An Efficient Circular Block Approach for Copy-Move Forgery Detection

Article · December 2015

CITATION
1

READS
69

3 authors, including:

Rafsanjany Kushol
Islamic University of Technology
4 PUBLICATIONS **2** CITATIONS

SEE PROFILE

An Efficient Circular Block Approach for Copy-Move Forgery Detection

Md Sirajus Salekin*, Rafsanjany Kushol, and Md. Hasanul Kabir

***Abstract*—Copy-move forgery is a special type of digital forgery in which a part of the image is copied and pasted somewhere else in the same image with the intent to cover any important image feature. In image forensics, to detect this type of forgery we need a robust detection method which ensures the correct detection even if the image is noisy, compressed, blurred, scaled, rotated, flipped, etc. In this paper, we are interested in the detection of copy-move forgery more accurately especially in case of noise, blur and compression by reducing the number of false positives and negatives. To address this issue, we have developed an efficient overlapping circular block approach for detecting the copy-move forgery using the mean and contrast information of the overlapping blocks of the image. The circular block approach ensures rotation invariance and mean-contrast feature selection approach and comparison ascertain better performance especially for compressed image with low quality factor and also for the blurred image. The proposed approach has been evaluated and compared with competitive approaches using comprehensive image dataset. Our experimental results indicate that our method can detect duplicated regions in copy-move forgery with higher accuracy, especially for JPEG compressed, blurred and noisy images.**

***Keywords*—Circular block, Copy-move forgery, Digital forensics, Duplicated region, Image forensics, Image forgery**

I. Introduction

The intention of digital forgery is to change the image's original information by adding or removing segment. On account of the handiness of image retouching or editing software tools in recent times, it is very easy to tamper any type of digital images. That's why it has been very common to add or remove anything from an original image which causes the lead of digital image forgery. Detecting digital image forgery is a challenging task in the field of crime, journalism etc.

Several types of forgery is possible based on the techniques used in forged image which we can group into three major categories. They are image splicing, image tampering or copy-moved. Image splicing uses two or more images to create a composite forged one where any part of an image is used with another image. Image tempering uses any image retouching tools for enhancing or reducing any image features without changing its appearance. And copy-move forgery is a special type of digital forgery in which a part of the image is copied and pasted somewhere else in the image with the intent to cover any important image feature. The idea of the copy-move forgery can be illustrated in Figure 1. Here, in the original image there was one swan, but in the forged image there are two swans. The second swan has been copied from the first one and pasted in a flipped manner.

Fig. 1: Example of copy-move forgery. From left to right: original Image, forged Image.

In this paper, our main intend is to detect copy-move forgery. For detecting this type of forgery we have to face some challenges such as forged segment can be exactly or approximately copied or modified copy. Modified copy is the advanced forgery where the main intention is to hide the forgery and makes the forgery detection difficult. While saving the image, it can be compressed and as a result some image

*Corresponding author.

Md Sirajus Salekin, Rafsanjany Kushol and Md. Hasanul Kabir are with the Deptartment of Computer Science and Engineering, Islamic University of Technology, Dhaka, Bangladesh. e-mail: salekin@iut-dhaka.edu, kushol@iut-dhaka.edu and hasanul@iut-dhaka.edu.

Manuscript received May 20, 2015; revised December 14, 2015.

information may be lost. Besides different kinds of noise like Gaussian noise or Gaussian blurring can be introduced for hiding copied information from the image. Also copied portion can be rotated or flipped when it is forged. So for detecting the copy-move forgery we need a robust detection method which ensures the correct detection even if the image is noised, compressed, blurred, scaled, rotated, flipped, etc.

For detecting copy-move forgery a number of methods have been proposed already. Most of the methods use square block or sub-block or circular block extraction through some feature using Discrete Cosine Transformation (DCT) [1], Principle Component Analysis (PCA) [2], [3], Single Value Decomposition (SVD) [4], Scale Invariant Features Transform (SIFT) [5], Local Binary Pattern (LBP) [6] etc. and then finding the match in different ways using a sorting process like lexicographical sorting [2], [4], k-d tree sorting [5], radix sorting [7] etc. J. Fridrich et al. [1] suggested one of the earliest methods which was overlapping square block extraction and using Discrete Cosine Transformation (DCT) co-efficient feature extraction process is done. Too much false matching are shown and for flat region this method does not perform well. Popescu et al. [2] proposed another way using block matching approach and for feature extraction method they suggested Principal Component Analysis (PCA). This method solves the previous problem by reducing feature vector but detects an approximate match with additive noise up to 30dB and JPEG image compression factor up to 65, not possible for rotation scaling or flipping. Li et al. [6] tried to reduce the dimension of the feature by using Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). Although the authors claim high accuracy in the presence of compression (JPEG), but proper robustness against scaling and rotation was not found. Babak Mahidan et al. [8] described a method which is based on blur moment invariants when blur degradation, additional noise, or arbitrary contrast changes are present in the duplicated regions. But their methods did not consider the rotating, flipping or scaling. Nattapol Chaitawittanun [9] suggested a clustering method which only works for JPEG, BMP and TIFF typed image. Here other terms like rotation, flipping or scaling were not considered yet.

Another type of approach is sub-block extraction. Different types of sub-block methods have been proposed for feature extraction which are comparatively faster than the others. Using RGB value and sub-block Luo et al. [10] proposed a seven feature extraction method which works only for color images. Lin et al. [7] proposed sub block method extracting nine features which work only for JPEG compression, noise and some fixed angles of 90, 180 and 270 degrees. Vivek Kumar Singh and R.C. Tripathi [11] proposed another method of sub-block and Discrete Wavelet Transform (DWT) which extracts nine features. But these have limitations for rotation, scaling, JPEG compression etc.

