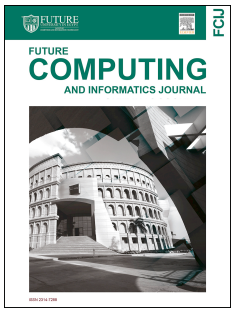
Accepted Manuscript



A Fast SIFT Based Method for Copy Move Forgery Detection

Hesham Ahmed Alberry, Abdelfatah Hegazy, Gouda i Salama

PII: S2314-7288(18)30011-4

DOI: 10.1016/j.fcij.2018.03.001

Reference: FCIJ 36

To appear in: *Future Computing and Informatics Journal*

Received Date: 22 January 2018

Revised Date: 14 March 2018

Accepted Date: 30 March 2018

Please cite this article as: Alberry HA, Hegazy A, Salama Gi, A Fast SIFT Based Method for Copy Move Forgery Detection, *Future Computing and Informatics Journal* (2018), doi: 10.1016/j.fcij.2018.03.001.

Title:

A Fast SIFT Based Method for Copy Move Forgery Detection

Authors:

Hesham Ahmed Alberry

Department of computer Science, Faculty of Computers and Information, Arab Academy for Science, Technology and Maritime Transport, Cairo, Egypt.

Alberry003@gmail.com

Abdelfatah Hegazy

Department of computer Science, Faculty of Computers and Information, Arab Academy for Science, Technology and Maritime Transport, Cairo, Egypt.

ahegazy@aast.edu

Gouda i.Salama

Department of computer engineering, MTC, Cairo, Egypt

gisalama@mtc.edu.eg

A Fast SIFT Based Method for Copy Move Forgery Detection

Abstract— Image forensics is an important area of research used to indicate if a particular image is original or subjected to any kind of tampering. Images are essential part of judgment in tribunals. For forensic analysis, image forgery-detection techniques used to identify the forged images. In this paper, an effective algorithm to indicate Copy Move Forgery in digital image presented. The Scale Invariant Feature Transform (SIFT) and Fuzzy C-means (FCM) for clustering are utilized in the proposed algorithm. A number of numerical experiments performed using the MICC-220 dataset. The authors created an additional dataset, which consisted of 353 color images. The proposed algorithm tested by using both datasets where the average detection time on the MICC-220 data set is reduced by 14.67 % over the existing traditional SIFT-based algorithm. For the created dataset, the average detection time reduced by 15.91 % over the existing traditional SIFT-based algorithm.

Keywords— Copy-move forgery, Forgery detection techniques, copy-move attack, Image forensics, SIFT (Scale Invariant Feature Transform).

1. INTRODUCTION

Today, digital images are used extensively in various fields in our life through important areas such as news reports, forensics sciences, surveillance services, online marketing and medical diagnosis. Moreover, they can be used as proof in tribunals, and in press to adjust the meaning of pictures in order to affect the readers' points of views. Thus, this area of digital image forensics [1] to specify the originality of digital image has become an important area of research to regain trust in digital image [2]. The forensic analysis for digital images helps in providing information to support law enforcement, security, and intelligence agencies. Various techniques can be introduced to examine and legitimize the digital image's content. The image forgery detection is analyzed to active and passive methods [3]. The active method relies on digital signatures or watermarking [4]. That method depends on the information taken previously from the original image. It is clear to notice that those methods are not powerful. Because they require certain equipment like particular cameras to add watermark or a signature to a captured image; moreover, it can be manipulated. On the other hand, passive methods are optimized to examine images without resorting to previous information, where we have to make vague decision concerning how images have been manipulated. The majority of passive methods depend on supervised learning by using the extraction of certain characteristics to distinguish the original picture from the fake one.

We have many easy image editing programs, such as Photoshop. Moreover, forger introduced various methods for image processing to obtain forged image in a tricky way such as copy move image forgery that uses the same image [5]; image splicing use diverse parts from various images to manipulated picture [6], and image retouching [7] that leave a fine modification in the picture. In image splicing, we optimize areas from various pictures to make a forged one. In copy-move image forgery, regions of the images could be duplicated into the same image to hide an important content in that image.

