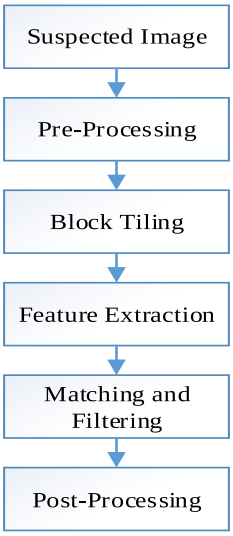

Figure 2. Primary Process of Block based CMFD [9]

In the first step, the pre-processing operations such as noise removal, color to grayscale conversion, cropping of the suspected image is done. In the second step, the pre-processed image is sub-divided into overlapping blocks of particular size, and a feature vector is extracted from each such block. The extracted features are subsequently matched in order to find the forged region and then filtering process is used to increase the probability of correct matches. The primary purpose of the filtering process is to classify the image into two categories, i.e., original and forged image. The final step is used to determine the correctness of the forgery detection system against different processes such as, image compression, scaling, rotation, etc. The block-based techniques are further segregated into four categories. They are frequency, dimensionality reduction, intensity, and moment-based CMFD techniques as shown in Figure 1. However, the key focus of this paper is to detect the frequency based copy-move forgery.

The remaining paper is structured as follows: Section II debates the related work concerning Block based copy-move image forgery detection. Section III presents the K-means Clustering. The propounded method for copy-move forgery detection is discussed in Section IV. Implementation details and investigational results are illustrated in section V, pursued by the conclusion and future scope.

## 2. RELATED WORK

Junliu Zhong and Yanfen Gan et al. [10] introduced an enhanced block-based CMFD method. The author used an auxiliary overlapped circular block in place of overlapped rectangular block to divide the suspicious input image. For each circular block, the extraction of the local and inner feature is achieved by using the Discrete Radial Harmonic Fourier Moments (DRHFMs). The matching feature vectors are searched by carrying out 2 Nearest Neighbors test and then, Euclidean distance and correlation coefficient is used to filter the similar feature vectors. Also, the morphologic operation is employed to remove isolated regions for auxiliary matting. As compared to the recent block and key-point based CMFD methods, the proposed method has less computational cost and more precise contour respectively.

Mohammed Hazim Alkawaz et al. [11] implemented the block-based CMFD method using DCT coefficients. In order to investigate the effects of distinct block size varying from 4 x 4 and 8 x 8 pixels on the presentation of the False Positive(FP) and False Negative(FN), threshold D_similar = 0.1 and distance threshold (N)_d = 100 are used to implement the ten input images. Accordingly, 8x8 overlapping blocks outperformed as compared to the 4x4 overlapping blocks with respect to accuracy. Additionally, the accuracy performance of different block sizes varies with the threshold value, size of the forged region and distance between the two forged regions.

Hajar Moradi-Gharghani and Mehdi Nasri [12] presented a novel method for CMFD. In this method, 2D DCT is utilized to extract feature vectors from non-overlapping blocks of the image, and then these feature vectors are sorted lexicographically. In the proposed work, the dispersion threshold is employed to remove large smooth portions of the image. The simulation results demonstrate that the propounded method find the regular, irregular and multiple forged regions with very small False-Positive in comparison with the classic methods in terms of false positive rate and detection accuracy rate.

Mohammad Farukh Hashmi et al. [13] suggested a unique CMFD technique which can withstand different attacks by using a combination of Dyadic Wavelet Transform (DyWT) and Scale Invariant Feature Transform(SIFT). The suspicious image is first decomposed into four sub-band images approximate (LL), horizontal (LH), vertical (HL) and diagonal details (HH). Then, SIFT is applied on the approximate (LL) sub-band image to extract the key-features and find a descriptor vector. The likeness between the feature descriptors is then obtained to determine whether the given image is fake or original. The proposed algorithm can extract a more significant number of key-points and is also robust to most of the attack and pre-processing techniques and hence detects the CMF efficiently.

