International Journal of Scientific and Technical Advancements

ISSN: 2454-1532

Transformation Based Parametric Analysis for Copy-Paste Tampering Detection

Kusam Sharma[1], Pawanesh Abrol[2]

[1, 2]Department of Computer Science & IT, University of Jammu, Jammu, J&K, India-180006

Email address: [1] kusamju@gmail.com , [2] pawanesh.abrol@gmail.com

Abstract— Copy-paste tampering is an important tampering method used in digital image manipulation. A wide range of techniques have been developed to detect and locate the tampered regions in a digital image. These copy-paste tampering detection techniques can be block-based or key-point based. Using image statistical parameters for detection of copy-paste tampering is also one of them. But, most of these methods generally fail to detect copied regions if the image or copied region is rotated before being pasted or after doing tampering in it or even if the image is resized to different dimensions after doing some manipulations in it. In this research work a non-overlapping block-based method has been proposed and analyzed. This method attempts to identify the impact of transformation on digital images having different types, formats and dimensions and to detect and locate the duplicated regions with rotation or resizing on the basis of selected parameters. Using some specific threshold values, the parameters of both the original and tampered image is computed, analyzed and compared with each other. The experimental results thus obtained signify that the suggested framework is capable in locating the duplicated areas and can work effectively for locating the copy-paste tampering of low to moderate nature. The effect of image rotation and resizing is also analyzed. The generated results can be used as the preliminary verification of the images for tampering and to improve the tampering detection process by locating most likely cases of possible image tampering. The suggested framework shows inefficiency while handling certain geometrical transformations.

Keywords—Block based tampering detection techniques; copy-paste tampering; non-overlapping block based techniques; overlapping block based techniques; resizing; rotation and transformation.

I. INTRODUCTION

Advancement in digital image processing technology may result into some heinous digital crimes. In order to prove the authenticity of a digital image during transmission is always a challenging task. The easy availability of several pre-existing and advanced image processing tools has slowed down the process of image security thus resulting in digital image tampering. The most common among the different types of digital image tampering is the copy-paste tampering. It is of two types copy-paste tampering in one image and digital splicing with different images. Copy-paste tampering in one image is a unique type of tampering in which a specific portion of the image is copied and pasted somewhere else in the same image with an intention to hide a particular object or information. As the copied segment comes from the same image its dynamic range, colour palette and many other important features will almost be alike to the rest of the image [1]. Many other post processes like edge smoothing, blurring and noise addition are later on used to remove the visible traces of tampering.

A large number of copy-paste tampering detection techniques are in existence now. SIFT, DCT, SURF, DWT, PCA, SVD, PAN's method, improved SVD, DWT-SVD, LPFT, DWT & PCA-EVD, FMT, LUO's method, etc are some of the renowned and widely accepted copy-paste tampering detection techniques. Out of these techniques, some are block-based and some are key-point based. In block based methods, the given image is segmented into either non-overlapping or overlapping segments or blocks. These detection methods can further be broadly classified into non-parametric or parametric methods. A large range of image parameters including statistical, textural and geometrical can be analysed using these non-overlapping block based parametric tampering detection methods. Analysis of statistical parameters of an image helps in detection of any kind of malicious modifications in it [2]. The qualitative and quantitative analysis of these parameters helps in determining and locating the tampered regions within an image [3]. These techniques can find their application in various fields of image enhancement, image restoration, image denoising, digital image tampering detection and edge detection and eye gazing [4]. These detection techniques are invariant to certain transformations like blurring, brightness changes etc.

Different statistical parameters can be used for detecting digital image forgeries like mean, standard deviation, variance, skewness, kurtosis, etc. Variance of an image is normally used to find how each pixel varies from the neighbouring pixel or centre pixel and is used to classify them into different regions. Certain sharp details like edges can easily be identified using variance [5]. Moreover, the shape parameters like kurtosis and skewness characterizes the tails of a probability model. Due to of which, any two probability models with same skewness, kurtosis, standard deviation and mean will have similar shapes [6-8].

The present research paper is focused on developing a parametric non-overlapping block based tampering detection model for detecting copy-paste tampering within an image and to analyze the behaviour of these statistical parameters after their implementation onto a wide range of digital images being transformed i.e. rotated at different degrees i.e. 0^o, 90^o, 180^o and 270^o and resized to three different dimensions of 10, 50 and 100 having different types, formats and dimensions. The proper utilization of these statistical parameters in accordance

Kusam Sharma and Pawanesh Abrol, "Transformation based parametric analysis for copy-paste tampering detection," *International Journal of Scientific and Technical Advancements*, Volume 2, Issue 1, pp. 247-254, 2016.

with transformations and different image types, formats and dimensions generally help in optimizing various image processing techniques especially in the area of image tampering detection. In this research work, the behaviour of three statistical parameters i.e. variance, skewness and kurtosis is observed and analysed for further tampering detection. The proposed method is robust not only to rotation, but also to resizing.