Because the convenient elements are similar to the copied parts, like color and noise, it is necessary and important to distinguish the manipulated areas from the actual ones. Moreover, to eliminate the visual traces of image forgeries, a counterfeiter uses different post-processing procedures like blurring, edge smoothing, and noise.

This paper concentrates on Copy Move Forgery Detection (CMFD) and introduce a fast technique optimizing Scale Invariant Feature Transform (SIFT) and fuzzy c-means (FCM) clustering. This paper classified into four sections. The first section handles the common workflow of (CMFD); the second one discusses the overview of SIFT forgery method and clustering method; the third one concentrates on the introduced model and the framework; the fourth section discusses the experimental results and discussions, and finally the fifth section handles the paper conclusion and the suggestions for future work.

1. WORK FLOW FOR CMFD

Most techniques for CMFD follow the same fundamental procedures [8] as shown in workflow figure 1. In the first step, the pre-processing procedure is applied to the input image. This step is very necessary for enhancing the picture data and the picture features and paves the way for more detection. The input image transformed into grey-scale and another preprocessing can be optimized such as filtering or image resizing. After this procedure of preprocessing, the feature extraction to obtain feature of the picture is optimized. This procedure is classified into block based method [9], which split image into blocks and then obtain integral feature for each block such as Discrete Cosine Transform DCT [10], Singular Value Decomposition (SVD) [11], Discrete Wavelet Transform DWT [12] and Histogram of Orientated Gabor magnitude (HOGM)[13]. Key point based technique [14], that distinguish high-entropy image regions such as Scale Invariant Features Transform (sift) [15], [16] and Speeded Up Robust Features (Surf)[17]. Hybrid technique which integrate both techniques [18], [19], [20], that introduced a blended feature.

After the feature extraction procedure, it is very important to match identical features that mark doubled regions, and then optimize filtering to diminish the fake matched features and finally decide if the image is forged or not.

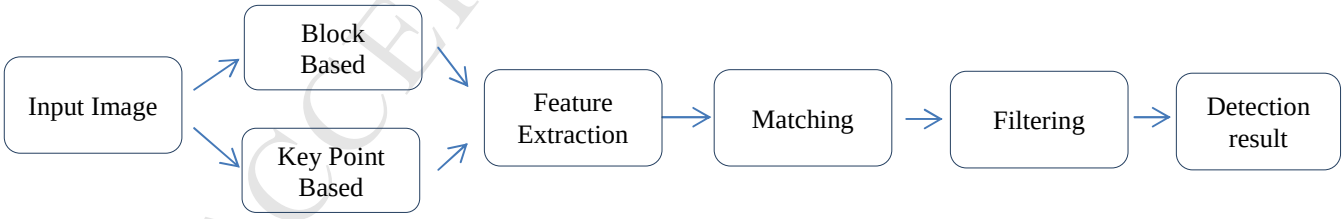


Figure 1Typical workflow for CMFD

2. REVIEW OF THE SIFT ALGORITHM AND CLUSTERING

2.1 SIFT ALGORITHM

Various ways are presented to explore the problem of (CMFD). The majority of the introduced algorithms in the feature extraction for revealing and illustrating local visual features often demand two procedures: the first procedure is detecting the interest points that are centralized, whilst the second procedure robust local descriptors are constructed to be invariant orientation and scaling [16], [21].

SIFT algorithm converts an image data into local feature vectors named SIFT descriptors. Those features have the power to geometric transformations that are constant to scaling and rotation. This algorithm is divided into the following three main stages:

1. *Scale Space Extrema Detection*

The scale-space image is known as as L(x, y, σ) that is created by the convolution process between function and image. In this situation, convolution between Gaussian function, G(x, y, σ), and an image I(x,y) is used:

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y) \quad (1)$$

$$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{-(x^2+y^2)/2\sigma^2} \quad (2)$$

Optimizing a computable approximation of Gaussian's Laplacian is used to elicit the key points of the image named Difference of Gaussians (DoG)[22], where, a DoG Image D is introduced as follows:

$$\mathrm{D}(\mathrm{x}, \mathrm{y}, \sigma) = \mathrm{L}(\mathrm{x}, \mathrm{y}, \mathrm{k}\sigma) - \mathrm{L}(\mathrm{x}, \mathrm{y}, \sigma) \quad (3)$$

Where L(x, y, kσ) is the convolution of the original image, I(x, y) with the Gaussian blur G(x, y, kσ) at scale kσ.

