Non-Overlapping Block-based Parametric Forgery Detection Model

Kusam Sharma
Research Scholar
Department of Computer Science & IT,
University of Jammu, J&K, India

Pawanesh Abrol, PhD
Professor
Department of Computer Science & IT,
University of Jammu, J&K, India

ABSTRACT

Modification of a digital image by adding or removing some of its elements using a wide variety of image processing tools results in image forgery. As a result authentication of originality of a digital image is becoming a challenging task. Copy-paste forgery is one of the forgeries belonging to context based forgery. Copy-Paste Forgery Detection (CPFD) aims at finding regions that have been copied and pasted within the same or different image. A small change in the image may change statistical parameters that can be analysed for initial assessment of the forgery. In the present research study, a parametric forgery detection model using non-overlapping block-based technique is developed to ascertain the copy-paste forgery in a given digital image. Statistical parameters of the input image are computed, analysed and compared with those of the forged image. The results show that the proposed model identifies the forged area of the given image and works well with low to moderate copy-paste forgery. The results obtained can be used as the initial verification of the images for forgery and to enhance the forgery detection process by identifying most likely cases of possible image forgeries. The proposed model is tested with large domain of images having different dimensions and for detecting forgery within an image. However, the model has limitations with certain geometrical transformations.

General Terms

Digital Image Forgery Detection Techniques.

Keywords

Copy-paste forgery, Block-based forgery detection techniques, Non-overlapping block-based techniques.

1. INTRODUCTION

Digital image forgery is the process of altering the material elements of an image using several pre-existing image processing tools. Digital image forgeries can be context based, graphical software based or content based. The context based forgery is created by varying the context of an image. Context-based image forgery detection technique locates duplicated image regions with in an image or between the two images or among more than two images. The copy-paste forgery is of two types, forgery in one image and digital splicing. Copy-paste forgery in one image belongs to context based forgery whereas digital splicing can be done with different images [1]. Since, the copied segments come from the same image, all of its properties, metric and topological, and statistical information will be same with the rest of the image. Detection of such forgeries is a very challenging task.

The copy-paste forgery detection techniques are further classified into two categories based on grouping of evaluated feature sets such as key-point based and block based. These are parametric based techniques. The key-point based methods like SIFT, SURF, LPFT, etc rely on the identification and selection of high entropy image regions instead of blocks. In block based techniques, the original image is divided into overlapping or non-overlapping blocks. The transformations are applied over the block to generate the feature vectors of the image features like statistical features, geometrical features or textural features. Block based forgery detection techniques can be non-overlapping or overlapping. Some of the non-overlapping block based techniques may include DCT, DWT, PCA, SVD, PAN's methods. The overlapping block based techniques include DCT, PCA, DWT, improved SVD, DWT-SVD, DWT & PCA-EVD, FMT, LUO's method etc. Block-based techniques are invariant to various transformations like flipping, brightness changes and blurring.

Block based forgery detection techniques can be parametric or non-parametric. The parametric block based forgery detection technique analyses a wide variety of image parameters like statistical, geometrical and textural. The statistical parameters are very significant and manipulation in an image can be detected by analysing the behaviour of these statistical parameters. These techniques can be applied in various fields like image enhancement, image restoration, image denoising and digital image forgery detection etc. Moreover, these techniques also find their application in the field of edge detection and eye gazing [2]. The analysis of these statistical parameters of an image helps in determining and locating the forged region within an image [3].

The present research work is context based and is carried out for developing a non-overlapping block based parametric forgery detection model for locating duplicated image regions with in an image. Understanding of these parameters may help in optimizing different image processing models especially in the field of forgery detection. There can be different statistical parameters for detecting image forgery. Besides mean and standard deviation there are other statistical parameters i.e. variance, skewness and kurtosis. The mean is used in applications such as noise removal or low pass filtering (smoothing) while variance can be used in identifying sharp details such as edges. Mean and variance of an image is used where pixel variation of images belongs to particular class are same. Variance is normally used to find how each pixel varies from the neighboring pixel or centre pixel and is used to classify them into different regions [4][5]. Standard deviation describes the variability of the data. It indicates how much on an average each of the values in the distribution deviates from the mean or centre of the distribution [6]. Skewness and kurtosis are the shape parameters. The skewness and kurtosis characterize the tails of a probability model rather than the central portion. As a result of which, any two probability models with same mean, standard deviation, skewness and kurtosis will have similar shapes [7] [8].

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 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.