The organization of this paper is as follows. Literature review and objectives are discussed in the next two subsequent sections II and III. The proposed statistical model showing the impact of transformations on non-overlapping block-based parametric model for copy-paste tampering detection is presented in section IV followed by experimental results and discussion in section V. In section VI, inferences and conclusion is discussed and section VII presents limitations and future work.

II. Literature Review

Copy-move tampering is a type of context based tampering which can be detected by using either block-based or key-point based techniques. Some of the renowned and widely accepted copy-paste tampering detection techniques are discussed below:

An efficient method based on key-point and feature computation algorithm known as Scale Invariant Feature Transform (SIFT) has been proposed in [9]. In this method, initially the key-points of an image will be located and their corresponding image features will be collected. Another novel passive-blind detection method based on block matching procedures is suggested in [10]. In this improved singular value decomposition (improved SVD) is applied to all the image blocks. Li et al. proposed an SVD based sorted neighborhood approach for detection by applying DWT (Discrete Wavelet Transform) for decomposing an image into four sub-bands [11]. Another camera-based non-intrusive method for copy-move tampering detection is based on image segmentation and a new denoising algorithm in which prior knowledge about the camera used to capture the image is not required [12]. Another FMT based method used to extract image features from image blocks to reduce the detection time by using Counting Bloom Filters instead of lexicographical sorting is suggested in [13].

The other type of tampering detection techniques for copy-move tampering detection involves block-based techniques which are further classified into non-overlapping and overlapping based techniques. Some of the renowned and recently developed overlapping and non-overlapping based tampering detection techniques are discussed below:

A method using radix sort as an alternative to lexicographic sorting is used for sorting the feature vectors is proposed by Lin et al. In order to obtain the final results, the medium filtering and connected component analysis are performed on the tentative detected results. This method fails to detect all copied regions of small size. This scheme performs well when the degree of rotation is 90^o, 180^o and 270^o [14]. Another method for detecting copy-move attacks based on DCT and DWT is proposed by Wang et al. In this method, DCT and DWT are applied to each block to extract features and then compare the statistical parameters of each block to detect duplicated regions. [15]. Another efficient and improved DCT based method for detection of copy-paste tampering is given by Huang et al [16]. This method works efficiently even in the presence of JPEG compression, additive white Gaussian noise and blurring. Muhammad et al. suggested a new two-phase detection method for locating image forgeries based on inconsistency of noise levels in different regions of the image [17]. In this method, an effective noise estimation method is used for initial noise estimation of non-overlapping image blocks. The kurtosis of the original natural image and the variance of the added noise are computed for tampering detection. This method detects image forgeries both quantitatively and qualitatively. Another segmentation method based on inconsistencies of noise for detecting digital image tampering is given by Mahdian et al [18]. In this method, Additive White Gaussian Noise is considered and the noise standard deviation of each block is estimated using median-based method. The main disadvantage is that authentic images may contain several isolated regions with totally different variances. It is hard to find the tampered regions when the noise degradation is very small of the rate of ðr < 2Þ.

Certain widely accepted, latest and authenticated parametric and non-parametric copy-move forgery detection approaches include a technique in which duplicated regions are detected by first applying a Principal Component Analysis (PCA) on small fixed-size image blocks to get a reduced dimension DCT block representation is given by Popescu et al. [19]. An image authentication method for gray and coloured images having different dimensions and formats for hybridization of colour histogram is is given by Dattatherya et al. In this method the first four statistical moments i.e. mean, standard deviation, skewness and kurtosis are considered to achieve the objectives of low cost and high speed [6]. An efficient technique which works by applying DWT (Discrete Wavelet Transform) to the input image to get a reduced dimension representation is given by Zhang et al. [20]. A localization approach for detection of image edge for the most common blur operations of composite forged image is proposed [21]. This technique accurately detects the blur operation traces of composite forged images. Huang et al. presented an automatic duplication region detection algorithm based on improved DCT [22]. This method works well in the complete absence of digital watermarks and can detect the duplicated regions even when an image is distorted by additive white Gaussian noise, JPEG compression or blurring.

Liu et al. proposed another efficient and robust detection method which uses circle block and Hu moments to detect and locate the duplicated regions with rotation [23]. Another improved algorithm based on the Fourier-Mellin which is robust to duplicated regions of large rotation angle in comparison to other existing algorithms which can only treat slight rotation is suggested by Li and Yu [24]. A SIFT based efficient method proposed by Shaikh et al. detects if copy-move tampering has occurred and also to estimate the parameters of the transformation used. This technique is effective in composite processing & multiple cloning. Moreover, this technique is able to detect the altered areas & geometric transformation parameters [25].

A wide range of copy-paste tampering detection techniques are in existence and can be classified on the basis of their domain of working. Block-based copy-paste tampering detection techniques include non-overlapping and overlapping techniques. In non-overlapping, there are several parametric and non-parametric techniques for tampering detection. Parametric techniques are efficient in detecting copy-paste tampering. In this proposed research, a parametric non-overlapping block-based copy-paste tampering detection technique is developed. The objectives of the present research study are discussed in the next section.