For getting the rotation invariant or scale invariant feature some methods use rotation Local Binary Pattern (LBP) [6] or Scale Invariant Feature Transform (SIFT) [12]. Hailing Huang et al. [5] proposed SIFT which focused on scale invariant feature. But for low SNR and small type of image they give very poor results. Besides Mohamadian Zahra [13] proposed a method using SIFT features and then using Zernik moments. His method works for rotation as well as flat regions, but failed to scale changing. Leida Li et al. [6] used LBP focusing on rotation invariant feature. But it cannot detect the forged segment if it is rotated by geometric random angles. Some methods also introduce circular block extraction for getting rotation invariant features. Junwen Wang et al. [14] used Gaussian Pyramid Decomposition and circular block extraction for rotation invariant features. But this gives poor performance for scale invariant features. Sergio Bravo-Solorio et al. [15] proposed a log-polar representation of a block of pixels which are summed along its angle axis, to get a 1-D descriptor invariant to reflection and rotation. But this method failed to detect in case of blurring, JPEG compression or noise. Sevinc Bayram et al. [16] claimed to use the notion of counting bloom filters as an alternative to lexicographic sorting for improving the computational complexity whereas showing poor result for additive noise or blurring.

Some method focused only particular side such as Weihai Li et al. [17] proposed a method using DCT Grid and BAG (Block Artifact Grid) which works only for JPEG images and it is robust for JPEG Compression. The method works even when the copied area does not belong to the same image. Shuiming Ye et al. [18] also proposed a method using DCT co-efficient and Blocking Artifact Measure (BAM) which works only for JPEG compression. On the

other hand M. Sridevi et al. [19] proposed a parallel method using JAVA thread where overlapping blocks and lexicographical sorting are done simultaneously.
Finally, at the matching step, each method uses some sorting process like lexicographical sorting [2], [4], k-d tree sorting [5], radix sorting [7] etc. for finding the match between two blocks. But finding a match may lead to false results if the matched block is not found in the neighborhood block. So the overall approach for detecting the forged image is to block feature extraction and sort the features of the block and figure out the duplicate regions. Each of the methods shows some weaknesses which can be illustrated by the comparative analysis of the methods in some survey papers [20]–[24].
In this paper, we depict a copy-move forgery detection method using mean-contrast information of the circular block of the image which is robust especially against blurring, compression and noise. As circular block has been considered so we get a rotation invariant feature which ensures the correct detection result in any angles. Besides our comparison of the block features is up to n-th sorted block in the neighborhood, as a result our extracted features are robust even if with low quality JPEG factor as well as blurring. Promising results have been found by our originated method even if the forged segment is rotated in any angles $(0 - 360\,^{\circ})$, flipped, compressed, noised or blurred.

II. Proposed Method

In copy-move forgery detection process, there are some challenging situations. Before pasting the copied segment, some additional layer can be added in the forged image which makes the image hard enough to detect. For these additional adulterations, copy-move forgery detection method faces a lot of troubles in getting the accurate result. The forged image may be noisy. In that case the detection method will not get proper pixel information. When we will try to compare the region, we will get some wrong information from the pixel because already the actual pixel value is adulterated. If the image is compressed after forged, then image information starts to loose with the change of quality factor gradually. As a result, we will not get enough information. It may happen that image has some flat or uniform region such as blue sky or river. In that case flat region may lead to false positive results. The copied and pasted segment may not be exactly the same as always. Sometimes using the retouching tools the pasted segment is slightly changed. In that case it is very difficult to get the similarity which causes difficulty in detecting the forged image. Before forged if the copied segment is scaled, then the original block will not be the same like forged. If the pasted segment is rotated before forged, then again the problem arises just like scaling. In that case when we will try to find out match, two block will not produce the same orientation. A similar problem like rotation can be observed in case of flipping. Another problem is, when we try to find out the match in the sorted block, the desired block may not be found in the neighbor block due to the compression, blurring, noise or any other retouching processing. In that case we need to look for the matched block in the neighborhood instead of only neighbor block.
The steps of our proposed method for detecting the copy-move forgery are illustrated in Figure 2. Our method is very simple but robust against different kinds of challenges. We go for each of the overlapping circular block and extract our desired reduced features following the proposed method. Finally, by sorting the feature vectors and finding the match in the neighborhood, we figure out the similarity of the duplicated regions.

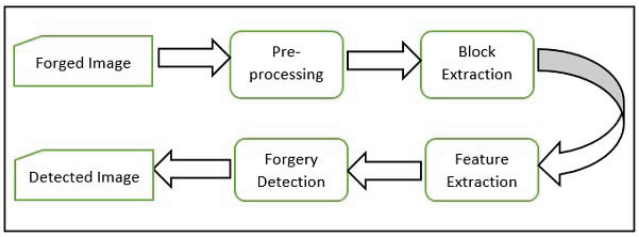

Fig. 2: Steps of copy-move forgery detection.

A. Pre-processing

For our detection method we need a gray scale image. So if we have any colored image, then we have to convert it into a gray scale image because the feature selection is totally texture base. For that conversion we can just follow the RGB image to gray scale conversion formula as follows.

$$I = 0.299R + 0.587G + 0.114B \tag{1}$$

It may happen that image is suffering from some kind of random noise. In that case, the Gaussian noise reduction process can be used for smoothing the image which removes the noise from the image as well as produces a smoother image.

B. Block Extraction

After completing with preprocessing, the circular overlapping block features are extracted for getting the rotation invariant features. As an overlapping block is taken so we will get all combinations of pixels which keeps all the segments under consideration. At first, the input image is divided into overlapping square blocks of $b \times b$ pixels. Each block contains three concentric circles which have a different radius (Figure 3). In the Figure 3, how the circular blocks are extracted from the $b \times b$ pixel square block is illustrated, where the largest circle is named as *circle 1*, the smaller one as *circle 2* and the smallest one as *circle 3*. Here, the radii of the circles are smaller chronologically. Thus, if the image size is $m \times n$ then we have a total $(m-b+1) \times (n-b+1)$ square blocks in the whole image. From each block, these three concentric circles are estimated for picking up the features. Moreover, for considering the circular block, the maximum covered area pixel will be included. We did not use direct any interpolation method. We considered the pixel to the boundary if its maximum area is covered by the circle. But any interpolation may also be used.