2. LITERATURE REVIEW

The digital image forgeries can be content based, context based or creation based. Several researchers have adopted different methods for detection of such forgeries. Copy-move forgery being the context based forgery is detected by two broadly classified techniques key-point based and block-based. Key-point based methods basically rely on the identification and selection of high entropy image regions instead of blocks. Some of the widely accepted and used key-point based copy-move forgery detection techniques are discussed below:

A novel approach to detect copy-move forgery which works even in the presence of rotation and scaling that took place before copying is presented by Wu et al. This method is based on LPFT (Log-Polar Fourier Transform). Similarity between the original and forged regions is revealed by comparing cross-spectrum coefficients of the LPFT magnitude spectra [9]. Another method based on an efficient key-point and feature computation algorithm known as Scale Invariant Feature Transform (SIFT) is proposed in [10]. In this method, the image key-points will be located and image features at the detected key-points will be collected. This method is robust to distortions of the duplicated regions. This method fails to detect reliable SIFT key-points in regions with little visual structures. Another automatic and robust forgery detection system based on SURF (Speeded Up Robust Features), which are fast detectors and descriptors and KD-Tree is used to identify the duplicated regions is proposed by Shivakumar et al [11]. This method sometimes fails in successfully detecting the few small sized copied regions. An efficient and reliable passive-blind detection method in which block matching procedures are used which first divides the image into the same size b x b blocks is suggested in [12]. In this improved singular value decomposition (improved SVD) is applied to all the image blocks. This algorithm has strong detection as well as anti-noise capabilities. An SVD based sorted neighborhood approach for detection in which an image is decomposed into four sub-bands by applying DWT (Discrete Wavelet Transform) is proposed by Li et al [13]. However, the computation of SVD takes a lot of time and the time complexity of sorting is reduced to O(7k log k) then that discussed in PCA method given by Popescu and Li. Another SVD based method for investigating the extent of noise for detecting forgery in digital images is given in [14]. An improved detection algorithm based on Discrete Wavelet Transform (DWT) and Principal Component Analysis – Eigen Value Decomposition (PCA-EVD) has been presented by Zimba in [15]. Another efficient non-intrusive method for copy-move forgery detection is based on image segmentation and a new denoising algorithm does not require prior knowledge about the camera used to capture the image [16]. An FMT based method is used to extract image feature from image blocks of size 16 to reduce the detection time [17]. Counting Bloom Filters are used instead of lexicographical sorting to improve the efficiency of detecting duplicated regions. The complexity is O(length (MN)). Lin et al. suggested a method in which radix sort is used for sorting the feature vectors of the divided overlapping sub-blocks as an alternative to lexicographic sorting, which is commonly used by the existing copy-move forgery detection schemes. The medium filtering and connected component analysis are performed on the tentative detected result to obtain the final result. Even though the proposed technique reduced the time complexity to O(9k) with the help of radix sort, the method fails to detect all copied region of small size. This scheme performs well when the degree of rotation is 90^o, 180^o and 270^o [18].

Another forgery detection method involves block-based copy-move forgery detection techniques which are further classified into non-overlapping and overlapping based techniques. Some of the recently developed and used non-overlapping and overlapping based forgery detection techniques are discussed below:

A passive forensic method for detecting copy-move attacks based on DCT and DWT is suggested by Wang et al. The test image is segmented into non-overlapping 8x8 blocks. DCT and DWT are applied to each image block to extract features and then compare the statistical parameters of each image block to detect replicated regions. The time complexity of their method for sorting is further reduced to O(k lg k) then that given in method proposed by Luo, Li and Popescu. This method is robust to compression up to JPEG quality level 20 and against additive noise [19]. Another improved DCT based method for detection of copy-paste forgery in digital images is given by Huang et al [20]. This method is capable of detecting the duplicated regions even in the presence of blurring, additive white Gaussian noise and JPEG compression. A new two-phase detection method to effectively locate image forgeries based on inconsistency of noise levels in different regions of the image is given in [21]. In this method, the image is first segmented into non-overlapping image blocks for initial noise estimation using an effective noise estimation method. The kurtosis of the original natural image and the variance of the added noise are computed for forgery detection. It not only improves the detection accuracy but reduces the computation complexity and detects image forgeries both quantitatively and qualitatively. This method works only for grayscale images. The advantage of this method is that no previous information about the original image and the imaging device is required. Another segmentation method based on inconsistencies of noise for digital image forgery detection is given by Mahdian et al [22]. In this method noise standard deviation of each block is estimated using median-based method.