III. Objectives

From literature review, it is clear that the analysis of statistical parameters of an image sometimes point out certain significant features of image tampering within an image being rotated to different degrees and resized to different dimensions. Moreover, parametric image analysis based on non-overlapping block-based method is one of the important methods used for analysis of an image. On the basis of above interpretations, this research study has been carried out with the following objectives:

- Study of digital image tampering detection algorithms.
- Understanding copy-paste tampering detection algorithms along with those based on rotation and resizing of the original image and recognition of important statistical parameters.
- Developing a statistical parameter based non-overlapping block-based model for detecting rotation and resizing based copy-paste tampering within the same image for parametric analysis.
- Implementation of the proposed parametric model onto a wide range of images being rotated to different degrees and resized to different dimensions.
- To observe the impact of rotation and resizing on the proposed parametric model.

The methodology of the proposed non-overlapping block-based parametric tampering detection model for detecting copy-paste tampering within an image being rotated to different degrees and resized to different dimensions is discussed in the next section.

IV. Methodology

In order to perform transformation based feature analysis for detecting copy-paste tampering, a parametric tampering detection model using non-overlapping block-based technique has been proposed. The schematic block diagram of proposed non-overlapping block based statistical model for copy-paste tampering detection for images rotated at different degrees and resized to different dimensions is presented in figure 1.

At first, an original test image (*I_{OT})* of any type, format and dimension is taken and normalized and is then divided into non-overlapping blocks of size [m x m]. After blocking of an image, the three statistical parameters variance (*v*), skewness (*S_k*) and kurtosis (*K*) of the original image are computed. On the other side, the same original image (*I_{OT})* is tampered using copy-paste tampering thus resulting into a tampered image (*I_{FT}*). The *I_{FT}* is then either rotated at different degrees i.e. 0°, 90°, 180° and 270° or resized to different dimensions i.e. 10, 50 and 100. After rotation or resizing, *I_{FT}* is divided into non-overlapping blocks of size [m x m] and its variance (*v*), skewness (*S_k*) and kurtosis (*K*) are again computed. The corresponding values of all the parameters under study for each block of *I_{OT}* are analysed and compared with those of *I_{FT}* for further tampering detection.

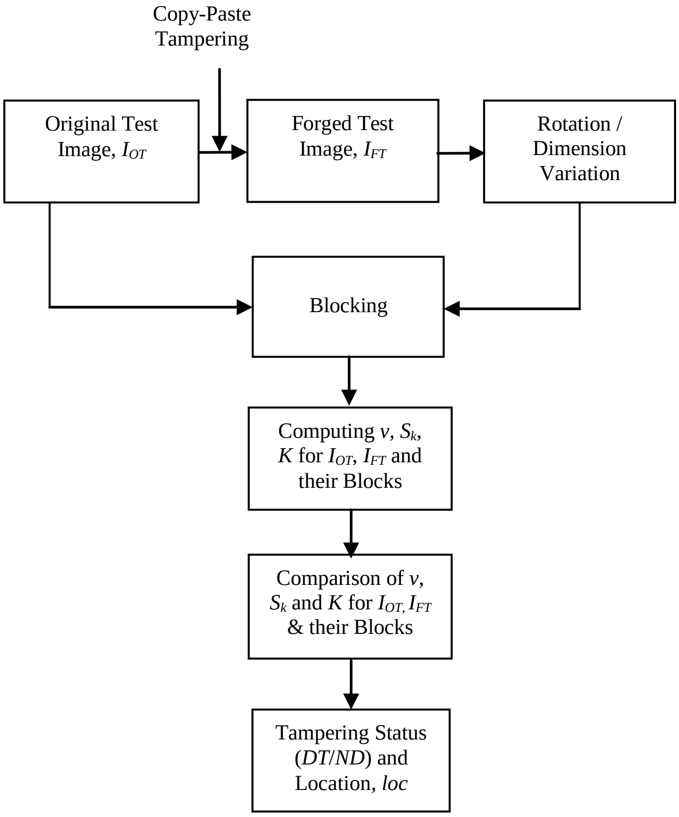
Copy-Paste Tampering
Original Test Image, I_{OT}
Forged Test Image, I_{FT}
Rotation / Dimension Variation
Blocking
Computing v, S_k, K for I_{OT}, I_{FT} and their Blocks
Comparison of v, S_k and K for $I_{OT,}$ I_{FT} & their Blocks
Tampering Status (*DT*/*ND*) and Location, *loc*

Fig. 1. Schematic block diagram of proposed non-overlapping block-based statistical model for copy-paste tampering detection for images rotated at different degrees and resized to different dimensions.

In both the cases of transformation, the statistical variation $\partial_p = |P_{IO} - P_{IF}|$ is computed and analyzed for all selected parameters for ascertaining the tampering and its extent. The permissible proportion of variation in the parameter under study is given by the threshold *t*. After testing a large domain of images and analyzing the behavior of above said parameters, the value *l* of threshold *t* is set. On the basis of variations observed, the tampering status *DT* (detected) or *ND* (not detected) is established. Moreover, the particular tampered location; i can be located by further analyzing the behavior of these statistical parameters and the model.