2. *Keypoint Localization*

The image extrema contains the image main points. In order to select the main point from image extrema where the main points are unsettled over image variation have to be selected through rejecting the points over image edges and those which are characterized by low contrast. The Taylor expansion of scale-space function D (x,y, σ) shifted such that the sample point is origin:

$$D(x) = D + \frac{\partial D^T}{\partial x} x + \frac{1}{2} x^T \frac{\partial^2 D}{\partial x^2} x \quad (4)$$

3. *Key point Descriptor Generation*

To ensure that The SIFT descriptors are constant in scaling and rotation, a canonical orientation is specified to each main point. In order to specify the descriptor orientation, a gradient orientation histogram is computed in the neighborhood of the key point. Particularly, for an image sample L(x, y, σ) at scale σ (the scale in which that key point was detected), the gradient magnitude m(x, y) and orientation θ(x, y) are computed using eq (3, 4):

$$m(x, y) = (((L(x+1, y) - L(x-1, y))^2 + ((L(x, y+1) - L(x, y-1))^2)^{\frac{1}{2}} \quad (5)$$

$$\theta(x, y) = tan^{-1}(\frac{L(x, y+1) - L(x, y-1)}{L(x+1, y) - L(x-1, y)}) \quad (6)$$

A feature vector with 128 elements is created for each descriptor. This vector is composed of the values of orientation histogram, in image plane and scale space form with 4X4 array of histograms and 8 orientation bins in each. The results obtained are 4X4X8=128element feature vector.

2.2 FUZZY C-MEANS CLUSTERING

FCM stands for Fuzzy C-means is defined as a technique of clustering that can be a section of data that is belong to two or more clusters [23],[24] , in order to decrease time complexity by clustering Sift key point and the time consumed for matching key points. It depends on reducing the following objective function:

$$J_m = \sum_{i=1}^{N}\sum_{j=1}^{c} u_{ij}^{m} \left\|x_i - c_j\right\|^2 \ , 1 \le m < \infty \qquad (7)$$

Where:

m is any real number greater than 1.

u_{ij} is the degree of member ship of x_i in the cluster j.

x_i is the ith of d dimension measured data.

c_j is the d-dimension center of the cluster.

$\|*\|$ is any norm expressing the similarity between any measured data and the center.

A refined application of the objective function introduced above is executed Fuzzy partitioning which is created with the update of membership uij and the cluster centers cj by:

$$u_{ij} = \frac{1}{\sum_{k=1}^{c}\left(\frac{\|x_i - c_j\|}{\|x_i - c_k\|}\right)^{\frac{2}{m-1}}} \qquad , c_j = \frac{\sum_{i=1}^{n} u_{ij}^{m} \cdot c_j}{\sum_{i=1}^{n} u_{ij}^{m}} \qquad (8)$$

This repetition will stop when $\max_{ij}\left\{\left|u_{ij}^{k+1} - u_{ij}^{k}\right|\right\} < \varepsilon$ where ε is a termination criterion between 0 and 1, whereas k are the iteration steps. This step assemble to a local minimum or a saddle point of jm.

The algorithm is performed by optimizing the following procedures:

1. *Initialize U=[u_{ij}] matrix, $U^{(0)}$*
2. *At k-step: compute the centers vectors $C^{(k)} = [c_j]$ with $U^{(k)}$* $\quad c_j = \frac{\sum_{i=1}^{n} u_{ij}^{m} \cdot c_j}{\sum_{i=1}^{n} u_{ij}^{m}}$
3. *modify $U^{(k)}$, $U^{(k+1)}$* $u_{ij} = \frac{1}{\sum_{k=1}^{c}\left(\frac{\|x_i - c_j\|}{\|x_i - c_k\|}\right)^{\frac{2}{m-1}}}$
4. *If $\| U^{(k+1)} - U^{(k)} \| < \varepsilon$ then STOP; otherwise return to step 2*