Some of the overlapping block-based feature extraction approaches for forgery detection includes a direct approach of applying an exhaustive search as proposed by Fridrich et al. This approach is computationally very expensive. It is simple and effective for small sized images. The second approach is of block-matching by using quantized DCT coefficients where the image is divided into overlapping blocks. The features of these blocks are extracted and then these blocks are vectorized and sorted lexicographically for further detection. This approach is robust to retouching operations. The computational time depends upon factors such as number of blocks, sorting techniques and the number of features [23]. Another DCT-SVD based method used for detection of copy-move forgery based on overlapping and non-overlapping technique is given by Zhao et al [24]. This method is quite efficient in detecting duplicated regions even in the presence of Gaussian blurring, AWGN, JPEG compression. Later on, Luo et al. proposed a new method based on pixel block characteristics. This approach firstly divides an image into small overlapped blocks, and then the similarity of these blocks is compared for identifying duplicated regions. The time complexity of their method for sorting is further reduced to O(7k lg k) then that given by Li and Popescu. This method is robust to compression up to JPEG quality level 30 and Gaussian blurring and additive noise with SNR 24 dB [25]. A block-based approach which exploits texture as feature to be extracted from blocks is given in [26]. This method is tested on both JPEG compressed and un-compressed images. Another DWT based technique to get a reduced dimension representation is robust to common post-processing operations and has lower computational complexity [27]. A novel image hashing method used for image forgery detection which employs both the local and global features of an image is given by Sundaram et al. The local features include position and texture features of each significant region of the image whereas the global features based on the complex Zernike moments represent the chrominance and luminance characteristics of the image [28].

There are certain widely accepted, latest and authenticated parametric and non-parametric copy-move forgery detection approaches.

An efficient technique for detecting and localizing duplicated regions in an image 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. The time complexity of sorting is O(32k lg k) [29]. Dattatherya et al. has given an image authentication method for gray and coloured images having different dimensions and formats for hybridization of colour histogram. It is associated with first four statistical moments i.e. mean, standard deviation, skewness and kurtosis to achieve the objectives of low cost and high speed. The authentication code is used to analyze the characteristics of received image from tampering point of view [30]. The technique proposed by Zhang et al. works by applying DWT (Discrete Wavelet Transform) to the input image to get a reduced dimension representation [31]. For the most common blur operations of composite forged image, a localization approach of forged region based on detection of image edge is proposed [32]. This technique can accurately detect the blur operation traces of composite forged images and can precisely locate the forged region. But the high complexity of the texture and the low robustness of edge detection algorithm may cause some false detection.

Several copy-paste digital image forgery detection approaches are existing at present and can be distinguished on the basis of their domain of working. Key-point based techniques include SIFT, SURF, LPFT, FMT, etc rely on the identification and selection of high entropy image regions instead of blocks. Block-based techniques include non-overlapping and overlapping techniques which include DCT, DWT, PCA, etc. In non-overlapping, there are several parametric and non-parametric techniques for forgery detection. Parametric techniques are simple and efficient in detecting copy-paste forgery. In this research work a parametric non-overlapping block-based copy-paste technique is developed for forgery detection. The objectives of the present research study are discussed in the next section.

3. OBJECTIVES

It is evident from the literature review that the analysis of image parameters may indicate some important aspects of image region duplication, tampering or forgery within an image. Further non-overlapping block-based parametric image analysis is one of the significant techniques that are used for image analysis. Based on these observations this study has been conducted with the following research objectives:

- Study of forgery detection algorithms for digital images.
- Understanding copy-paste forgery detection models and identification of significant statistical parameters.
- Developing a non-overlapping block-based model for detecting copy-paste forgery within the same image.
- Analysis of the parametric result for ascertaining the extent and location of the forgery within an image using non-overlapping block-based parametric forgery detection model.

In the next section, methodology of the proposed non-overlapping block-based parametric forgery detection model for detecting copy-paste forgery has been presented.

4. METHODOLOGY

In order to detect copy-paste forgery, a statistical parameter based forgery detection model using non-overlapping block-based technique has been proposed. The block diagram of the proposed non-overlapping block based forgery detection model is presented in Figure 1.