Li. Yuenan [14] examined the CMFD algorithm based on polar cosine transform (PCT) and approximate nearest neighbor searching. The rotationally-invariant and orthogonal properties of the PCT are used to extract the robust and compact features from overlapping patches. The possible similar regions are detected by identifying the patches with similar features which is expressed as approximate nearest neighbor searching and solved by employing Locality-Sensitive Hashing (LSH). Also LSH based alikepatch detection approach is enough effective than the popular lexicographical sorting.The accuracy of the proposed scheme is further enhanced by developing a set of post-verification criteria in order to filter out the false matches. The experimental results revealed that the proposed method is robust to various post-processes such as scaling etc.

Khizar Hayat and Tanzeela Qazi [15] proposed CMFD technique based on the hybrid transform i.e. DCT and DWT. The suspicious input image is first divided into blocks using a discrete wavelet transform, and the DCT is appliedto those blocks. The correlation coefficients then compare the individual blocks. The authors also developed unique multiplication mask based IFD method in order to test the efficacy of the method. The presented image forgery detection method can detect both copy-move and Image splicing types of forgeries.

Toqeer Mahmood et al. [16] suggested an efficient and effective technique for the detection of region duplication forgery in digital images. The region duplication forgery detection (RDFD) is achieved by using the Stationary Wavelet Transform (SWT) based features. Toqeer Mahmood et al.'s technique divides the approximation sub-band of SWT into overlapping block sizes such as 4×4 and 8×8. The experimental results showed that 4x4 overlapping blocks produce more false detection thereby affecting the performance of the RDFD algorithm. The proposed technique makes use ofreduced length of the feature vector which helps in reducing the execution time of the algorithm.

## 3. K-MEANS CLUSTERING

K-means Clustering technique was introduced by James Mac Queen, in 1967. It is used to classify a given data set into 'K' groups where K is a positive integer number and are fixed prior. The center of each group or cluster is called the centroid. K-means clustering is an iterative algorithm and involves the two main steps namely: cluster assignment step and move centroid step. In the first step, the algorithm assigns all of the data points to the cluster, whose centroid is close to it; and in the second step, the mean value of all the data points present in the cluster is calculated, and the centroid is then moved to that mean location. The cluster assignment step and move centroid step are continuously repeated until there is no change in the clusters or the centroids stop moving. It is fast and robust and provides best results on separation of data sets from each other. However, it is challenging to select the optimal number of clusters and also the selection of initial centroids is random.

## 4. PROPOSED METHOD

The primary goal of the copy-move forgery detection technique is to determine whether an image contains a duplicated region or not. One right solution to this problem is to compare the original and the duplicated region by using pixel by the pixel-based approach. However, the main problem with this approach is that it consumes more computational time and hence costly when the size of the image is large. Another approach to this problem is a block-matching procedure in which the input image is segmented into small fixed-sized overlapping blocks. The flow chart of the propounded CMFD algorithm is presented in Figure 3. In the first step, the processes such as resizing, grayscale conversion, etc. are applied to the suspicious image, if the input image is RGB, etc. In the proposed work, the grayscale version of the colored image is obtained by using the standard formula given in Eq. 1.

$$I = 0.228R + 0.587G + 0.114B \tag{1}$$

Where, R, G, B and I are the three color channels of the input color image and its luminance component respectively.