The suggested interface for rotation and resizing based tampering detection is tested for more than 600 images having different types, dimensions and formats and is developed in MATLAB version 7.6.0.324 (R2008a). The experimental results thus obtained for both the cases of transformation i.e. rotation and resizing are further analysed and discussed in the next section.

V. Results And Discussions

The results thus obtained for transformation based parametric analysis for copy-paste tampering detection are analysed after the implementation of the suggested non-overlapping block-based parametric model onto a wide range of images being rotated at different degrees and resized to different dimensions. A selected case out of tested 600 cases showing significant statistical difference in its parameters of both original and tampered gray scale images rotated at different degrees thus depicting copy-paste tampering detection based on threshold *t* for selected block size, S=32 is shown in table I.

The parametric difference ∂ is computed for all the parameters of original and tampered images along with their corresponding blocks. The difference in variance, skewness and kurtosis of original and forged image is given by ∂_v, ∂_{Sk} and ∂_K respectively.

TABLE I. Block-wise parametric differences of original and tampered image rotated at different degrees depicting copy-paste tampering detection based on threshold *t*, (*t*>=*l*) for selected Block Size, S=32.

Rotation						
Test image I_T	**Rotation at**	**Image blocks**	**Parametric variation (*t*>=*l*)**			**Tampering status & location, *loc***
			t_1=10	**t_2=0.05**	**t_3=0.5**	
			∂_v	∂_{Sk}	∂_K	
I_{T1} (Rect)	**0°**	**B_1**	11.00	0.04	0.13	**DT (B_1, B_2, B_3, B_4)**
		B_2	14.00	0.11	1.07	
		B_3	11.00	0.94	3.14	
		B_4	14.00	0.04	0.18	
		I_{T1}	3.00	0.21	0.62	
	90°	**B_1**	11.00	0.04	0.13	**DT (B_1, B_2, B_3, B_4)**
		B_2	58.00	0.32	1.16	
		B_3	55.00	0.74	3.04	
		B_4	14.00	0.04	0.18	
		I_{T1}	3.00	0.21	0.62	
	180°	**B_1**	55.00	0.75	2.38	**DT (B_1, B_2, B_3, B_4)**
		B_2	58.00	0.26	0.32	
		B_3	55.00	1.49	4.87	
		B_4	58.00	0.29	0.69	
		I_{T1}	3.00	0.21	0.62	
	270°	**B_1**	55.00	0.75	2.38	**DT (B_1, B_2, B_3, B_4)**
		B_2	14.00	0.87	2.89	
		B_3	11.00	0.88	2.29	
		B_4	58.00	0.29	0.69	
		I_{T1}	3.00	0.21	0.62	

Moreover, for each statistical parameter, the value *l* of threshold *t* is set after testing a large domain of images and analysing the behaviour of these parameters. On the basis of variations observed, the tampering status is recognized. The value of t_1 for ∂_v, t_2 for ∂_{Sk} and t_3 for ∂_K is set to 10, 0.05 and 0.5 respectively. The image I_{T1} rotated at 0°, 90°, 180° and 270° shows least variation for S_k and k and maximum variation for *v*. The overall statistical variation for all the three parameters for image I_{T1} is similar even if the image is rotated at different degrees. Further in Table I, blocks B_1, B_2, B_3 and B_4 of test image I_{T1} rotated at 0°, 90°, 180° and 270° show significant statistical variation in all the three parameters thus confirming the existence of tampering in all the four blocks. The statistical difference in variance is similar for blocks B_1, B_3 and B_2, B_4 when the image is rotated at 0° and 180°. The statistical variation in skewness is similar for blocks B_1 and B_4 when the image is rotated at 0° and 90°.

The ∂_{Sk} of all the images except I_{T1} are greater than 1.0 thus signifying that the ∂_{Sk} is substantial and the distribution is far from symmetrical. Also, it is deduced from the results generated above that the ∂_k of the image I_{T1} rotated at different degrees and for all its blocks is greater than 0. This positive kurtosis image I_{T1} would have a fairly uniform distribution of gray levels.

Figure 2 depicts the relationship of three statistical parameters ∂_v, ∂_{Sk} and ∂_K for original and tampered image I_{T1} rotated at 0°, 90°, 180° and 270°. Tampering can be observed in all the cases. Also, maximum variation is seen in ∂_v and least variation in ∂_{Sk} for test image $I_{T1.}$ The statistical variation in ∂_v is noticeable for all the four cases when the image is rotated to different degrees. The statistical variation in ∂_{Sk} is relatively very small as compared to ∂_v.

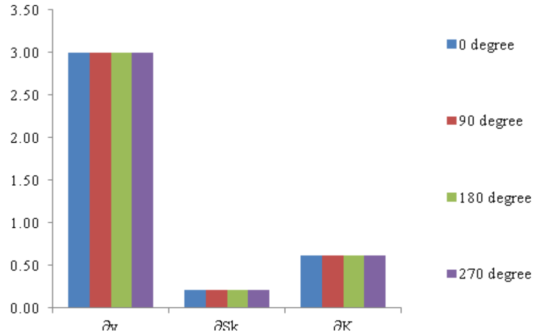

Fig. 2. Parametric variations in ∂_v, ∂_{Sk} and ∂_K for original and forged image I_{T1} rotated at 0°, 90°, 180°, 270° for selected block size S=32.