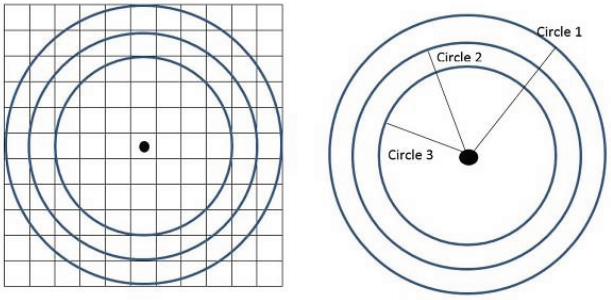

Fig. 3: Circular block extraction of image.

C. Feature Extraction

For an image of size $m \times n$, a total number of $(m - b + 1) \times (n - b + 1)$ square blocks is generated. Each block contains $b \times b$ pixel features which is not feasible for finding the forged portion of the image and also too large for sorting and comparison. So a reduced feature vector is needed for sorting and comparison. A reduced feature vector is developed in our proposed method. For each overlapping circular block B_i, a feature vector $V_i = (\mu_1, \mu_2, \mu_3, \sigma_1, \sigma_2, \sigma_3, \mu'_1, \mu'_2, \mu'_3, \sigma'_1, \sigma'_2, \sigma'_3)$ is computed and saved in an array. From each overlapping circular block, these 12 features will be calculated where feature vector V_i will be according to the following formulas.

$$\mu_i = \frac{\Sigma(I_k(x,y))^2}{N_k} \tag{2}$$

$$\sigma_i = \frac{\Sigma(I_k(x,y) - \mu_i)^2}{N_k * \mu_i} \tag{3}$$

$$\mu'_i = \frac{\mu_i}{\mu_1 + \mu_2 + \mu_3} \tag{4}$$

$$\sigma'_i = \frac{\sigma_i}{\sigma_1 + \sigma_2 + \sigma_3} \tag{5}$$

Where $i = 1, 2, 3$ represents the feature vector, k represents the concentric circles (Figure 3) and (x, y) represents the pixel position of the block. From each concentric circular block, mean and contrast information of the image segment are calculated which are totally rotation invariant features. Here μ, I, N represent the mean, contrast, intensity and number of pixels respectively. If our forged object is rotated before pasted then we will not get the same feature using square small block. But if we use circular block we can unlock this problem. That's why we are using circular block instead of square block. Since a circular block is considered so for any copied segment even if it is rotated the features will be same as like without rotation. That's why the proposed method is robust against any angles $(0 - 360\,^\circ)$ as well as flipping also. Besides, the consideration of three concentric circular blocks gives us the ratio features among them, which ensures more robustness in the detection process.

D. Forgery Detection

After getting all feature vectors for each block we get the final value of a two dimensional array where each row is representing each block and its features. Before making comparison, this two dimensional array needs to be sorted so that similarity can be found with less comparison. Because the similar blocks according to features will appear in the neighborhood. Each row will be lexicographically sorted using Radix Sort [6] method. For finding out the similarity between two blocks each block is compared with up to n-th consecutive blocks in the sorted rows. For information loss or some post-processing it may happen that desired similar block has just gone far from the immediate

position. So we are going for up to n-th consecutive rows in the neighborhood. And as a result, it is more reliable that we will find out the proper matching. For finding the successful similarity, we also need to consider some special criteria. For instance, two blocks are said to be matched, if they maintain a specific distance between them. Otherwise, they will be considered as uniform region. Again, if the distance between two blocks ensures that they are uniform or flat region, then they are discarded from the matched list. Euclidian distance can be calculated for distance measure (Equation (6)).

$$D(V_i, V_j) = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}. \quad (6)$$

We are doing this to avoid the uniform flat regions and to ensure that our copied region is keeping aloof for a minimum distance. If it is sure that they are not flat region, then we can go for the forged portion size means the image block size, which will control the detection of our desired type forged image. It will assist us to avoid a lot of unnecessary false positive results. If we take very small blocks for detecting region, we have to go for a larger region for finding the forgery. But small block may also increase the false positive result as well. So it is better to use a medium size block. Apart from these, we also need to consider that how many close collected blocks will be considered as a forged area. If the collection of the blocks is very small, then we can discard them considering as a flat region. Finally, for feature matching, we are using the feature vector and get the similar rows from the two dimensional array which lead to duplicated regions. As we have taken the overlapping circular block features, and our feature vector is strong enough to fight against rotation so rotated forged portion can easily be detected. Moreover, using some morphological operation like erosion or dilation on the final output we can also improve our results.

III. Experimental Result and Performance Analysis

A. Experimental Setup and Data Set

In our experiments, the proposed copy-move forgery detection method has been implemented in Matlab 2010 and all the simulations are performed on a personal computer of 2.13 GHz processors with 2 GB main memory. All the test images are collected from a benchmark image dataset[1]. Several existing methods have also been implemented for comparative performance analysis and run for each image dataset. As there are several challenges in copy-move forgery like rotation, flipping, adding noise, JPEG compression, Gaussian blurring etc. so images have been selected in manner so that we can get images of copy-move forgery including different types of challenges. In our experiment, we have used the 3 concentric circular blocks which size were 11×11, 9×9, 7×7 respectively and the distance threshold was 35 pixels to consider a forged area. We have select these values empirically. Besides, for our experiment we have taken 10 images for each type of modification. Our first section of the dataset contains only forged images without any modification and their corresponding ground truth (actual output result). Flat region and different contour are considered here. Second section of the dataset contains noisy forged images and their corresponding ground truth. For checking the performance of noisy images, different additive Gaussian noise was added to Matlab program. Different noise ratios in decibel assure the performance checking of our method with different noise level. Third section of the dataset contains blurred images made by Matlab program. Blurring was done with different standard deviation and the window size was 5×5. As different standard deviations are used, so the performance of our method for different blurred level can be easily observed. The Fourth section of the dataset contains rotated and flipped images. Rotation was done for different angle values, including $0-360\,^{\circ}$. On the other hand flipping was done for both horizontal and vertical position. Our final and fifth section of the dataset contains compressed images with different JPEG quality factor. Quality factor controls the compression rate of the original image. For different JPEG quality factor, gradually the some of the image information will be lost. For all the types of the images, the performance of our detection method was observed with some of the existing methods to make a comparative analysis.