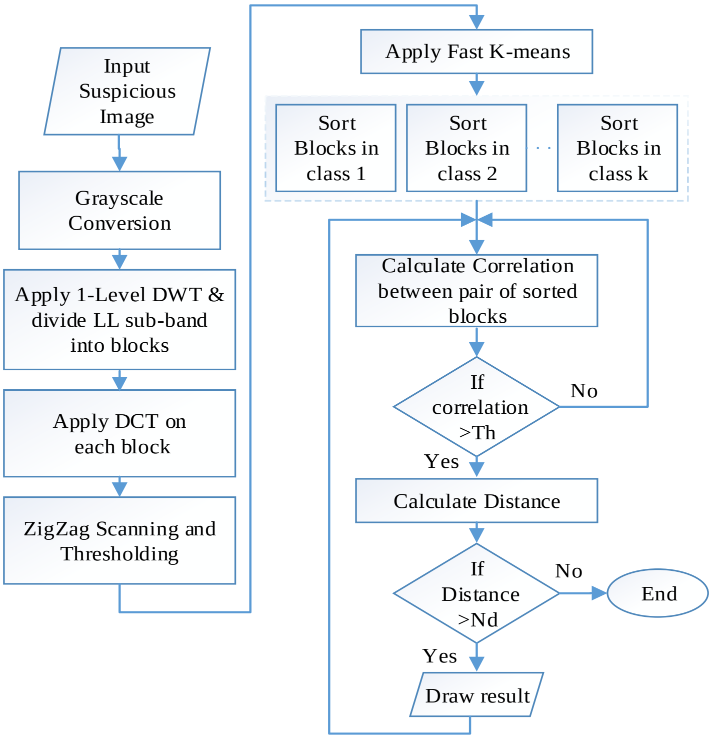

Figure 3. Flow Chart of the Proposed Method

In second step, one-level DWT is employed on the grayscale image I of size PxQ in order to obtain the four frequency sub-bands approximate (LL1), vertical (HL1), horizontal (LH1), and diagonal details (HH1). Out of the four sub-bands, the lowest frequency sub-band (LL1) image of size MxN (where M=P/21 and N=Q/21) is divided into small fixed size overlapping blocks of size mxm (here mxm=8x8) with a sliding factor of only one pixel. The total number of small fixed size blocks Nb is given by Eq. 2.

$$N_b = (M - m + 1) \times (N - m + 1) \tag{2}$$

In the third step, DCT is calculated for each fixed size 8x8 block. Each resulting m2 coefficient block is then reshaped as a one-row vector in zigzag order starting from the top left corner to the bottom right corner in the matrix as presented in Figure: 4. The DCT coefficients having indices > 9 are set to zero in order to reduce the feature vector length and hence reduce the overall processing time. The block feature vectors are retained in a single matrix A, and their number is always equal to the total number of blocks. After this, Fast K-means clustering technique [17] which is a simple and iterative approach is employed to cluster the duplicate blocks into K positive integer number of classes based on features. Figure: 5 shows an example of how blocks are clustered and sorted into classes.

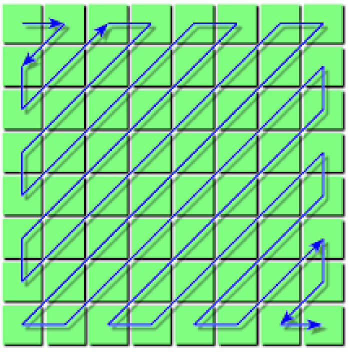

Figure 4. Zig-Zag Scanning Order

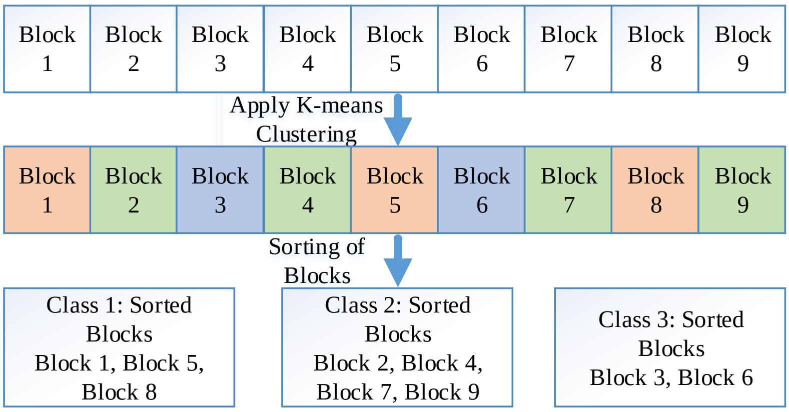

Figure 5. Example of clustering and sorting of blocks into classes

The block feature vectors stored in matrix A are then lexicographically sorted by a non-comparison and fast, stable data sorting algorithm called radix sort. In order to find the duplicated region, each row As(i) of the sorted matrix As is compared to As(i+1). The correlation and the spatial distance between the pair of sorted blocks are evaluated by using Eq. 3 and Eq. 4. The spatial distance is calculated in order to eliminate false detection.