3 PROPOSED MODEL

The introduced technique depends on the SIFT algorithm to elicit solid features which enable it to specify if a region of an image was a copy-moved. The introduced technique decreases time complexity of SIFT using FCM clustering method. In the proposed algorithm, SIFT keypoints are clustered on the basis of their descriptors then , center keypoint and its neighbor are matched with other center keypoint and its neighbor clusters instead of identifying all keywords in the picture. The proposed algorithm has the ability to reveal Copy Move forgery very fast without influencing the accuracy of matching process. Fig 2. Illustrates a block diagram of the proposed

algorithm. First, SIFT algorithm from the image is used to elicit key points. Then, the feature descriptor is elicited from every key point on the image including 128 dimensional.

The resemblance between the descriptors is calculated to specify the matching among the descriptors for specifying the potential forgery on the image. The basic obstacle in this algorithm is the computational complexity of the matching stage where it is very high as a result of the big number of key points elicited from the image and the matching process among them. Using clustering algorithm for clustering the keypoints depending on their descriptors can be a solution to this issue.

Specifying data points for every cluster such that items in the same cluster as similar as possible, but items that belong to the diverse clusters are as various as possible, optimizing three main fundamental parameters to enhance their best values and every center of the clusters key points and their close neighbors are matched only to other clusters rather than assembling all the other key points.

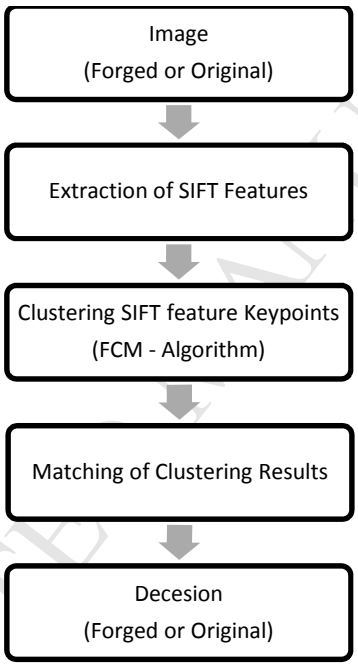


Figure 2. A block diagram of the proposed method

4 EXPERIMENTAL SETUP

Experiments are executed on total 573 pictures. Two data sets were used to test the model; MICC-220 and our own data set. MICC-220 is created by 220 images, where 110 images are tampered and 110 are original. The resolution of the picture differs from 722 × 480 to 800 × 600 pixels and the size of the false patch involve the average 1.2% of the whole image. The main issue in MICC-220 is the falsification and all the conversion located in the fake images was performed inconsiderably. This issue can be solved to measure the suggested algorithm through a real falsification by proposing new data set. The data set includes 353 images that are obtained from Google search engine. 260 images are tampered and 93 are original. In order to test the model with various kinds of attacks, the images are manipulated deliberately. The resolution of images differs from 3024 × 1963 to 800 × 600 pixels. To examine the results, it is compared with [16], where the performance time is decreased with the same accuracy rate optimizing the same standard dataset and our own data set. Fig 3,4 display the suggested algorithm SIFT matched pairs from the two optimized datasets that give examples for original image, tampered image, and detection result matched pairs.

Figure 3. Examples from our own Data set original images, tampered images, and detection result matched pairs.