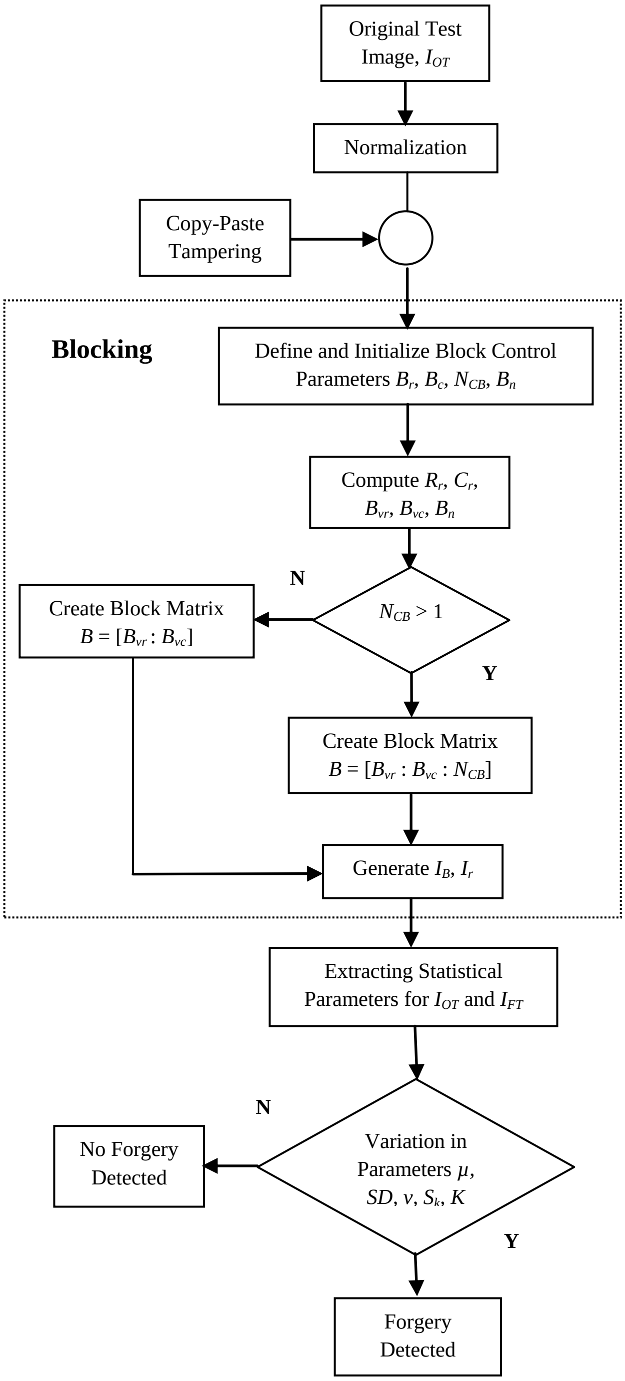
Original Test Image, I_{OT}
Normalization
Copy-Paste Tampering
Blocking
Define and Initialize Block Control Parameters B_r, B_c, N_{CB}, B_n
Compute R_r, C_r, B_{vr}, B_{vc}, B_n
N
$N_{CB} > 1$
Y
Create Block Matrix $B = [B_{vr} : B_{vc}]$
Create Block Matrix $B = [B_{vr} : B_{vc} : N_{CB}]$
Generate I_B, I_r
Extracting Statistical Parameters for I_{OT} and I_{FT}
N
Variation in Parameters μ, SD, v, S_k, K
Y
No Forgery Detected
Forgery Detected

Fig 1: Proposed non-overlapping block-based parametric model for copy-paste forgery detection with additional control parameters

Initially an original image (I_{OT}) of any type is taken from the data source. After normalization, I_{OT} is divided into four non-overlapping blocks of size [m x m]. Parameters like block row (B_r), block column (B_c), number of colour bands (N_{CB}), number of blocks (B_n) are defined and initialized. Based on the image size and block size; values for row residue (R_r), column residue (C_r), block vector row (B_{vr}), block vector column (B_{vc}) and (B_n) are computed. A two or three-dimensional block matrix B is created depending on the number of colour bands (N_{CB}), resulting in the generation of blocked image (I_B) along with image residue (I_r). The I_r can further be used in cases when there is a mismatch between block size and image dimension. After the segmentation of an image, the parameters mean (μ), standard deviation (SD), variance (v), skewness (S_k) and kurtosis (K) of the original image are computed. Copy-paste forgery is done in the original image resulting into a forged image (I_{FT}). This copy-paste forged image is again segmented into non-overlapping blocks and all parameters under study are computed. Each corresponding block of I_{OT} are analysed and compared with those of I_{FT} for further forgery detection. The statistical variation $\boldsymbol{\partial p = |P_{IO} - P_{IF}|}$ is computed and analysed for ascertaining the forgery.

Threshold t, defines the permissible proportion of variation in the parameter under study. The value l of threshold t is set after testing a wide range of image sets and analysing the behaviour of parameters. Based on the variation, the forgery status DT (detected) or ND (not detected) is established. Further analysis is done to find the specific location, i where the forgery is actually been done. The proposed interface for forgery detection is developed in MATLAB version 7.6.0.324 (R2008a) and is tested for more than 200 gray scale bmp images.