$$C_r = \frac{\sum_{i=1}^{n}\left(Sx_i - \overline{Sx}\right)\left(Sy_i - \overline{Sy}\right)}{\sqrt{\sum_{i=1}^{n}\left(Sx_i - \overline{Sx}\right)^2 . \sum_{i=1}^{n}\left(Sy_i - \overline{Sy}\right)^2}} \qquad (3)$$

Where ‘n’ represents the total number of coefficients in the block. Sx, Sy are the DCT coefficients of the block and $\overline{Sx}$, $\overline{Sy}$ are their mean respectively. If the correlation (Cr)>Threshold (Th), then the pair of blocks is considered to be identical.

$$D_S = \sqrt{\left(AS_i^x + AS_{i+1}^x\right)^2 + \left(AS_i^y + AS_{i+1}^y\right)^2} \qquad (4)$$

Where $\left(AS_i^x, AS_i^y\right)$ and $\left(AS_{i+1}^x, AS_{i+1}^y\right)$ are the positions of the sorted blocks at (i) and (i+1) position respectively.

## 5. IMPLEMENTATION AND ANALYSIS

In this section, a brief detail about the Image Database and the Performance evaluation criteria for the proposed CMFD is presented. Further, the extensive experimental results of the CMFD method are evaluated in Experiment and Results Section.

### 5.1 Image Database

The performance of the proposed CMFD method based on hybrid transform and Fast K-mean clustering technique has been evaluated using reliable database MICC-F220. MICC-F220 database consists of 220 images. Out of 220 images, 110 are forged and 110 original. The performance of the algorithm is tested on a set of grayscale images of size 128x128 pixels with BMP format. The simulation results are achieved using MATLAB (R2016a) software on Windows 10 Pro, 64-bit Operating System, X64-based processor with Intel Core i7 processor having 8GB RAM.

### 5.2 Performance Evaluation Criteria

Copy-move forgery detection technique is said to be efficient only when it detects and locates the forged portions of the image correctly. Copy-move forgery detection is considered as a classification problem because it tries to classify the pixels or portions of the image as either copied or unique. Researchers use different evaluation metrics such as precision (P), recall (R), and F-measure or F1 Score to evaluate the performance of their classsification algorithms on different datasets. Thus, the efficiency of the propounded CMFD technique is assessed only by examining the different evaluation metrics defined in Eq. 5, Eq. 6, Eq. 7 and Eq. 8. The harmonic average of evaluation metrics given in Eq. 5, and Eq. 6 yields the metric in Eq. 7. F1 Score reaches its best value at 1 and worst at 0 which means perfect precision and recall. Precision (P), recall (R), and F1 Score together determines the accuracy of the proposed image copy-move forgery detection technique.

$$P = \frac{TP}{TP + FP} \tag{5}$$

$$R = \frac{TP}{TP + FN} \tag{6}$$

$$F_1 Score = \frac{2.P.R}{P + R} \tag{7}$$

Where TP, FP, and FN represents the total number of correctly detected forged images; the total number of original images wrongly detected as forged, and the total number of forged images incorrectly missed respectively. Also, the accuracy of the forgery detection technique is computed by using Eq. 8.

$$Accuracy = \frac{T_P + T_N}{T_P + T_N + F_P + F_N} \tag{8}$$

## 6. EXPERIMENTAL RESULTS

The performance evaluation metrics of the proposed CMFD method based on hybrid transform (DCT+DWT) and Fast K-mean clustering technique is computed in Table 1 and Table 2. The two tables (Table 1 and Table 2) show the comparison of the suggested algorithm with different recent and relevant algorithms with regard to recall, precision, F1 score and forgery detection time respectively. From the comparative analysis shown in Table 1, it is clear that the results are prominently convincing as compared to the works claimed by [10], [11], [13-16], [18-25]. The proposed forgery detection method achieved a precision value of 99.08, recall value of 98.18 and F1 Score value of 98.63 % which is relatively high in comparison to other previous related works assembled in Table 1.