B. Performance Measurement

The performance has been measured by calculating Precision and Recall. Precision (also called Positive Predictive Value) is the fraction of retrieved instances that are relevant; while Recall (also called sensitivity)

[1]http://www5.cs.fau.de/research/data/image-manipulation/

is the fraction of relevant instances that are retrieved. High recall means that an algorithm returned most of the relevant results, while the high precision means that an algorithm returned substantially more relevant results than irrelevant. For classification tasks, the terms true positives T_p, true negatives T_n, false positives F_p, and false negatives F_n compare the results of the classifier under test with trusted external judgments. The terms positive and negative refer to the classifier's prediction (sometimes known as the expectation), and the terms true and false refer to whether that prediction corresponds to the external judgment (sometimes known as the observation). Besides Precision and Recall, F-measure value is also measured. The higher the F-measure is, the better the method performs. For our image dataset we have calculated the average Precision, Recall and F-measure values (Equations (7-9)).

$$Precision = \frac{T_p}{T_p + F_p} \tag{7}$$

$$Recall = \frac{T_p}{T_p + F_n} \tag{8}$$

$$F - measure = \frac{2}{1/Precision + 1/Recall} \tag{9}$$

C. Comparative Analysis

In this section, the output images of our detection method for each type of dataset will be shown and compared the result of our detection method with other methods [1], [2], [6], [7], [11] graphically. The proposed approach shows superior detection performance compared to conventional approaches. As for our experiment, image dataset is divided into five sections after considering different modification, so gradually each dataset image will be described with our proposed method's performance comparing to others.

1) Exact Copy-move Forgery: At first, the dataset images which contain no modification before forged are tested and the result of precision and recall are shown in the following diagram Figure 4. We have compared the results with some existing methods [1], [2], [6], [7], [11] as well as our proposed method also. Although the accuracy of the most of the methods is good enough, but our proposed method provides a little bit more accuracy than others method. The observation of output results is quite good compared with the ground truth. Almost all the output images are similar with ground truth. Because of our strong feature selection we can easily avoid the uniform region effect for the forged images, for example sky. Figure 5 illustrates one of the output results our proposed copy-move forgery detection method.

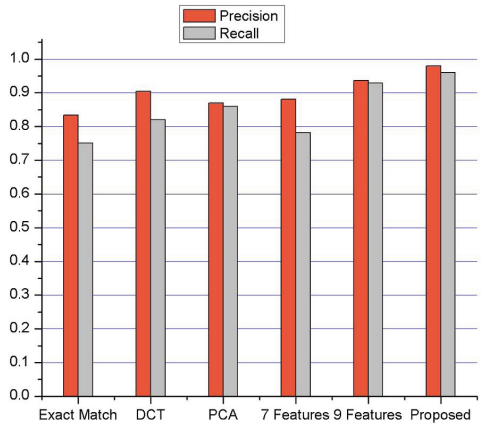

Fig. 4: Comparison with Exact match [1], DCT [1], PCA [2], 7 Features [10], 9 Features [7] and proposed copy-move forgery detection methods.

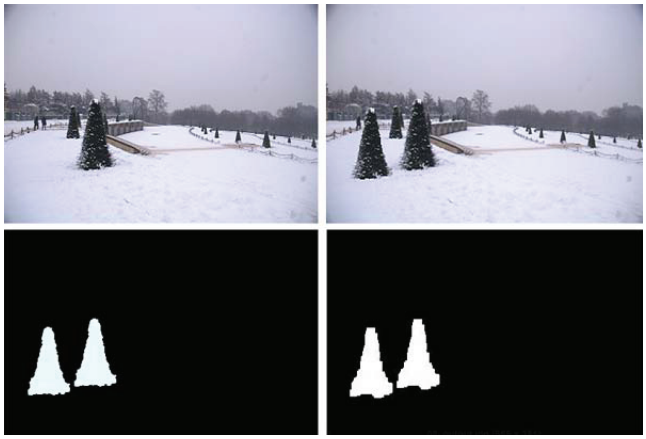

Fig. 5: Proposed method's performance for without any modification. From top left to right: original image, forged image; bottom left to right: ground truth, proposed method result.

2) Gaussian Noise: Our second dataset contains noisy images with different Signal to Noise Ratio (SNR) in dB. We know that when the SNR value is low, the image becomes noisier. After running the simulation, it is observed that our method successfully detects any copy-move forgery while the SNR is gradually decreasing. Figure 6 shows one of our output

Fig. 6: Proposed method's performance for Gaussian noise. From top left to right: original image, forged image, ground truth; bottom left to right: proposed method result with SNR = 40, 30, 20 respectively.

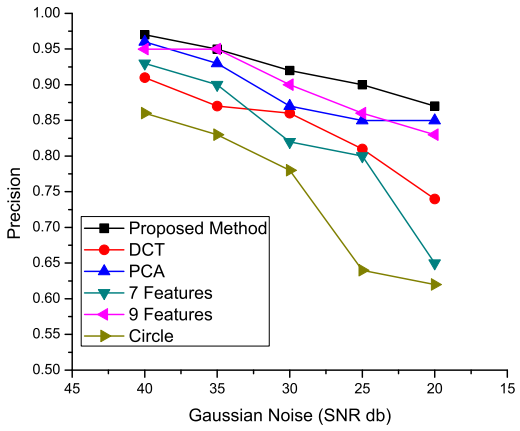

Fig. 7: Comparison of our detection method and DCT [1], PCA [2], 7 Features [10], 9 Features [7], circle [14] methods for noisy images (average precision).