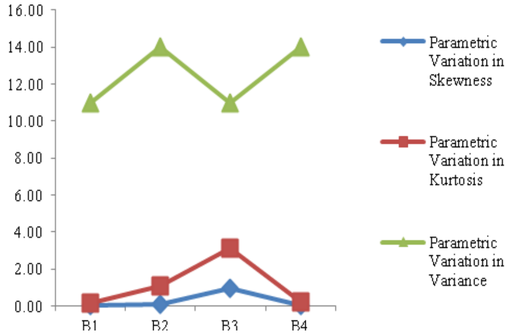

Fig. 3. Block-wise parametric variation in ∂_v, ∂_{Sk} and ∂_K for original and forged image I_{T1} rotated at 0°

Block-wise parametric variation among three parameters ∂_v, ∂_{Sk} and ∂_K is shown in Figure 3 for original and tampered image I_{T1} rotated at 0°. The statistical difference in variance is similar for blocks B_1, B_3 and B_2, B_4 when the image is rotated at 0°.

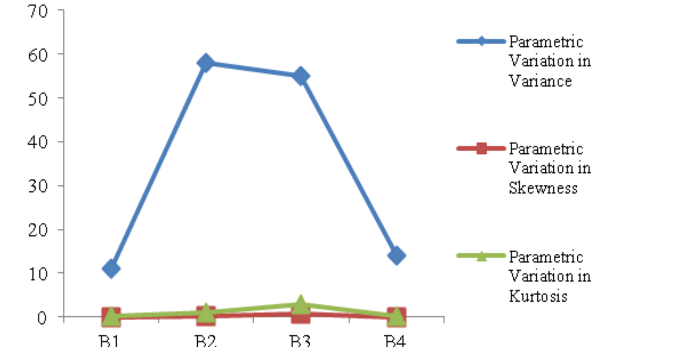

Fig. 4. Block-wise parametric variation in ∂_v, ∂_{Sk} and ∂_K for original and forged image I_{T1} rotated at 90°.

Variation in skewness, kurtosis and variance for original and tampered image I_{T1} rotated at 90° can be seen in figure 4. Moreover, ∂_v shows maximum variation than ∂_{Sk} and ∂_K.

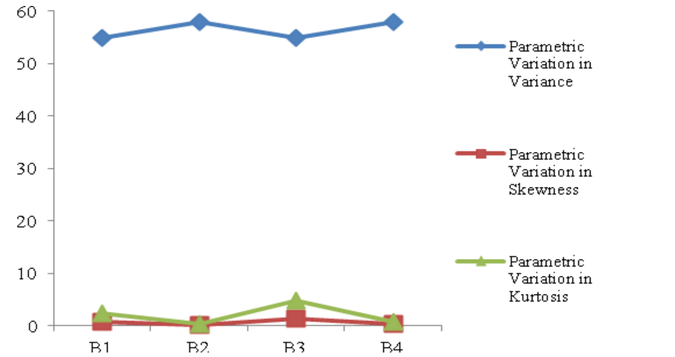

Fig. 5. Block-wise parametric variation in ∂_v, ∂_{Sk} and ∂_K for original and forged image I_{T1} rotated at 180°.

Similarly, figure 5 shows the relationship among three statistical parameters ∂_v, ∂_{Sk} and ∂_K for original and tampered image I_{T1} rotated at 180°. Also, maximum variation is seen in ∂_v and least variation in ∂_{Sk} and ∂_K.

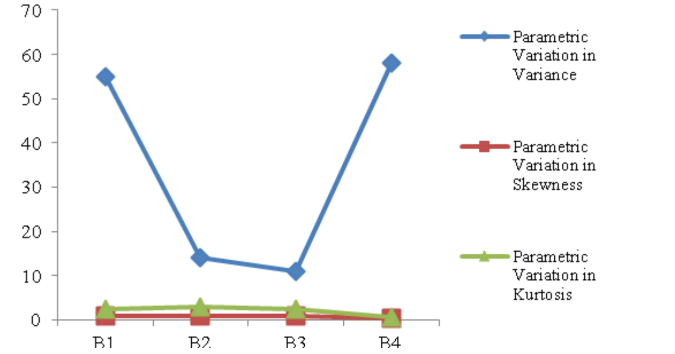

Fig. 6. Block-wise parametric variation in ∂_v, ∂_{Sk} and ∂_K for original and forged image I_{T1} rotated at 270°.

Variation in all the three parameters for original and tampered image I_{T1} rotated at 270° can be seen in Figure 6. The parameter ∂_v for block B_4 shows the maximum variation.