Table 1. Comparison of precision, recall and F1 score

| Algorithm | Precision (%) | Recall (%) | F1 Score (%) |
|---|---|---|---|
| MH Alkawaz et al. [11] | 64.529 | 96.579 | 75.166 |
| Li. Yuenan [14] | 98 | 99 | 98 |
| K. Hayat et al. [15] | 72.50 | 96.30 | 81.801 |
| Toqeer Mahmood et al. [16] | 98.835 | 95.518 | 97.028 |
| Reza Davarzani et al. [22] | 93.57 | 90.45 | 91.98 |
| M. Bashar et al. [23] | 95.55 | 72.45 | 88.86 |
| S. Bayram et al. [24] | 96.38 | 17.87 | 30.15 |
| M. Emam et al. [25] | 88.5 | 76.9 | 82.3 |
| Pun CM et al. [19] | 94.7 | 89.9 | 92.2 |
| Junliu Zhong et al. [10] | 94.7 | 91 | 92.81 |

| | | | |
|---|---|---|---|
| G. Lynch [21] | 97 | 95 | 95.98 |
| V. K Singh & R. C Tripathi [18] | 80 | 75 | 77.42 |
| Mohammad Farukh Hashmi et al. [13] | 88 | 80 | 83.81 |
| Ashwini V Malviya & Siddharth A Ladhake [20] | 95.65 | 91.67 | 93.62 |
| Proposed Method | 99.08 | 98.18 | 98.63 |

Table 2. Comparison of the forgery detection time of different methods

| Algorithm | Forgery Detection Time(Seconds) |
|---|---|
| B.L Shiva Kumar and S. Baboo, [26] | 61.86 |
| I. Amerini et al., [27] | 56.32 |
| Mariam Saleem, [28] | 10.17 |
| G. Lynch, [21] | 7.68 |
| V.K Singh and R. C Tripathi [18] | 6.40 |
| Proposed Method | 2.12 |

Table 2 shows that the proposed algorithm also achieved improved time complexity of 2.12s as compared to the works presented in [18], [21], [26-28]. The application of the hybrid transform and Fast K-means clustering technique helped to reduce the length of feature vector and thus avoid the superfluous distance calculation by applying the triangle inequity and keeping track of lower and upper limits for distances between points and centers respectively, which in turn resulted in faster computation. The Bar chart representation of Table 2 is shown in Figure: 6.

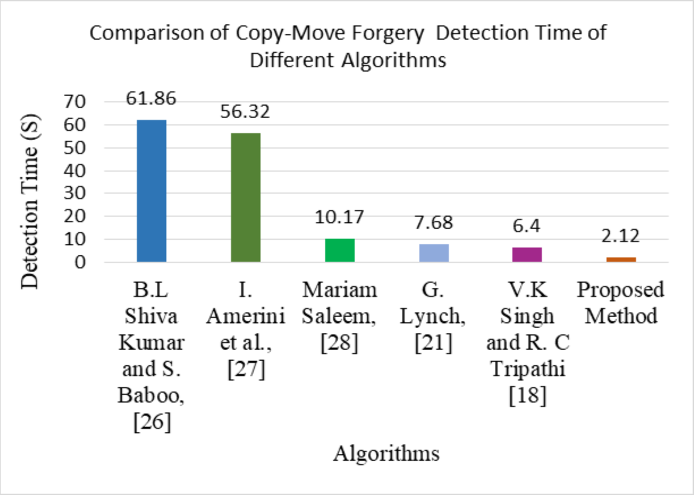

Figure 6. Bar Chart representation for comparison of forgery detection time

From experimental outcomes, it is also observed that the accuracy of the DCT based algorithm varies with the image size. When the size of the suspected image increases, the accuracy of the algorithm decreases and increases the time taken to detect the forgery. Figure: 7 displays the original image, forged image and CM forgery detected image while moving from left to right in the row.