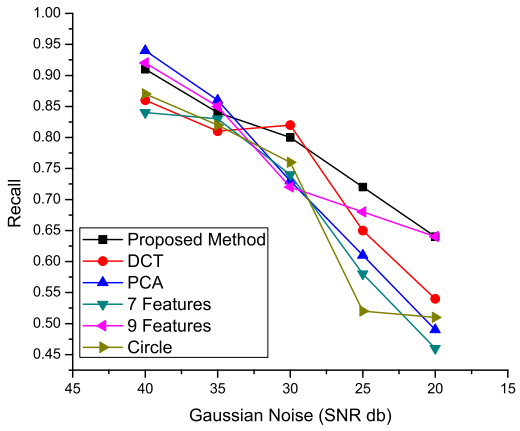

Fig. 8: Comparison of our detection method and DCT [1], PCA [2], 7 Features [10], 9 Features [7], circle [14] methods for noisy images (average recall).

results of our detection method with different SNR dB and the performance of our method can be visualized which is quite robust even if the SNR is 20. Finally, the average value of precision and recall is taken for comparing our method with others method. The following graphs Figure 7, 8 stand for the comparison of our detection method and some previous methods for Noisy images with different SNR dB. Compared to others, the proposed method is showing better performance continuously with different SNR values which leads that proposed method is quite strong with different Gaussian Noise levels.

3) Gaussian Blurring: Our third dataset contains blurred images with different Standard deviation (for our experiment window size is 5×5). If we increase the standard deviation, then the image will be more blur. Form the experiment, it is found that our proposed method almost correctly detects any copy-move

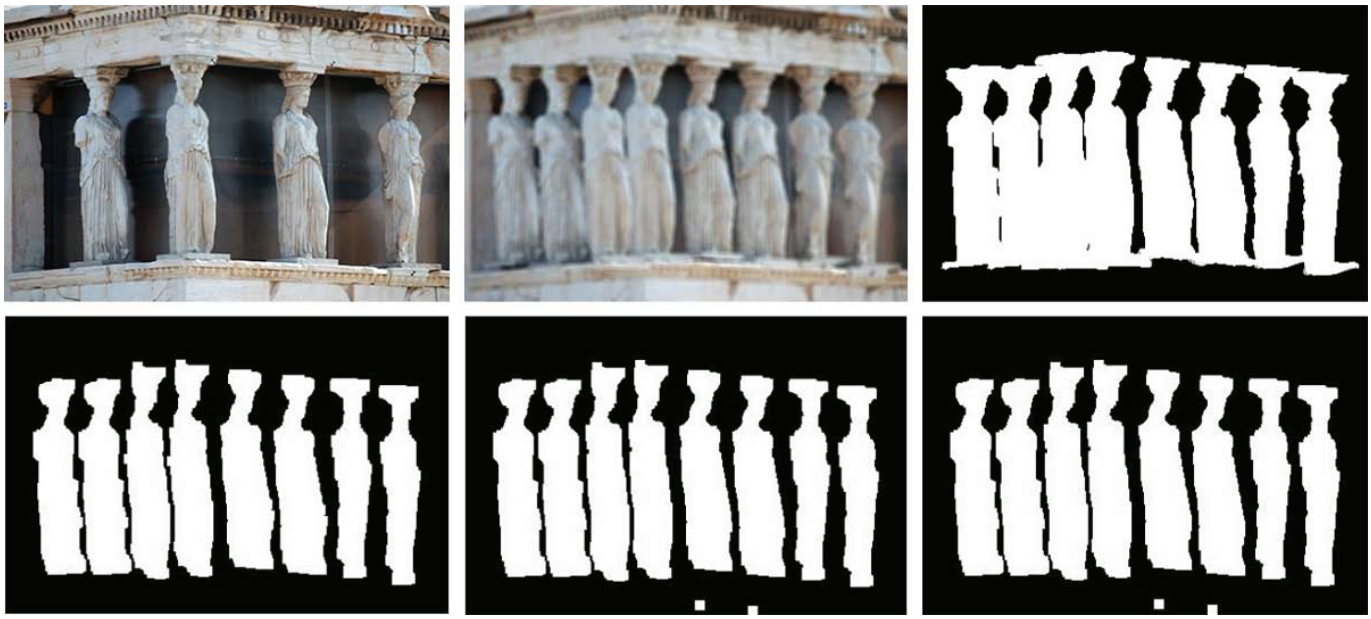

Fig. 9: Proposed method's performance for Gaussian blur. From top left to right: original image, forged image, ground truth; bottom left to right: proposed method result with standard deviation = 4, 5, 6 respectively.

forgery even if the standard deviation is less than 10 for 5×5 window. Figure 9 exemplify one of output results of our proposed method with different Standard deviation and shows that how robust our method is. Like the noise, this time Precision and Recall values of ours and others implemented methods are also evaluated for the image set to compare. The following graphs, shown in Figures 10 and 11, stand for the comparison of our detection method and previous methods for Blurred images with different Standard deviation. Maintaining different Standard deviation, different levels of blur are added and the performance is checked. It is found that the proposed method can detect the forged image easily in spite of high level blurring compared to others.

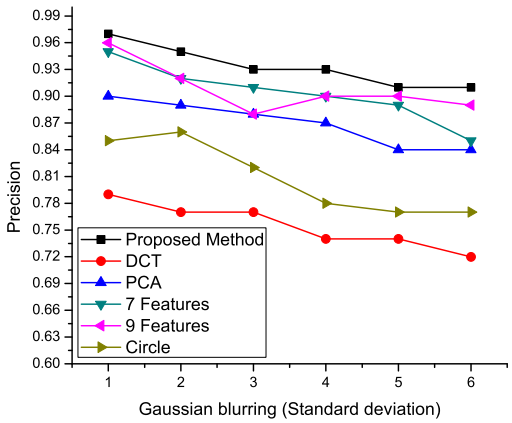

Fig. 10: Comparison of our detection method and DCT [1], PCA [2], 7 Features [10], 9 Features [7], circle [14] methods for blurred images (average precision).

