International Journal of Advanced Trends in Computer Applications
www.ijatca.com

Detection of Splicing in Low Contrast Digital Images using Noise Based Features

[1]Amandeep Kaur, [2]Navdeep Kanwal, [3]Lakhwinder Kaur
[1,2,3] Computer Science and Engineering, Punjabi University Patiala, Punjab
[1]amandeepkaur2177@gmail.com, [2] navdeepkanwal@gmail.com, [3]mahal2k8@gmail.com

Abstract: *The main issue in image forensics is to discover whether an image is authentic or forged and, if forged, to locate which regions have been manipulated. The simple accessibility of image manipulation software have proliferated the possibility of image forgery. Detection of Splicing forgery is targeted in this paper. Noise component of a color image have been utilized to extract features from suspected image. As the consistency of noise between RGB color channel of forged and authentic image are different, so it leaves the clues of forgery. First digit features are extracted using Benfords' law and provided to the SVM classifier Columbia uncompressed image splicing detection evaluation dataset and CASIA v1.0 dataset are used to test the proposed technique. Our technique outperforms various previous techniques of image splicing detection.*

Keywords: *Forgery Detection, Image Forensics, Low Contrast, Splicing Forgery.*

I. INTRODUCTION

An image can more emphatically impact viewers than a large number of words. Images follow a progressively common and productive approach to communicate with people than the content does. Computerized visual media is one of the eminent techniques of exchanging data due to a growth in user-friendly and affordable devices [1]. All the while, the wide comprehensive accessibility of image editing tools such as (Photoshop, GIMP, Coral paint) has proved to be exceptionally basic for neophyte users to alter the images. This expands the likelihood of forging of visual information, which is never again confined to specialists. Thus, the certainty and trustworthiness that images once had, is dissolved by the progression of advanced innovation [2] [3].

These days manipulation of images are possible at the cost of the couple of clicks, which prior used to take hours or days. Every time the images are not manipulated to deceive people. In reality, the vast majority of forged images on the internet are made for insignificant excitement. Yet, there are several images which are forged/ fake still, they are publicized as real. It is essential to analyze these images to retain their authenticity. The forged images have spread in every aspect of society (counterfeiting, antique faking, entertainment etc), to misinterpret the information. Thus, the integrity and authenticity of images are believable no more.

There are various ways to forge images such as copy-move, splicing, retouching, morphing, enhancing, computer generated [4]. The prevalent image forgery methods are copy-move and splicing. Copy-move is performed on the same image, where part of the image is copied and pasted onto some other part, in-order to hide or add information in the image whereas splicing is a composite of two or more images which involves replacing of image fragments onto some other image [5].

Forgery detection is the method of demonstration to determine if, an image is genuine or forged while localization is the process of discovering/localizing the forged area in a forged image [6]. Noise is definitely introduced into an image during the phase of image acquisition and due to inherent characteristics of each camera sensor, the variation in the noise among cameras are peculiar. In this paper, we have put forward RGB noise related features to determine spliced images and to localize the forgery. Here, we concentrate on the irregularities in the correlation of noise in the RGB image. The strong correlation between channels is broken in case of spliced images. We evaluate how these features are susceptible to the size of Sliding window, which is utilized in the detection process.

The review of related work is covered in section II and the present work is discussed in section III. Then in section IV proposed methodology is discussed to detect the Splicing forgery. Section V consists of

results and discussions, finally conclusion is reached in section VI.

II. RELATED WORK

In this segment past methodologies, committed to distinguish authentic and forged images, are highlighted. In [7] the author discovered periodicity in DCT coefficients in doubly quantized images while this conduct is absent in single quantization image locales. In [8] Markov feature extraction approach as well as DCT coefficient quantization are used for detection of splicing forgery. In addition, two Markov feature selection techniques consisting of maximization and summation of color and directional characteristics have also been used. In [9] the classification technique is depicted to identify multiple JPEG compression phases conducted on a single image, to detect clues of forgery. SVM classifier is used for this purpose. In [10] image is segmented into various blocks with different noise variations and based on it the blocks are clustered into authentic and suspicious blocks. Further, the identified suspected areas are again segmented into smaller blocks to estimate noise and classified to achieve the final detection and localization outcomes. In [11] author has suggested an approach based on the color development of an image to identify if the fragment of the image is associated with the original image. The author has estimated the difference in the color consistency between the two image fragments. In [12], forgery is recognized by bi-coherence features and the features are assessed by a SVM classifier. In [13] the author have used Multi Task Fully Convolutional Network along with one branch to study the surface label and the other one to know the borders of the spliced areas in the image. In [14] the image is segmented into non-overlapping blocks. Block Matching and 3D Collaborative Filtering (BM3D) is used to estimate the irregularities in the levels of noise in various blocks. The noise inconsistency is utilized to cluster blocks where blocks with comparatively greater noise levels are determined as forged areas. In [15], the author has proposed an algorithm with the block wise Markov features as well as the coefficient wise Markov features in the DCT domain for determining the splicing forgery. In [16] the author has identified the Deblur regions and extracted their features to further, classify the features using binary classifier acquired from LDA. Then K- nearest neighbor matting is done to get the exact boundaries for splicing localization. In paper [17] proposed a technique to detect splicing incorporating hybrid feature set. A data set is formed, and image pre-processing is done. Feature Extraction is done via LBP, LTE, HoG, DWT, further training and classification of data is performed to obtain the results. [18] proposed image splicing detection by extracting features on the basis of color filter array (CFA).