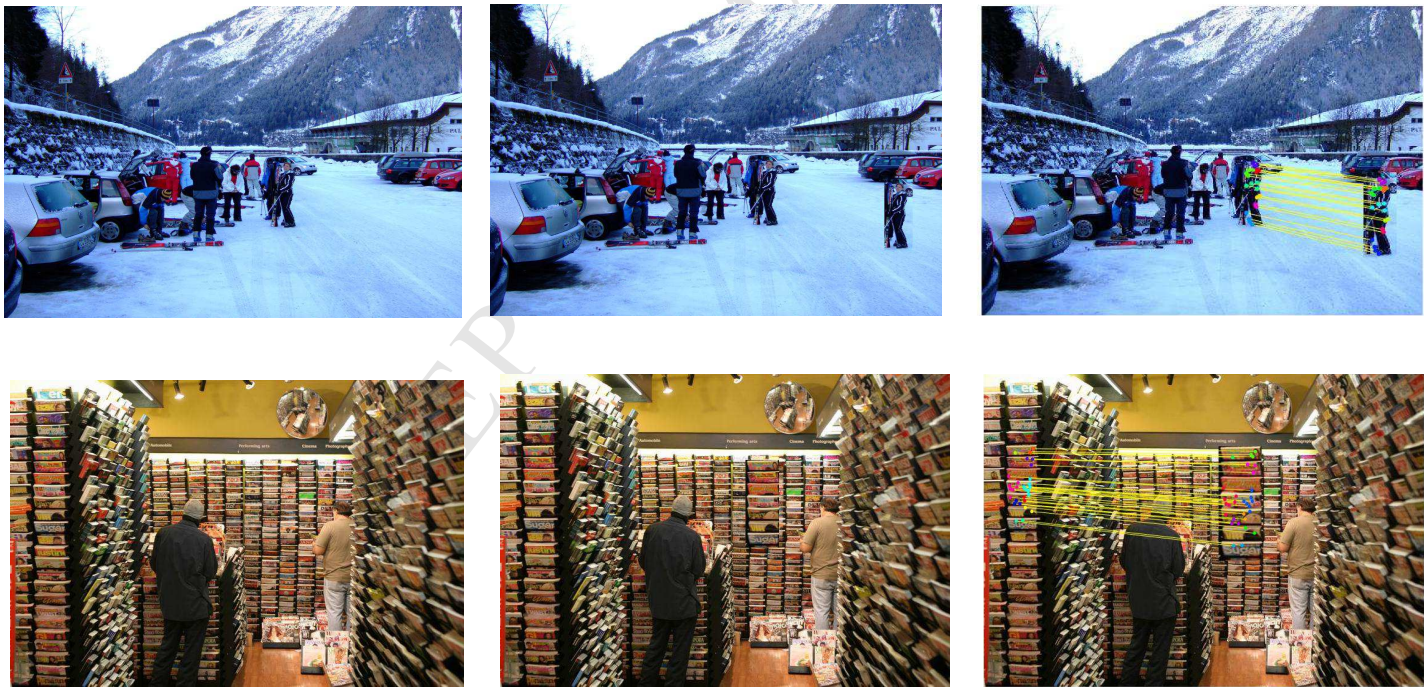


Figure 4. Examples from MICC-220 Data set original images, tampered images and detection result matched pairs.

5.2 Evaluation Metrics

The performance of detection method is measured in the light of true positive rate (TPR), false positive rate (FPR), and time complexity where:

$$\text{TPR} = \frac{\text{Images detected as forged being forged}}{\text{Total number of forged images}} \quad (9)$$

$$\text{FPR} = \frac{\text{Images detected as forged being original}}{\text{Total number of original images}} \quad (10)$$

TPR refers to the percentage of forged images which are correctly specified. FPR refers to the percentage of the original images, that are falsely specified as a manipulated one. A comparison is made between the values of FPR, TPR, and time (in seconds) for data sets optimizing SIFT without FCM clustering [16] and with clustering combination. There are three fundamental main parameters in FCM algorithm, that are used for their best value to obtain the best results. Those parameters are:

a. Number of Clusters

Number of clusters to create. Four values for this parameter {2,4,6,8}

b. Maximum number of iterations

The maximum number of training epochs. Four values for this parameter {25,50,75,100}

c. Minimum amount of improvement

Minimum improvement in objective function between two consecutive iterations. Four values for this parameter {0.001, 0.0001, 0.00001, 0.000001}

The performance of a clustering algorithm may be affected by the chosen values of parameters. There are many ways for selecting these parameters. In data-mining and data analysis software packages, the number of clusters is specified by the user. To obtain a satisfactory clustering result, the number of iterations needed for the user to execute the algorithm must be defined. The validity of the clustering result is assessed visually without applying any formal performance measures. In the proposed model, a wide range of parameters are applied where the performance measured in terms of accuracy and time complexity. A narrower range of values is determined for each parameter as shown in the conducted experiments.