4) Rotation and Flipping: Our forth dataset contains some rotated and flipped images. Rotation was done with different random angles ($0-360\,^{\circ}$) including 90, 180, 270 degrees for others. As our features are calculated from circular block, for any random rotation our method will work correctly. As image block can be moved by any angles in the case of rotation, some false positive results may arise especially if the image contains uniform regions. But still our features are robust enough to detect any copy-move forgery with any angle ($0-360\,^{\circ}$) rotation and flipping (Both horizontal and vertical) with an acceptable level of accuracy. Figure 12 illustrates one of our output results of the proposed method. As we have considered rotation invariant features in our method, so rotated or flipped copy-move forgery can be easily identified.

5) JPEG Compression: When an image is compressed, some of the image information will be lost. Actually, it depends on the quality factor of the compression. Using different quality factor we can control the image compression rate. If we decrease the quality factor gradually, we will get more compressed image

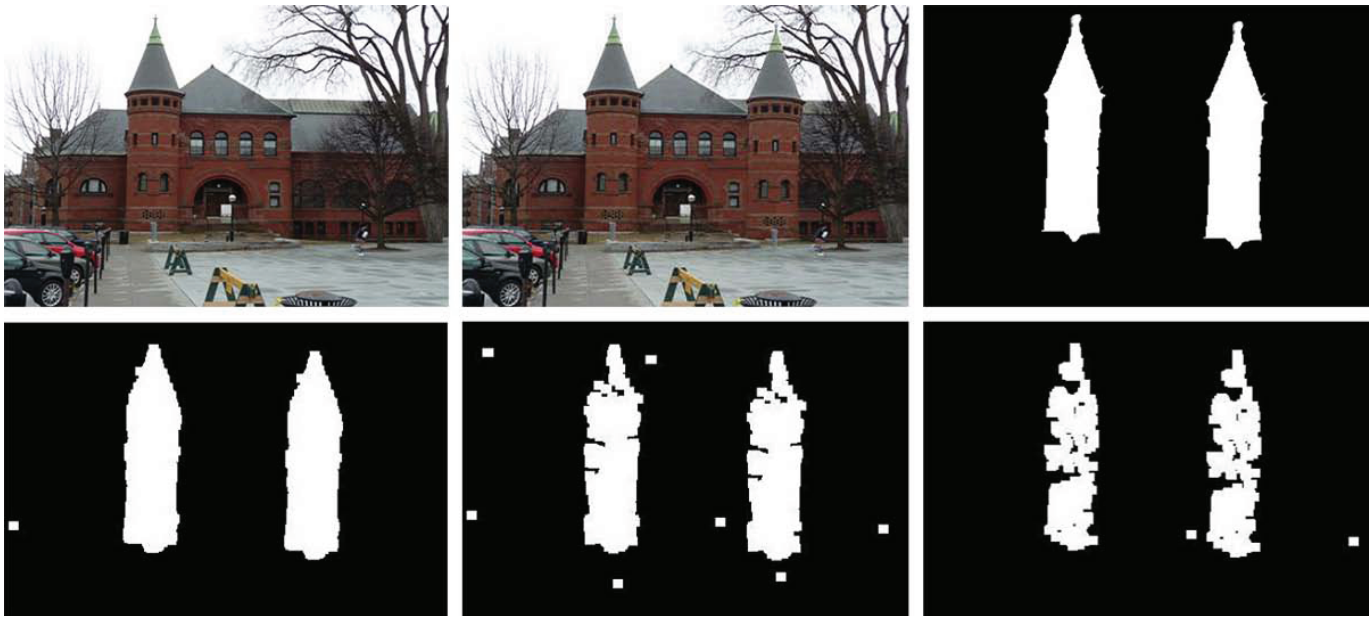

Fig. 13: Proposed method's performance for JPEG compression. From top left to right: original image, forged image, ground truth; bottom left to right: proposed method result with QF = 90, 70, 50 respectively.

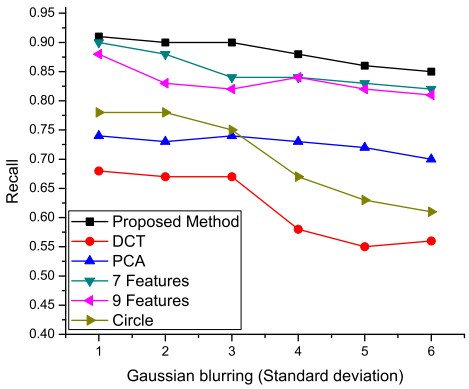

Fig. 11: Comparison of our detection method and DCT [1], PCA [2], 7 Features [10], 9 Features [7], circle [14] methods for blurred images (average recall).