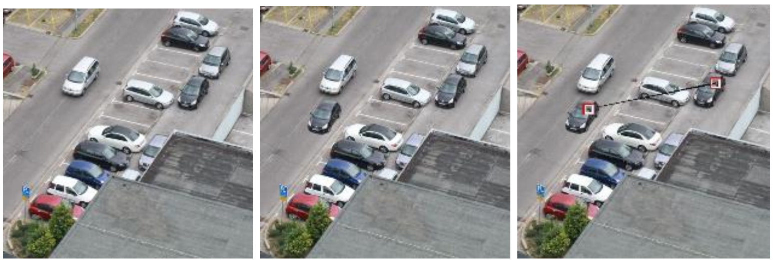

Figure 7. Visual Result of the proposed method

Furthermore, the F1 score value of the presented work is found to be closer to 1 which means perfect precision and recall values as compared to the other approaches present in the literature.

## 7. CONCLUSION

In this paper, an effective, efficient and automatic copy-move forgery detection method based on hybrid transform and fast K-means clustering technique which works in the absence of the prior knowledge about the image is presented. Firstly, DWT is used to reduce the image dimensions, and then DCT is used to limit the extent of the feature vector elements. In order to reduce the computation time further, Fast k-means clustering technique is used. FKM clustering technique helps to evade the unnecessary distance calculation by applying the trio inequality. However, it is clear from the conducted experiments, and the results obtained that the presented algorithm outperforms the other recent and relevant methods in terms of both detection time and accuracy. In the future, the performance of the system can be examined after applying various attacks such as compression, scaling, rotation, etc. The proposed algorithm can be tested for detecting multiple copy-pasted areas within the same image. The system can be improved further in order to reduce the forgery detection time to few seconds or even microseconds.

## REFERENCES

[1] Huynh T, Huynh K, Le T, Nguyen S, " A survey on image forgery detection techniques," In *Computing & communication technologies-research, innovation, and vision for the Future(RIVF)*, Can Tho, Vietnam, pp. 71–76, 2015.

[2] W. Luo, Z. Qu, F. Pan, J. Huang, "A survey of passive technology for digital image forensics," *Front. Computer Science China 1*, pp. 308–322, 2009.

[3] Muhammad Ali Qureshi and Mohamed Deriche, "A Bibliography of Pixel based blind image forgery detection techniques," *Signal Processing: Image Communication*, Vol. 39, pp. 46-74, 2015.

[4] D. Chauhana, D. Kasatb et al., "Survey on Keypoint Based Copy-move Forgery Detection Methods on Image," *International Conference on Computational Modeling and Security, Procedia Computer Science*, Vol. 85, pp. 206-212, 2016.

[5] R. Kaushik et al., "On Image Forgery Detection Using Two Dimensional Discrete Cosine Transform and Statistical Moments," *4th International Conference on Eco-friendly Computing and Communication Systems*, pp. 130-136, 2015.

[6] C. T, Bourouis S, Hamrouni K., "Copy-move image forgery detection based on SIFT descriptors and SVD-matching," In *Advanced Technologies for Signal and Image Processing (ATSIP), 1st International Conference on. IEEE,* pp. 125–129, 2014.

[7] Bo X, Junwen W, Guangjie L, Yuewei D, "Image copy-move forgery detection based on SURF," In *Multimedia Information Networking and Security (MINES), International Conference on IEEE,* pp. 889–92, 2010.

[8] J. Zheng, W. Hao,and W. Zhu, "Detection of Copy-Move forgery based on key-points positional relationship," December 2012.

[9] V. Christlein, C. Riess, et al., "An Evaluation of Popular Copy-Move Forgery Detection Approaches," *IEEE Transactions on Information Forensics and Security,* Vol. 7, Issue 6, pp. 1841-1854, 12 Sep 2012.