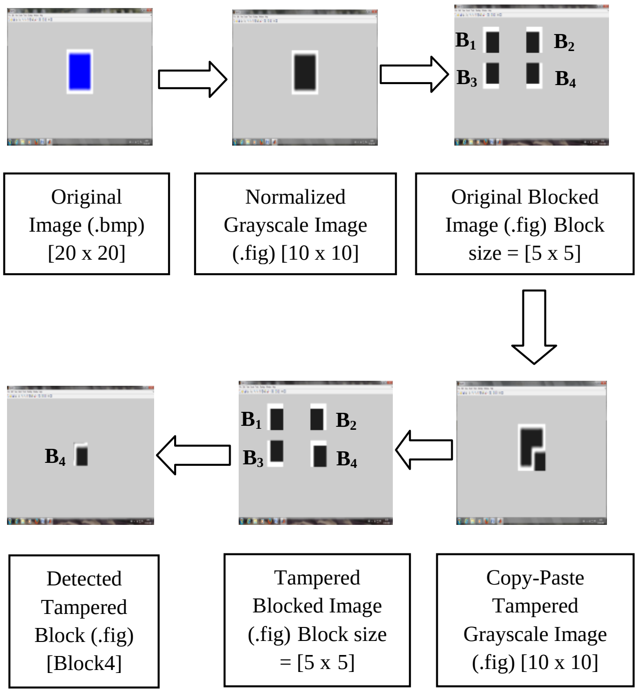
B_1
B_2
B_3
B_4
Original Image (.bmp) [20 x 20]
Normalized Grayscale Image (.fig) [10 x 10]
Original Blocked Image (.fig) Block size = [5 x 5]
B_4
B_1
B_2
B_3
B_4
Detected Tampered Block (.fig) [Block4]
Tampered Blocked Image (.fig) Block size = [5 x 5]
Copy-Paste Tampered Grayscale Image (.fig) [10 x 10]

Fig 2: Parametric non-overlapping block-based copy-paste image forgery detection stages

Figure 2 shows the stages of the proposed parametric non-overlapping block-based copy-paste image forgery detection model. The original image I_{OT} after normalization is divided into four non-overlapping blocks of size [m x m]. Then, copy-paste forgery is done in the original image resulting into a forged image I_{FT}. This forged image is again segmented into four non-overlapping blocks of same dimension and all statistical parameters under study are computed and compared for both I_{OT} and I_{FT}, thus giving the forged block B_4.

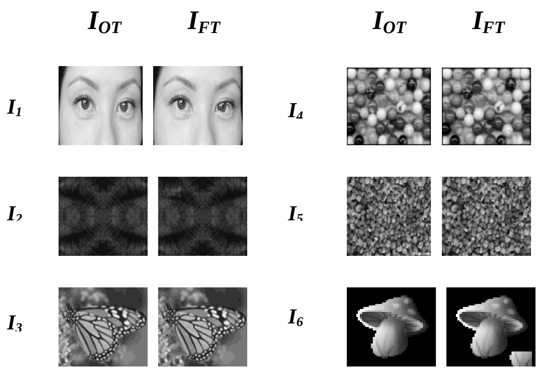

Fig 3: Set of gray-scale copy-paste forged images (I_{FT}) along with their corresponding gray-scale original images (I_{OT})

Figure 3 shows the original test image I_{OT} and the corresponding forged image $I_{FT.}$ The copy-paste forgery has been induced manually in the original image. A set of six gray-scale bmp images with corresponding forged images have been shown in it.

The experimental results thus obtained are further analysed and discussed in the next section.

5. RESULTS AND DISCUSSIONS

The experimental results are obtained after the implementation of the proposed parametric non-overlapping block-based model for copy-paste forgery detection. The cases shown in Table 1 are selected cases out of 200 test results where there is significant variation of the different statistical parameters of original and forged images depicting copy-paste forgery detection based on threshold *t*. One of the cases of I_{T10} shows the Not Detected i.e. ND status since all the threshold values are below *l*. The statistical variation ∂ in the given above said parameters for original and forged images and their blocks is computed for each parameter. The statistical variation in each parameter is given by ∂_{μ}, ∂_{SD}, ∂_{v}, ∂_{Sk} and ∂_{K}.

The threshold *t*, the permissible proportion of statistical variation in the parameter under study, for each statistical parameter is set. The value *l* of threshold *t* is set after testing a wide range of image sets and analysing the behaviour of statistical parameters. Based on the variation, the forgery status is established. Further analysis is done to find the specific location of the forgery in the image after dividing it into four non-overlapping blocks. The value of threshold t_1 for ∂_{μ}, t_2 for ∂_{SD}, t_3 for ∂_{v}, t_4 for ∂_{Sk} , t_5 for ∂_{K} is set to 0.3, 0.2, 3, 0.6 and 3 respectively. The image I_{T5} is showing least variation for all statistical parameters whereas I_{T4} and I_{T8} are showing maximum variation for *K*, I_{T6} is showing maximum variation for *v*.

Moreover, the ∂_{Sk} of the images $I_{T3,}$ I_{T4}, $I_{T6,}$ I_{T8} and I_{T9} are greater than 1.0, which signifies that the ∂_{Sk} is substantial and the distribution is far from symmetrical. These asymmetrical distributions will have long tail to the right and a positive skew.