The Table II shows the block-wise parametric variation ∂_i along with corresponding threshold t_i for a selected image I_{T2} resized to three different dimensions of 10, 50 and 100. l for each parametric variation has been computed after testing a large domain of images. Any t_i less than corresponding l is considered as *ND* otherwise considered as *DT*. Further the table also shows the corresponding blocks of the image in three different dimensions in which tampering has been observed. Block B_3 of test image I_{T2} resized to three different dimensions shows significant variation in all the three parameters thus confirming the existence of tampering in it.

Table II. Block-wise parametric differences of original and tampered image resized to different dimensions depicting copy-paste tampering detection based on threshold t, (t>=l).

Resizing						
Test image I_T	**Resizing at**	**Image blocks**	**Parametric variation (t>=l)**			**Tampering status & location, *loc***
			t_1=2	**t_2=0.01**	**t_3=0.1**	
			∂_v	**∂_{sk}**	**∂_K**	
I_{T2} (Aahil)	**10**	**B_1**	0	0	0	**DT (B_3)**
		B_2	2	0	0.01	
		B_3	5	0.02	0.06	
		B_4	0	0	0	
		I_{T2}	6	0	0.01	
	50	**B_1**	0	0	0.01	**DT (B_3)**
		B_2	0	0	0	
		B_3	4	0.34	0.95	
		B_4	1	0	0	
		I_{T2}	4	0.71	1.87	
	100	**B_1**	0	0	0.01	**DT (B_3)**
		B_2	0	0	0	
		B_3	34	1.68	4.61	
		B_4	0	0	0	
		I_{T2}	10	3.08	8.1	

The blocks B_1, B_2 and B_4 of test image I_{T2} show no or insignificant statistical variation in any of its parameters thus depicting that no tampering has been done in these blocks.

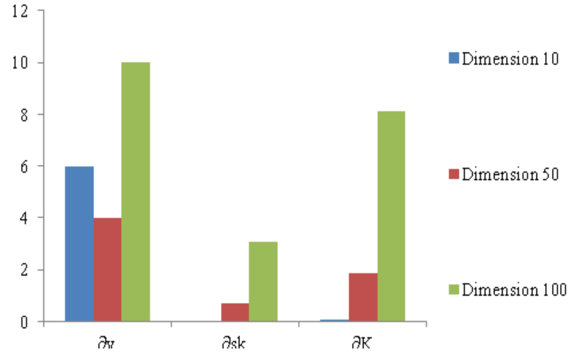

Fig. 7. Parametric variation in v, S_k and K of original and forged image I_{T2} resized to dimensions 10, 50, 100.

Figure 7 shows the relationship among three statistical parameters variance, skewness and kurtosis of original and tampered image I_{T2} resized to different dimensions of 10, 50 and 100. ∂_v shows maximum variation.

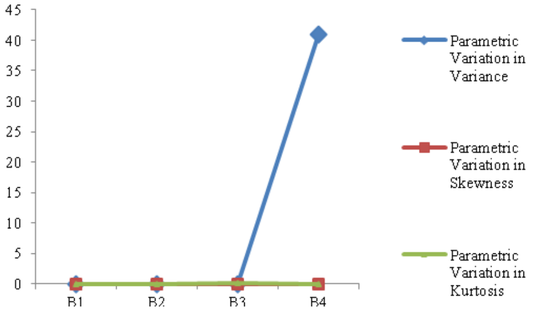

Fig.8 Block-wise parametric variation in *v*, S_k and *K* of original and forged image I_{T2} resized to dimension 10

The block-wise parametric variation in *v*, S_k and *K* of original and tampered image I_{T2} having resized dimension of 10 is shown in Figure 8. The variation in the statistical parameters of block B_3 shows tampering in it. The blocks B_1, B_2 and B_4 of test image I_{T2} show no or insignificant statistical variation in any of its parameters thus depicting that no tampering has been done in these blocks.

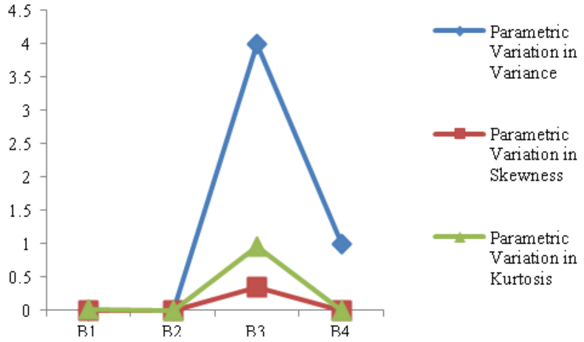

Fig. 9. Block-wise parametric variation in *v*, S_k and *K* of original and forged image I_{T2} resized to dimension 50.

Figure 9 shows the block-wise parametric variation in *v*, S_k and *K* of original and tampered image I_{T2} having resized dimension of 50. The block B_3 shows minimum variation for ∂_{Sk} whereas maximum variation for ∂_v.