[10] J. Zhong, Y. Gan and J. Young et al., "A new block-based method for copy move forgery detection under image geometric transforms," *Multimedia Tools Applications, Springer,* Vol. 76, pp. 14887-14903, 2017.

[11] MH Alkawaz, G. Sulong, T. Saba, A. Rehman, “Detection of copy-move image forgery based on discrete cosine transform,” *Neural Comput Appl*, 2016.

[12] H. Moradi-Gharghani and M. Nasri, “A New Block-based Copy-Move Forgery Detection Method in Digital Images,” *IEEE Conference on Communication and Signal Processing,* 6-8 April 2016.

[13] M. Farukh Hashmia, Vijay Anand, Avinas G. Keskar, “Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform,” *AASRI Conference on Circuit and Signal Processing,* pp. 84-91, 2014.

[14] Yuenan Li, “Image Copy-Move Forgery detection using Polar Cosine Transform and Approximate Nearest Neighbor Searching,” *Forensic science International,* Vol. 224, Issue 1, pp. 59-67, 2013.

[15] K. Hayat, T. Qazi, “Forgery detection in digital images via discrete wavelet and discrete cosine transforms*,” Comput Electr Eng.*, 2017.

[16] Toqeer Mahmood, Zahid Mehmood, Mohsin Shah and Zakir Khan, “An efficient forensic technique for exposing region duplication forgery in digital images,” *Applied Intelligence,* Vol. 48, Issue 7, pp. 1791–1801, July 2018.

[17] C. Elkan, “Using the triangle inequality to accelerate K-means,” *ICML,* Pp. 147-153, 2003.

[18] V. K. Singh and R. C. Tripathi, "Fast and efficient region duplication detection in digital images using sub-blocking method,” *International Journal of Advanced Science and Technology*, Vol. 35, pp. 93-102, 2011.

[19] Pun CM, Yuan XC, and Bi XL, “Image Forgery Detection using adaptive over segmentation and feature points matching*, IEEE Transaction on Information Forensics and security*,” Vol. 10, pp. 1705-1716, 2015.

[20] Ashwini V Malviya and Siddharth A Ladhake, “Pixel based Image Forensic Technique for copy-move forgery detection using Auto-Color Correlogram,” *Seventh International conference on communication, computing, and virtualization*, Vol. 79, pp. 383-390, 2016.

[21] G. Lynch, F. Y. Shih and H.Y. M. Liao, “An efficient expanding block algorithm for image copy-move forgery detection,” *Elsevier Information Sciences,* Vol. 239, pp. 253-265, 2013.

[22] Reza Davarzani, Khashayar Yaghmaie, Saeed Mozaffari,and Meysam Tapak, “Copy-move forgery detection using multiresolution local binary patterns,” *Forensic Science International,* Vol. 231, pp. 61–72, 2013.

[23] M. Bashar, K. Noda, N. Ohnishi, and K. Mori, “Exploring duplicated regions in natural images,” *IEEE Trans. Image Processing,* March 2010.

[24] S. Bayram, H. T. Sencar, and N. Memon, “An efficient and robust method for detecting copy-move forgery,” In *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 1053-1056, 2009.

[25] M. Emam, Q. Han, and X. M. Niu, “PCET based copy-move forgery detection in images under geometric transforms,” *Multimedia Tools and Applications,* Vol. 75, Issue 18, pp. 11513-11527, 2016.

[26] B. L Shiva Kumar, S. Baboo, “Detection of Region Duplication forgery,” *International Journal of computer science issues,* Vol. 8, No. 4, pp.199-205, 2011.

[27] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, G. Serra, “Geometric tampering on estimation by means of the SIFT based forensic analysis,” *Proceedings of the IEEE ICASSP*, Dallas, TX, USA, 2010.

[28] Mariyam Saleem, “A Key-Point based robust algorithm for detecting cloning forgery,” *International Journal of current engineering and Technology,* Vol. 4, No. 4, August 2014.