Table 1. Parametric differences of original and forged images depicting copy-paste forgery detection based on threshold *t*, (*t*>=*l*)

Test image I_T	Parametric variation (t>=*l*)					Forgery status
	t_1=0.3	t_2=0.2	t_3=3	t_4=0.6	t_5=3	
	∂_{μ}	∂_{SD}	∂_{v}	∂_{Sk}	∂_{K}	
I_{T1}	00.19	00.20	02.66	00.06	00.28	DT
I_{T2}	00.48	00.33	04.74	00.87	02.21	DT
I_{T3}	01.46	00.39	09.64	01.92	06.56	DT
I_{T4}	03.89	00.23	02.11	07.85	25.43	DT
I_{T5}	00.01	00.02	01.01	00.06	00.19	DT
I_{T6}	01.26	00.55	22.94	01.38	07.37	DT
I_{T7}	01.41	00.31	14.18	00.69	05.31	DT
I_{T8}	00.63	00.38	08.85	18.12	68.33	DT
I_{T9}	00.26	00.21	05.35	01.07	03.09	DT
I_{T10}	00.00	00.00	00.00	00.00	00.00	ND

Also, it is deduced from the results generated above that the ∂_k of all the images except I_{T10} are greater than 0. These positive kurtosis images would have a fairly uniform distribution of gray levels.

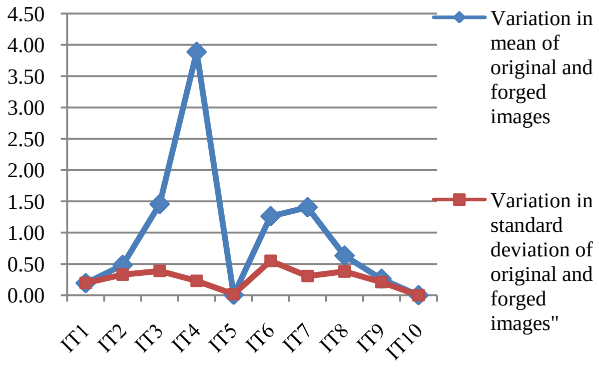

Fig 4: Parametric difference in *μ* and *SD* of original and forged images (I_{T1}-I_{T10})

Figure 4 depicts the relationship of two statistical parameters *μ* and *SD* of original and forged images (I_{T1}-I_{T10}). Forgery can be observed in all the test images except I_{T10}. Also, maximum variation is seen in *μ* for test image I_{T4} and in test image I_{T6} for *SD*. The statistical variation in these two parameters is noticeable.

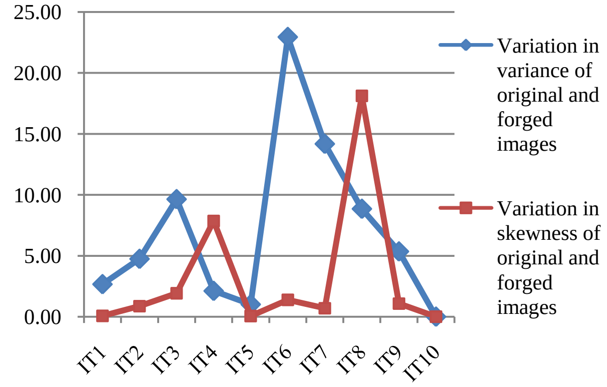

Fig 5: Parametric difference in v and S_k of original and forged images (I_{T1}-I_{T10})

Variance and skewness of original and forged images (I_{T1}-I_{T10}) shows forgeries in all the images except I_{T10} shown in Figure 5. The graph shows maximum variation in variance for test image I_{T6} and in test image I_{T8} for skewness. For maximum cases, the statistical variation in variance is significant.

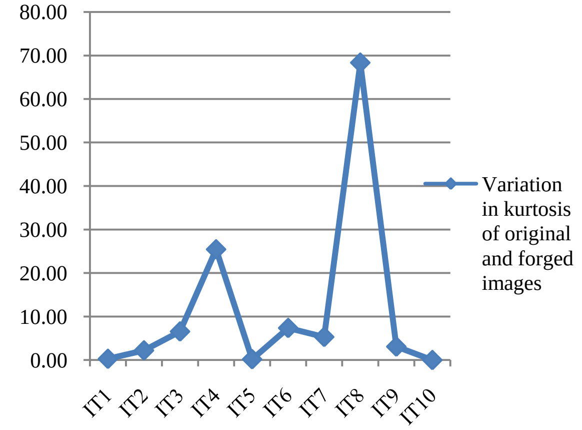

Fig 6: Parametric difference in K of original and forged images (I_{T1}-I_{T10})

Variation in kurtosis for original and forged images (I_{T1}-I_{T10}) can be seen in Figure 6 shows the behaviour of another parameter kurtosis of original and forged images (I_{T1}-I_{T10}) thus depicting the presence of forgery in all the images except I_{T10}. The images I_{T8} and I_{T4} show maximum variation whereas image I_{T10} shows no variation in kurtosis.

The Table 2 shows the parametric variation ∂_i along with corresponding threshold t_i for selected two different images I_{T4} and I_{T7} and their corresponding blocks. These two images are selected from Table 1 on the basis of significant variation in their statistical parameters and their corresponding graphs. l for each parametric variation has been computed after testing a wide range 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 both the images in which forgery has been observed.