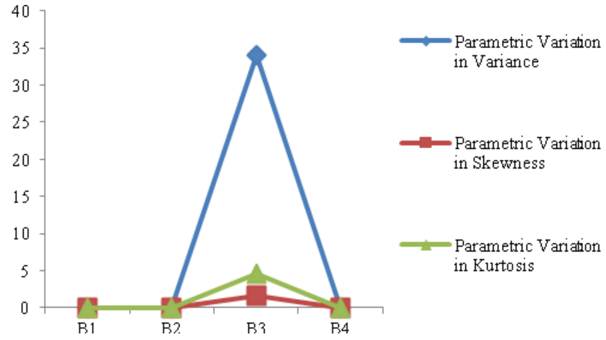

Fig. 10. Block-wise parametric variation in *v*, S_k and *K* of original and forged image I_{T2} resized to dimension 100.

Figure 10 shows the block-wise parametric variation in *v*, S_k and *K* of original and tampered image I_{T2} having resized dimension of 100. The block B_3 shows maximum variation for ∂_v and minimum variation for ∂_{Sk}.

The transformation based comparison of the parameters using non-overlapping block-based model for copy-paste tampering detection are presented in table III.

Table III. Performance based comparison for different parameters using non-overlapping block-based model for copy-paste tampering detection.

Performance based comparison for different parameters using non-overlapping block-based model for copy-paste tampering detection			
Transformation	**Statistical parameters**	**No. of tampered cases detected for rotation & resizing**	**Percentage**
Rotation	∂_v	8	**67**
	∂_{sk}	8	**67**
	∂_K	8	**67**
Resizing	∂_v	7	**70**
	∂_{sk}	4	**40**
	∂_K	5	**50**

As per the table, the overall percentage of all the selected statistical parameters of the detected tampered images out of the selected 12 images considered under rotation is 67% whereas the overall percentage of all the selected statistical parameters of the detected tampered images out of the selected 10 images considered under resizing is 53%.

The transformation based comparison of the statistical parameters is shown in Figure 11. It is observed that ∂_{Sk} shows minimum percentage of resizing based detected tampered cases whereas ∂_v shows maximum percentage of resizing based detected tampered cases. In rotation based cases, all the parameters are equally efficient and are showing the same percentage for detected tampered cases.

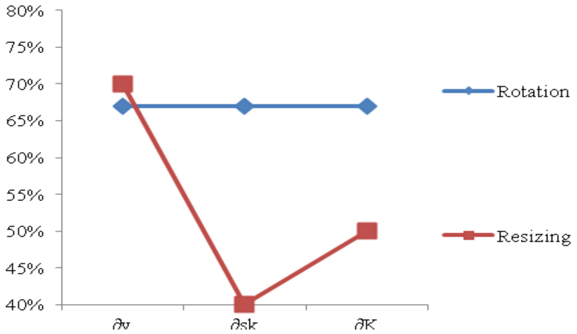

Fig. 11. Performance based comparison for different parameters under study (in %age).

During the process of detection of copy-paste tampering, it is very important to select and set the appropriate size of the smallest block of an image. For which several experiments have been conducted for block size and parameter selection. Larger size of image block increases computational complexity whereas smaller size causes too many false matches. Finally, in first case of transformation, block size

S=32 is selected and considered for further experimentation when the image is rotated at different degrees i.e. 0^o, 90^o, 180^o and 270^o. Whereas in the second case of transformation, after making several experiments and testing for different dimensions, the three different dimensions of 10, 50 and 100 are selected for image resizing. This experimental model is implemented on to a wide variety of images having different types, dimensions and formats, rotated to different degrees and resized to different dimensions. The experimental results thus obtained for both the cases of transformation are further shown, analyzed and discussed in this research paper.

The inferences and conclusion about the proposed experimental model are presented in the next section.

VI. Inferences and Conclusion

The proposed non-overlapping block based model for detection of copy-paste tampering within an image is based on analysis of statistical parameters. It is implemented on images having different types, formats and dimensions. Using this model, three parameters have been analysed using specific threshold values. These threshold values have been determined by performing special different tests for each of the selected parameters. Using MATLAB interface, more than 600 images having different types, formats and dimensions taken from different sources has been tested. The proposed model is implemented to analyse the impact of transformations i.e. rotation and resizing onto a wide variety of images using manual tampering. On the basis of selected values of *l* and *t*, the experimental results thus obtained indicate different tampering condition, region where it is located and its extent. It is further observed that variance is the most efficient parameter to show maximum difference in original and tampered image rather than skewness and kurtosis. Moreover, the value of the parameters is dependent on the size of the image blocks. With the increase in size of image block, value of parameter also increases and vice-versa. The final decision about tampering is given after comparing the block-wise values of the statistical features of original image and tampered image. The experimental results thus obtained signify that the suggested framework is capable in locating the duplicated areas and can work effectively for locating the copy-paste tampering of low to moderate nature. The generated results can be utilized for preliminary verification of the images for tampering and to improve the tampering detection by locating most likely cases of potential digital image tampering.

VII. Limitations and Future Work

In certain cases, the inappropriate selection of block size may fail to detect closely matching blocks or generate too many false matches. The suggested framework gives sound and reasonable results and can be further analyzed for certain other transformations over a large domain of images having different formats, dimensions and different block sizes.