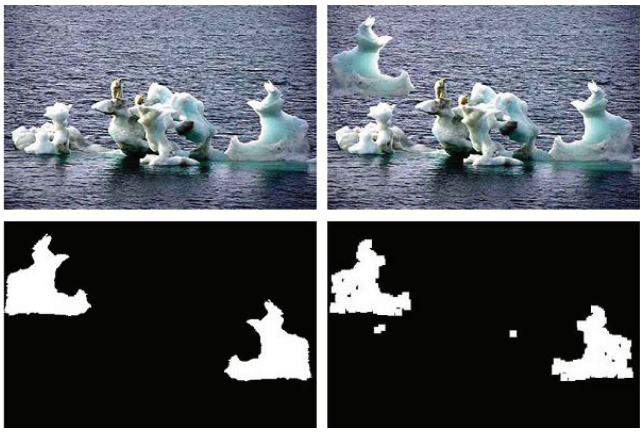

Fig. 12: Proposed method's performance for flipped image. From top left to right: original image, forged image; bottom left to right: ground truth, proposed method result.

and as a result we will lose more image information. And the detection of forged image will be tougher. The performance our proposed method is evaluated for different JPEG compression quality factors which is our fifth part of the dataset. Figure 13 illustrates the concepts of compression effect. Last three images provide the output result of our proposed method with JPEG compression quality factor 90, 70, 50 respectively. Besides, following graphs (Figure 14, 15) give us the view of the performance of our result with respect to precision and recall. We observed that up to quality factor 60 most of the methods are able to detect the forgery, but the accuracy is very less when quality factor goes under 60 and the performance of recall is highly less than the performance of precision. But our method is able to detect even if the quality factor is 40. The combination of our robust features and checking nth consecutive blocks of matching help to achieve this robust result against different JPEG quality factor.

Most of the cases the performance of our proposed

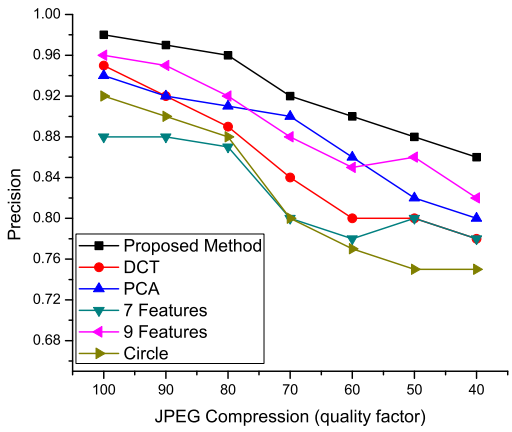

Fig. 14: Comparison of our detection method and DCT [1], PCA [2], 7 Features [10], 9 Features [7], circle [14] methods for different JPEG compression (average precision).

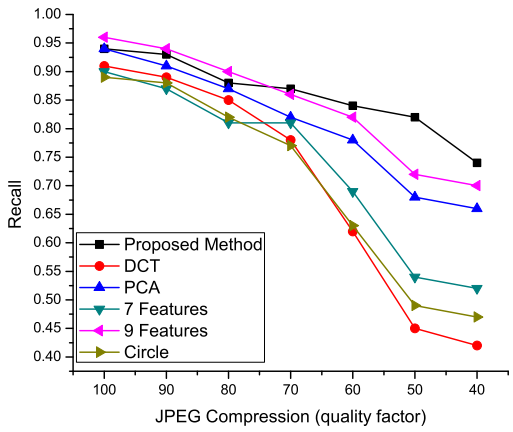

Fig. 15: Comparison of our detection method and DCT [1], PCA [2], 7 Features [10], 9 Features [7], circle [14] methods for different JPEG compression (average recall).

method is well enough. For example, in case of JPEG compression other methods are not able to detect if the quality factor is less than 50. But our method is able to detect even if the quality factor is 30 with an acceptable accuracy. In case of Gaussian blurring, for a window size of 5×5 and standard deviation of 1-10, our method is able to detect Copy-Move forgery with high accuracy where the other method's performance is quite poor. In case of noise, our method is also able to detect with Gaussian noise up to SNR dB 20 with a better performance compared to others. As we have considered circular block for feature extraction, our method is also able to detect if the copied region is rotated or flipped without calculating any complex calculation. Another thing is, instead of searching only consecutive block, we are looking for the similar block in the sorted neighborhood, which ensures better performance even after blurring or compression. Table 1 shows different Image dataset output result with average precision and recall value using all the sample images of ours for different n values. It can be observed that we would get better results if we search the matching for higher n value, but after a certain n value we will get almost constant results. Moreover, from the results of Figure 6, 9, 12, 13 it is obvious that we did not use any morphological operation on the output results. But if we do some morphological operation like erosion or dilation, some furnish results can easily be made avoiding the random false portion detection.

Table 1 shows different Image dataset output result with average precision and recall value as well as F-measure value using all the sample images of ours. For different SNR values of noisy images, different blurring level with standard deviation and image compression with different JPEG quality factor are considered for the image sets.

IV. Conclusion

The main challenge of copy-move forgery detection is to make it robust against any kinds of modification like compression, scaling, noise addition, rotation, flipping, etc. This paper describes a detection method for copy-move forgery which is simple and efficient in the alteration of JPEG compression, flipping, rotation for any angles, noise or blurring. The overlapping circular block approach ensures the rotation invariant feature and our proposed feature extraction ensure the robustness of our method even if high blur or low JPEG quality factor. In addition, the consideration of the comparison after sorting up to n-th consecutive blocks instead of comparing two consecutive blocks also leads the better accuracy in the case of JPEG compression and blurring. That's why our proposed method establishes better performance, especially with Gaussian noise, blur and compression. But it may lead some false positive results in case of rotation, if the image area is bested with flat or uniform region whereas

TABLE 1: Result of proposed method on different image dataset

Image Dataset	Proposed Method Result			
	Different Values of n	Average Precision	Average Recall	Average F-Measure
Noisy Image (SNR = 35)	2	0.97	0.76	0.85
	5	0.96	0.80	0.87
	10	0.96	0.90	0.92
	15	0.94	0.91	0.92
	20	0.93	0.91	0.92
Blurred Image (St. Deviation = 3)	2	0.97	0.70	0.81
	5	0.94	0.82	0.87
	10	0.93	0.89	0.90
	15	0.92	0.90	0.91
	20	0.90	0.90	0.90
Compressed Image (QF = 70)	2	0.97	0.76	0.85
	5	0.94	0.82	0.87
	10	0.92	0.88	0.90
	15	0.91	0.89	0.90
	20	0.90	0.87	0.88

the rotated forged image detection is successful. As there are almost same intensity container for a uniform or flat region, the matched area will be incorporated with some false areas. That's why, we may get some false results for some rotated images surrounded with flat or uniform region which is negligible. Moreover, our proposed method is not scale invariant. If the forged part of image is pasted with different scale in lieu of the actual size, then our method fails to detect the forged part accurately. So our future work is to decrease the false positive response for rotation in case of flat region and try to make it scale invariant detection method.