Table 2. Block-wise parametric differences of original and forged images depicting copy-paste forgery detection based on threshold *t*, (*t*>=*l*)

Image blocks	Parametric variation (*t*>=*l*)					Forgery status & location, loc
	t_1=0.3	t_2=0.2	t_3=3	t_4=0.6	t_5=3	
	∂_μ	∂_{SD}	∂_v	∂_{Sk}	∂_K	
I_{T4}	03.89	00.23	02.11	07.85	25.43	DT (B_2,B_3, B_4)
B_1	00.00	00.00	00.00	00.00	00.00	
B_2	05.82	00.10	38.11	06.90	06.61	
B_3	06.39	02.38	40.42	01.79	00.31	
B_4	03.34	01.07	06.73	01.59	05.17	
I_{T7}	01.41	00.31	14.18	00.69	05.31	DT (B_1,B_2, B_3)
B_1	01.54	00.59	13.83	00.53	01.01	
B_2	03.04	00.78	15.76	03.20	06.79	
B_3	01.05	00.61	39.65	00.61	02.26	
B_4	00.00	00.00	00.00	00.00	00.00	

Further in Table 2, blocks B_2, B_3, B_4 of test image I_{T4} and blocks B_1, B_2, B_3 of test image I_{T7} shows statistical variation in all their parameters thus confirming the existence of forgery. The block B_1 of test image I_{T4} and block B_4 of test image I_{T7} show no statistical variation in any of its parameters thus depicting that no forgery has been done.

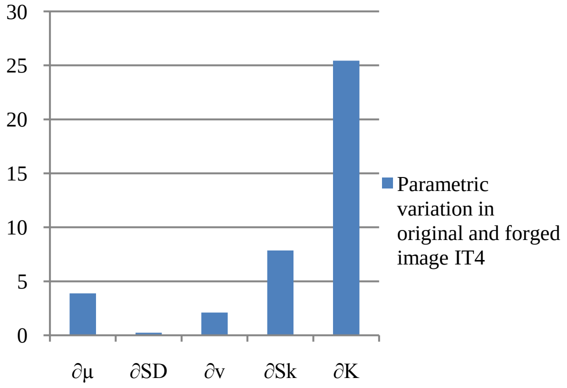

Fig 7: Parametric variation in original and forged image I_{T4}

Figure 7 represents the column chart for parametric variation of original and forged image I_{T4} thus giving the evidence of forgery. The graph shows maximum variation in kurtosis and insignificant variation in standard deviation for test image I_{T4}.

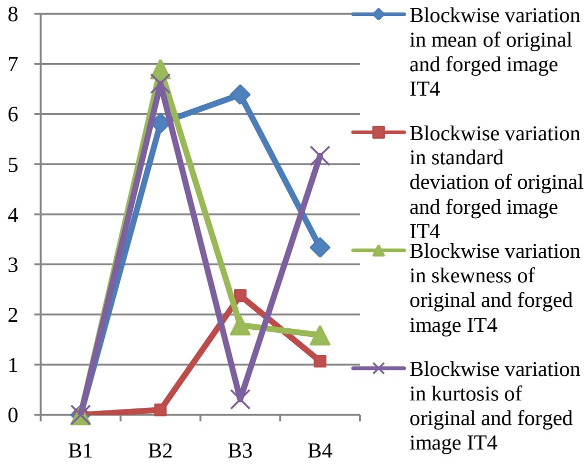

Fig 8: Block-wise parametric variation in μ, SD, v, S_k and K of original and forged image I_{T4}.

Figure 8 shows the relationship among four statistical parameters mean, standard deviation, skewness and kurtosis for blocks of original and forged image I_{T4}. The statistical variation in these parameters shows forgery in three blocks B_2, B_3, B_4. Block B_1 shows no variation for any of these parameters whereas B_2 shows maximum variation for mean, skewness and kurtosis and least for standard deviation.

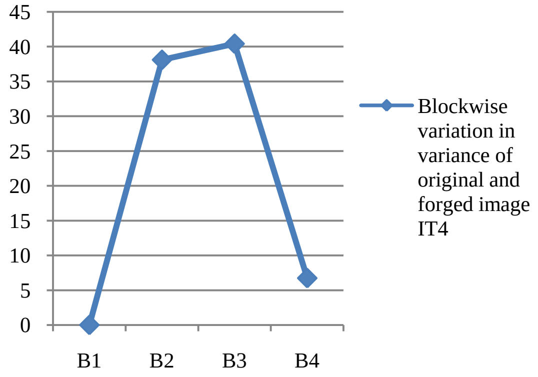

Fig 9: Block-wise parametric variation in v of original and forged image I_{T4}

Figure 9 shows the block wise variation in variance of original and forged image I_{T4}. Maximum variation in variance for blocks B_2 and B_3 can be seen in the graph.