5.3 Results

Table 1 reports the performance measures (TPR, FPR and the Detection time) of the SIFT based algorithm [16] using the two data sets. It could be noticed that the TPR of MICC-220 is superior than our own data set because our own data set are professional forged digital image with diverse combination of post processing on image in an deceiving way. Also, it could be seen that the total detection time for our own data set is more than the total time of MICC-220 data set because our own data set includes 353 images with resolution differs from 3024 × 1963 to 800 × 600 pixels ,while the MICC-220 includes 220 images with resolution differs from 722 × 480 to 800 × 600 pixels.

Table.1 Results of the SIFT algorithm in terms of the three evaluation metrics for both data sets

	MICC-220	**Our own Data Set**
TPR	99.09%	71.69%
FPR	9.09%	10.83%
Detection Time (hh:mm:ss)	00:16:15	01:15:57

5.3.1 Changing FCM parameters in MIC-220:

Three main fundamental parameters are used for their best values to enhance the performance time with the same accuracy in the FCM algorithm. First parameter: the number of clusters, which differs from 2 to 8 as shown in Table 2, the number of clusters that offer high accuracy rate, and a minimum performance time is adopted as the best result and shaded in the table. The number of clusters was specified in the light of the performance time and accuracy standard of the introduced technique for all images in the MIC-220 dataset.

Table 3 displays the second parameter changing maximum number of repetitions, which differed from 25 to100 and minimum performance time is adopted as the best result and is shaded. Table 4 illustrates the third parameter changing minimum amount of improvements to fulfill the best results.

Table.2 Changing Number of Clustering. Cluster Number -> {2, 4, 6, 8}

ClusNum ->	2	4	6	8
TPR	98.18%	99.09%	98.18%	98.18%
FPR	7.27%	7.27%	7.27%	9.09%
Detection time	00:12:19	00:12:45	00:12:55	00:13:10

Table.3 Changing Maximum number of iterations. Maximum Iteration -> {25,50,75,100}

MaxItr ->	25	50	75	100
TPR	99.09%	99.09%	99.09%	99.09%
FPR	7.27%	9.09%	7.27%	7.27%
Detection time	00:15:37	00:13:52	00:13:25	00:13:26

Table.4 Changing Minimum amount of improvement. Minimum Improvement -> {0.001, 0.0001, 0.00001, 0.000001}

MinImpr ->	0.001	0.0001	0.00001	0.000001
TPR	99.09%	99.09%	99.09%	99.09%
FPR	7.27%	7.27%	7.27%	8.18%
Detection time	00:13:33	00:13:28	00:13:23	00:13:37

5.3.2 Changing FCM parameters in our own dataset:

There are three main fundamental parameters results in the new introduced data set in FCM algorithm. Changing number of clusters is shown in table 5. Table 6 illustrates change values of the maximum number of repetitions. Table 7 clarifies change values of minimum amount of enhancement and best result shaded in tables.

Table.5 Changing Number of Clustering. Cluster Number -> {2, 4, 6, 8}

ClusNum ->	2	4	6	8
TPR	71.54%	71.15%	71.54%	71.92%
FPR	10.75%	10.75%	11.83%	11.85%
Detection time	01:00:21	01:02:00	01:11:04	01:03:52

Table.6 Changing Maximum number of iterations. Maximum Iteration -> {25, 50, 75,100}

MaxItr ->	25	50	75	100
TPR	71.15%	71.15%	71.15%	71.15%
FPR	10.75	10.75%	10.75%	10.75%

Detection time	01:08:01	01:09:17	01:22:52	01:01:57

Table.7 Changing Minimum amount of improvement. Minimum Improvement -> {0.001, 0.0001, 0.00001, 0.000001}

MinImpr ->	0.001	0.0001	0.00001	0.000001
TPR	71.54%	70.77%	70.77%	71.54%
FPR	11.83%	11.83%	11.83%	11.85%
Detection time	01:08:17	01:03:44	00:58:12	00:58:26

5.3.3 Best Parameters and Improvements

Tables 8 illustrate the enhancement in the accuracy and detection time by applying the proposed algorithm on the MICC-220 data set. It could be noticed that, the average detection time after applying the proposed algorithm is enhanced by 14.67 % than applying the SIFT based algorithm with the same accuracy.