References

[1] Kusam, P. Abrol, and Devanad, “Digital tampering detection techniques: A review,” *BVICAM’s International Journal of Information Technology*, vol. 1, no. 2, pp. 125-132, 2009.

[2] K. Sharma and P. Abrol, “Non-overlapping block-based copy-paste forgery detection model,” *International Journal of Computer Applications*, vol. 133, no. 3, pp. 17-24, 2016.

[3] V. Kumar and P. Gupta, “Importance of statistical measures in digital image processing,” *International Journal of Emerging Technology and Advanced Engineering*, vol. 2, pp. 56-62, 2012.

[4] A. Sharma and P. Abrol, “Research issues in designing improved eye gaze based HCI techniques for augmentative and alternative communication,” *International Journal of Emerging Technologies in Computational and Applied Sciences*, vol. 6, no. 2, pp. 149-153, 2013.

[5] M. Tajrobekar (2014) Where must we use variance and mean of image? [Online].Available:http://www.researchgate.net/post/ Where_must_we_use_variance_and_mean_of_image.

[6] Dattatherya, S. V. Chalam, and M. K. Singh, “A generalized image authentication based on statistical moments of color histogram,” *ACEEE International Journal on Recent Trends in Engineering and Technology*, vol. 8, no. 1, 2013.

[7] D. J. Wheeler (2011) Problems with Skewness and Kurtosis, Part One. [Online]. Available: http://www.qualitydigest.com/inside/ quality-insider-article/problems-skewness-and-kurtosis-part-one.html.

[8] D. J. Wheeler (2011) Problems with Skewness and Kurtosis, Part Two. [Online]. Available: http://www.qualitydigest.com/inside/ quality-insider-article/problems-skewness-and-kurtosis-part-two.html.

[9] X. Pan and S. Lyu, “Region duplication detection using image feature matching,” *IEEE Transactions of Information Forensics and Security*, vol. 5, no. 4, pp. 857-867, 2010.

[10] L. Kang and X. Cheng, “Copy-move forgery detection in digital image,” *IEEE 3rd International Congress on Image and Signal Processing*, vol. 5, pp. 2419-2421, 2010.

[11] 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,” *IEEE International Conference on Multimedia and Expo*, pp. 1750-1753, 2007.

[12] N. Muhammad, M. Hussain, G. Muhamad, and G. Bebis, A Non-Intrusive Method for Copy-Move Forgery Detection, ISVC, Part II, LNCS, Springer-Verlag, 2011, vol. 6939, pp. 516-525.

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

[14] H. J. Lin, C.W. Wang, and Y. T. Kao, “Fast copy–move forgery detection,” *WSEAS Transactions on Signal Processing*, vol. 5, no. 5, pp. 188–197, 2009.

[15] X. Wang, X. Zhang, Z. Li and S. Wang, “A DWT-DCT based passive forensics method for copy-move attacks,” *3rd IEEE International Conference on Multimedia Information Networking and Security*, pp. 304-308, 2011.

[16] Y. Huang, W. Lu, and D. Long, “Improved DCT-based detection of copy-move forgery in images,” *Elsevier, Forensic Science International*, vol. 206, issues 1-3, pp. 178-184, 2011.

[17] X. Pan, X. Zhang, and S. Lyu, “Exposing image forgery with blind noise estimation,” in *Proceedings of the 13th ACM multimedia workshop on Multimedia and Security*, pp. 15-20, 2011.

[18] B. Mahdian and S. Saic, “Using noise inconsistencies for blind image forensics,” *Elsevier, Image and Vision Computing*, vol. 27, issue 10, pp. 1497-1503, 2009.

[19] A. C. Popescu and H. Farid, “Exposing digital forgeries by detecting duplicated image regions,” Department of Computer Science, Dartmouth College, Tech. Rep. TR2004-515, 2004.

[20] J. Zhang, Z. Feng and Y. Su,” A new approach for detecting copy-move forgery in digital images,” *11th IEEE International Conference on Communication Systems*, pp. 362-366, 2008.

[21] Z. Zhang, Z. Yu, and B. Su, “Detection of composite forged image,” *IEEE International Conference on Computer Application and System Modeling*, vol.11, pp. 572-576, 2010.

[22] Y. Huang, W. Lu, W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery in images," *Elsevier, Forensic Science International*, vol. 206, pp. 178–184, 2011.

[23] G. Liu, J. Wanga, S. Lian, and Z. Wanga, "A passive image authentication scheme for detecting region-duplication forgery with rotation," *Elsevier, Journal of Network and Computer Applications*, vol. 34, pp. 1557–1565, 2011.

[24] W. Li and N. Yu, "Rotation robust detection of copy-move forgery," in *Proceedings of 17th IEEE International Conference on Image Processing*, pp. 213-216, 2010.

[25] M. N. Shaikh, Y. R. Kalshetty, and D. J. Ghanawajeer, "A SIFT for copy-move attack detection & transformation recovery," *International Journal of Advanced Engineering Research and Studies*, vol. 3, issue 1, pp. 108-111, 2013.