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

6. INFERENCES AND CONCLUSION

This parametric model for copy-paste forgery detection within an image is based on non-overlapping block based techniques. Five statistical parameters have been analysed by using specific threshold values. The threshold values have been ascertained by performing different tests for each of the selected parameters. A domain of more than 200 images taken from different sources in bmp format has been tested using MATLAB interface. The forgery has been induced manually at different locations within the given image.

The results observed for different statistical parameters and for different images along with their blocks depict the forgery status, its extent and location as per careful selection of t and l values. Out of five statistical parameters, variance and kurtosis are the ideal parameters showing maximum variation in original and forged image. The results obtained can be used as the initial verification of the images for forgery. This may enhance the forgery detection process by identifying the most likely cases of possible image forgeries.

7. LIMITATIONS AND FUTURE WORK

Parametric block-based copy-paste forgery detection model may fail when the copied region undergoes some geometrical transformations like scaling, rotation, translation, etc. The proposed model generates satisfactory results and is further explored for certain other features and parameters over a wider range of images having different types, formats and dimensions.

8. 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] A. Sharma and P. Abrol, “Eye Gaze Techniques for Human Computer Interaction: A Research Survey”, International Journal of Computer Applications, vol. 71, no. 9, pp. 18-29, May 2013.

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

[4] Tajrobekar, M. 2014. Where must we use variance and mean of image? Available online at:. http://www.researchgate.net/post/ Where_must_we_use_variance_and_mean_of_image.

[5] Wegmuller, M., Weid, J.P., Oberson, P. and Gisin, N. 2000. High resolution fiber distributed measurements with coherent OFDR. In *Proc. ECOC’00*, paper 11.3.4, p. 109.

[6] Statistics: Standard deviation Available online at:. http://www.khanacademy.org/math/probability/descriptive-statistics/ variance_std_deviation/v/statistics-standard-deviation.

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

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

[9] Wu, Q., Wang, S. and Zhang X. 2010. Detection of image region-duplication with rotation and scaling tolerance. Computational Collective Intelligence, Technologies and Applications - Second International Conference, ICCCI, Part I, vol. 6421, pp. 100-108.

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

[11] B. L. Shivakumar and S. S. Baboo, “Detection of region duplication forgery in digital images using SURF”,

International Journal of Computer Science Issues, vol. 8, no. 1, pp. 199-205, Jul. 2011.

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

[13] Li, G., Wu, Q., Tu, D. and Sun, S. 2007. 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.

[14] D. Sharma and P. Abrol, "Investigating the Extent of Noise in Digital Images using SVD", International Journal of Software and Web Sciences, vol. 4, no. 1, pp. 6-14, May 2013.

[15] M. Zimba and S. Xingming, "DWT-PCA (EVD) based copy-move image forgery detection", International Journal of Digital Content Technology and its Applications, vol. 5, no. 1, pp. 251-258, Jan. 2011.

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

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

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

[19] Wang, X., Zhang, X., Li, Z. and Wang, S. 2011. A DWT-DCT based passive forensics method for copy-move attacks. IEEE Third International Conference on Multimedia Information Networking and Security, Nov. 2011, pp. 304-308.

[20] 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, March 2011.

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

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

[23] Fridrich, J., Soukal, D. and Lukáš, J. 2003. Detection of copy-move forgery in digital images. In Proceedings of Digital Forensic Research Workshop, Cleveland OH, USA.

[24] J. Zhao and J. Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD", Elsevier, Forensic Science International, vol. 233, issues 1-3, pp. 158-166, Dec. 2013.

[25] Luo, W., Huang, J. and Qiu, G. 2006. Robust Detection of Region Duplication Forgery in Digital Images. In Proceedings of the 18th International Conference on Pattern Recognition, vol. 4, pp. 746-749.

[26] Ardizzone, E., Bruno, A. and Mazzola, G. 2010. Copy-move forgery detection via Texture Description. Proceedings of the 2nd ACM workshop on Multimedia in forensics, security and intelligence, pp. 59-64.

[27] S. Khan and A. Kulkarni, "An efficient method for detection of copy-move forgery using Discrete Wavelet Transform", International Journal on Computer Science and Engineering, vol. 2, no. 5, pp. 1801-1806, 2010.

[28] A.M. Sundaram and C. Nandini, "Feature based image authentication using symmetric surround saliency mapping in image forensics", International Journal of Computer Applications, vol. 104, no. 13, pp. 43-51, October 2014.

[29] Popescu, A. C. and Farid, H. 2004. Exposing digital forgeries by detecting duplicated image regions. Technical Report. Department of Computer Science, Dartmouth College.

[30] 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, Jan 2013.

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

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