Table 8 enhancement percentage of the proposed algorithm optimizing MICC-220 dataset.

	MICC-220	Improvement
TPR	99.09%	0%
FPR	9.09%	0%
Detection Time (hh:mm:ss)	00:13:52	14.67 %

Tables 9 illustrate the enhancement in the accuracy and detection time by applying the proposed algorithm our own data set. It could be noticed that, the average detection time after applying the proposed algorithm is enhanced by 15.91 % than applying the SIFT based algorithm.

Table.9 Enhancement percentage of the introduced technique optimizing our own dataset.

	our own data set	Improvement
TPR	71.92%	0.23 %
FPR	11.85%	1.2 %
Detection Time (hh:mm:ss)	01:03:52	15.91 %

5.4 Discussions

According to the results obtained from the tables, it is obvious that blending fuzzy c-means with the sift algorithm has apparent effect on the time complexity on the algorithm. The simple attacks and conversion in MICC-220 have their impact on the high values of TPR and FPR comparing those values in our own dataset. It is obvious that using the number of clusters, the maximum number of repetition and the minimum enhancement FCM parameters grant more deep insight on the algorithm effect. Keeping default value of other parameters with optimizing both the default values of each parameter or using one parameter does not grant the best way to improve the algorithm so the three parameters should be sequentially optimized.

It is obvious that after using the MICC-220 dataset, there are no main enhancement in the accuracy (TPR and FPR), but the enhancement is significant relating to terms of time complexity. In the introduced dataset, enhancement was in both metrics accuracy and time. The essential justification is optimizing FCM clustering on key points SIFT features and locations decreases the ambiguity done before assembling particularly when falsification is deliberately executed.

6 Conclusion &Future Work

The researchers usually optimize the key point based techniques for detection of Copy Move forgery. While raising the number of key points, the computational requirements will raise in these techniques, so minimal execution time will be needed. In this research, the researcher optimized FCM technique for clustering the SIFT key points to decrease time complexity. The experimental results indicate that the propose algorithm decreases the detection time of appreciably same accuracy standards and minor enhancement in some cases. This research detects also in the status of rotation, scaling and multiple Copy Move attacks.

In this research, a new data set is created for CMFD that includes more manipulated pictures that were performed deliberately by professionals. The obtained data set is an open source and free to be optimized as benchmarking for more comparisons. According to this research, it is highly recommended that optimizing multiple clustering algorithms or even using the FCM by matrix optimization rather than the sequential optimization done.