REFERENCES

[1] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," in *in Proceedings of Digital Forensic Research Workshop*. Citeseer, 2003.

[2] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," *Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515*, 2004.

[3] A. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," *Trans. Sig. Proc.*, vol. 53, no. 2, pp. 758–767, Feb. 2005. [Online]. Available: http://dx.doi.org/10.1109/TSP.2004.839932(410) 53

[4] G. Li, Q. Wu, D. Tu, and S. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on dwt and svd," in *Multimedia and Expo, 2007 IEEE International Conference on*, July 2007, pp. 1750–1753.

[5] H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using sift algorithm," in *Computational Intelligence and Industrial Application, 2008. PACIIA'08. Pacific-Asia Workshop on*, vol. 2. IEEE, 2008, pp. 272–276.

[6] L. Li, S. Li, H. Zhu, S.-C. Chu, J. F. Roddick, and J.-S. Pan, "An efficient scheme for detecting copy-move forged images by local binary patterns," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 1, pp. 46–56, 2013.

[7] H.-J. Lin, C.-W. Wang, Y.-T. Kao *et al.*, "Fast copy-move forgery detection," *WSEAS Transactions on Signal Processing*, vol. 5, no. 5, pp. 188–197, 2009.

[8] B. Mahdian and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants," *Forensic science international*, vol. 171, no. 2, pp. 180–189, 2007.

[9] N. Chaitawittanun, "Detection of copy-move forgery by clustering technique." *International Proceedings of Computer Science & Information Technology*, vol. 50, 2012.

[10] W. Luo, J. Huang, and G. Qiu, "Robust detection of region-duplication forgery in digital image," in *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on*, vol. 4. IEEE, 2006, pp. 746–749.

[11] V. K. Singh and R. 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.

[12] I. Amerini, M. Barni, R. Caldelli, and A. Costanzo, "Counter-forensics of sift-based copy-move detection by means of keypoint classification," *EURASIP Journal on Image and Video Processing*, vol. 2013, no. 1, 2013. [Online]. Available: http://dx.doi.org/10.1186/1687-5281-2013-18

[13] M. Zahra, "Image duplication forgery detection using two robust features," *Research Journal of Recent Sciences*, vol. 1, no. 12, pp. 1–6, 2012.

[14] J. Wang, G. Liu, H. Li, Y. Dai, and Z. Wang, "Detection of image region duplication forgery using model with circle block," in *Multimedia Information Networking and Security, 2009. MINES'09. International Conference on*, vol. 1. IEEE, 2009, pp. 25–29.

[15] S. Bravo-Solorio and A. K. Nandi, "Passive forensic method for detecting duplicated regions affected by reflection, rotation and scaling," in *European Signal Processing Conference*, 2009, pp. 824–828.

[16] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on*. IEEE, 2009, pp. 1053–1056.

[17] W. Li, Y. Yuan, and N. Yu, "Detecting copy-paste forgery of jpeg image via block artifact grid extraction," in *International Workshop on Local and Non-Local Approximation in Image Processing*, 2008.

[18] S. Ye, Q. Sun, and E.-C. Chang, "Detecting digital image forgeries by measuring inconsistencies of blocking artifact," in *Multimedia and Expo, 2007 IEEE International Conference on*. IEEE, 2007, pp. 12–15.

[19] M. Sridevi, C. Mala, and S. Sandeep, "Copy–move image forgery detection in a parallel environment," pp. 19–29, 2012.

[20] V. Christlein, C. Riess, and E. Angelopoulou, "A study on features for the detection of copy-move forgeries." in *Sicherheit*, vol. 2010, 2010, pp. 105–116.

[21] S. Kumar, S. P. Das, and S. Mukherjee, "Copy-move forgery detection in digital images: Progress and challenges." *International Journal on Computer Science & Engineering*, vol. 3, no. 2, pp. 653–663, 2011.

[22] V. Christlein, C. Riess, J. Jordan, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 6, pp. 1841–1854, 2012.

[23] S. Bayram, H. T. Sencar, and N. Memon, "A survey of copy-move forgery detection techniques," in *IEEE Western New York Image Processing Workshop*. Citeseer, 2008, pp. 538–542.

[24] B. Shivakumar and L. D. S. Santhosh Baboo, "Detecting copy-move forgery in digital images: a survey and analysis of current methods," *Global Journal of Computer Science and Technology*, vol. 10, no. 7, pp. 61–65, 2010.

Md Sirajus Salekin received his B.Sc. Engg. in Computer Science and Engineering degree from Islamic University of Technology (IUT), Bangladesh in 2013. Currently he is working as a lecturer in the Department of Computer Science and Engineering, Islamic University of Technology (IUT), Bangladesh and also pursuing his M.Sc. Engg. in Computer Science and Engineering at the same university. His research interests include image processing, computer vision, pattern recognition, machine learning and data mining.

Rafsanjany Kushol received his B.Sc. Engg. in Computer Science and Engineering degree from Islamic University of Technology (IUT), Bangladesh in 2013. Currently he is working as a lecturer in the Department of Computer Science and Engineering, Islamic University of Technology (IUT), Bangladesh and also pursuing his M.Sc. Engg. in Computer Science and Engineering at the same university. His research interests include image processing, graph theory and computer vision.

Md. Hasanul Kabir received his B.Sc. degree from Islamic University of Technology (IUT), Bangladesh and PhD degree in Computer Engineering from the Kyung Hee University, South Korea. Currently he is working as an associate professor in the Department of Computer Science and Engineering, Islamic University of Technology (IUT), Bangladesh. His research interests include feature extraction, motion estimation, image processing, computer vision and pattern recognition.