7 References

[1]	Kirchner,"Notes on Digital Image Forensics and Counter Forensics, In: Forensic Analysis of Re-sampled Digital Signals", pp.1-97, 2012.
[2]	Warbhe, Anil Dada, R. V. Dharaskar, and V. M. Thakare. "Computationally Efficient Digital Image Forensic Method for Image Authentication." Procedia Computer Science 78 ,pp464-470 ,2016.
[3]	O.Al-Qershi and B.Khoo," Passive detection of copy-move forgery in digital images: State-of-the-art", Forensic Science International 231, pp. 284–295, 2013.
[4]	Qasim, Asaad F., Farid Meziane, and Rob Aspin. "Digital watermarking: applicability for developing trust in medical imaging workflows state of the art review." Computer Science Review 27 ,pp45-60,2018.
[5]	R.S.Oommen, Jayamohan.M and Sruthy S,"A Survey of Copy-Move Forgery Detection Techniques for Digital Images", International Journal of Innovation in Engineering and Technology, Volume 5 Issue2, pp.429-426, 2015.
[6]	Salloum, Ronald, Yuzhuo Ren, and C-C. Jay Kuo. "Image Splicing Localization Using A Multi-Task Fully Convolutional Network (MFCN), Journal of Visual Communication and Image Representation 51,pp201-209 2018.
[7]	Meenakshi Sundaram, Nandini,"IMAGE RETOUCHING AND IT'S DETECTION - A SURVEY", International Journal of Research in Engineering and Technology" Volume: 04 Special Issue: 14,pp.30-34,2015
[8]	N.B.AbdWarif, A.W.AbdulWahab, M.Y.Idris, R.Ramli,R. Salleh, Sh.Shamshirb and K.KwangRaymond," Copy Move Forgery Detection :Survey ,challenges and future directions", Journal of Network and Computer Applications 75, pp.259–278, 2016.
[9]	A.Warbhe, R.V.Dharaskar and V.Thakare, " Block Based Image Forgery Detection", International Journal of Engineering Sciences & Research Technology, ISSN: 2277-9655 pp.289-296, August 2015.
[10]	S.Kumar, J.Desai, S.Kumar and J.Desai," A Fast DCT Based Method for Copy Move Forgery Detection, IEEE 2nd international conference on image information processing, pp.649-654 , 2013.
[11]	Zhang, Ting, and Rang-ding Wang. "Copy-move forgery detection based on SVD in digital image." Image and Signal Processing, 2009. CISP'09. 2nd International Congress on. IEEE, 2009.
[12]	Yadav, Preeti, and Yogesh Rathore. "Detection of copy-move forgery of images using discrete wavelet transform." International Journal on Computer Science and Engineering 4, no 4,p.565-570, 2012.
[13]	Lee, Jen-Chun. "Copy-move image forgery detection based on Gabor magnitude." Journal of Visual Communication and Image Representation 31, pp.320-334, 2015.

[14]	A.Dada, R. V. Dharaskarb and V. M. Thakarec,"ASurvey on Keypoint Based Copy-Paste Forgery Detection Techniques", Science Direct Computer Science 78, pp.61-67, 2016
[15]	Warif, Nor Bakiah Abd, Ainuddin Wahid Abdul Wahab, Mohd Yamani Idna Idris, Rosli Salleh, and Fazidah Othman ,"SIFT-Symmetry: A robust detection method for copy-move forgery with reflection attack", Journal of Visual Communication and Image Representation 46,pp 219-232,2017
[16]	I.Amerini, L.Ballan, R.Caldelli, A.Bimbo and G. Serra," A SIFT-based forensic method for copy-move attack detection and transformation recovery", IEEE Transactions On Information Forensics And Security6.3, pp1099-1110,2011
[17]	R.Raj and N.Josephb," Keypoint Extraction Using SURF Algorithm For CMFD ", Procedia Computer Science 93 ,pp.375 -381, 2016.
[18]	F.Yanga, Jingwei Lia, Wei Lua and Jian Wengb," Copy-move forgery detection based on hybrid features", journal of engineering applications of artificial intelligence 59 , pp.73-83, 2017
[19]	Z.Ting, Wang Rang-ding," Detection of duplication regions uniform and non-uniform regions", International Conference Computer Modelling and Simulation IEEE , pp.455-460,2013.
[20]	Hayat, Khizar, and Tanzeela Qazi. "Forgery detection in digital images via discrete wavelet and discrete cosine transforms." Computers & Electrical Engineering 62 pp448-458,2017.
[21]	Suvarna G. Upase, Sunil V. Kuntawar,"Copy-Move Detection of Image Forgery by using DWT and SIFT Methodologies", International Journal of Computer Applications (0975 – 8887)Volume 148 – No.7, pp.37-39,2016
[22]	D.G.lowe,"distinctive Image Features from Scale-Invariant Keypoints",International journal of computer vision,Vol 60,no 2 ,pp1-22,2004
[23]	Gong, Maoguo, Yan Liang, Jiao Shi, Wenping Ma, and Jingjing Ma. "Fuzzy c-means clustering with local information and kernel metric for image segmentation." IEEE Transactions on Image Processing 22, no. 2 , pp.573-584,2013.
[24]	Yang, Miin-Shen, and Yessica Nataliani."Robust-learning fuzzy c-means clustering algorithm with unknown number of clusters." Pattern Recognition 71, pp45-59 ,2017.