III. PRESENT WORK

The present work was based on proof that forged areas of an image produce local statistical effects which does not leave any impact on the neighboring areas of an image. New features were proposed to study the noise of an image. This research had proved that a forged image would have more correlation among the R, G, B color channels. This work was based on feature extraction but no use of machine learning[19] .

IV. PROPOSED METHODOLOGY

Effortlessness in reenacting origin and information in digital images, the reliability has constantly been questioned. It initiated the requirement for image forgery detection and localization because of its consequences in almost every field. In Fig1. the structure of the proposed methodology.

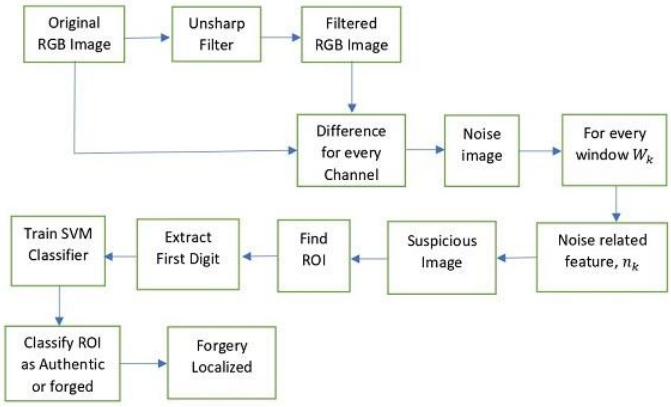

Figure1: Structure of proposed Methodology

4.1 Noise Based

A usually utilized method to mask the traces of forgery is to incorporate local random noise into the forged areas of an image. Normally, the noise in an authentic image is spread uniformly throughout the image. So, inclusion of local random noise leads to inconsistencies in the authentic image's noise. In this manner, recognition of different noise level may detect the presence of forgery.

Preprocessing

The very first step in digital image forensics is the image acquisition process. At the point when a scene is caught by digital camera, photons transmitting from the scene go through the optical framework (such as lens) and meet onto the focal plane. Color filter array (CFA) is used to filter the incident light to get the color information of light. It gives specific light wavelength to every color. Bayer" filter mosaic is frequently used. Then the light is passed to the imaging sensor, it can be a Charged Couple device (CCD, is

mostly preferred) or Complementary metal oxide semiconductor (CMOS). Thus, the sensor yield is information of light containing red, green and blue pixels on a sole layer. The signal is interpolated to get a canonical 3-channel representation. Demosaicing algorithms are used to acquire the leftover pixel values in each layer depending upon the neighborhood pixels. Several post-processing operations such as demosaicing, gamma correction and white balancing are carried out before the storage of an image [20].

At every pixel 'i' of the color tested image, Unsharp filter is utilized to de-noise the image to get a filtered RGB image as given in eq. (1). Unsharp filter enhances the appearance of details by enhancing small-scale acuity. The process of sharpening is performed by utilizing a little blurred version of the original image and computing its difference from the original image to determine the presence of edges by creating an unsharp masking. Further, Contrast is improved along these edges by utilizing this mask, yielding a sharper final image. In this work, we freely concentrate to take out noise from every RGB channel by evaluating the difference between the tested image and its unsharp filtered image is shown in eq. (2). For every pixel we got three noise values to be specific as r_i, g_i, b_i.

$$H = fspecial('unsharp') \quad (1)$$

$$Y = imfilter(X, H) \quad (2)$$

$$N(i) = \big(X(i) - Y(i)\big) \quad (3)$$

4.2 Feature Extraction

The proposed features depend upon the described statistical characteristics outlined for noise values in a sliding window. The noise-based feature, which is utilized to determine the image to be suspicious or not.

The size of the Sliding Window characterizes the measure of data utilized to evaluate the noise features whereas the step size describes the accuracy of the resulting detection in the relating pixel of an image. The proposed method is based on using a sliding window to meet the goals of extracting local features considering the pixels neighborhood. The considered image of pixels is segmented into overlapping blocks such as K sliding windows, each of size $w * w$, which is shown in equation (4):

$$(W_k)_k = 1 \ldots . K \quad (4)$$

Sliding windows are moved with a step size of s, similar to $s \leq w$. To prevent border issue, we examine entire sliding window, then

$$K = \frac{mn}{s^2} - w(n+m) \quad (5)$$

Noise Based Feature:

We propose a noise-based feature which is devoted to determine if the image under examination is forged or not. The point cloud of every sliding window calculates a value of noise related feature. Noise based feature is aimed to determine the blocks that overlay authentic regions with forged regions. To evaluate the dispersion, we have utilized the difference in the Euclidean distance from each stage of the cloud towards its center of mass. Let's assume that every triplet $q_i^{rgb} = (r_i, g_i, b_i)_{i=1\ldots n=w^2}$ in the sliding window W_k is, then:

$$n_k = \frac{1}{n}\sum_{i=1}^{n}\left(d\left(q_i^{rgb}, q_i^{-rgb}\right) - \mu\right)^2 \quad (6)$$

In sliding window , stands for the Euclidean distance and μ stands for the mean of the Euclidean distance and is the center of mass in the cloud in window .

Feature Matching:

The noise related features are compared to find the suspect. The value is examined and the sliding window is recognized as forged, on condition that for any k, the interval of to the mean value of the set is higher than the specified threshold

Localization Analysis:

4.6.1 First Digit Law:

The first digit law is otherwise called Benfords‟ law or Newcomb-Benfords' law. Benfords' found that the likelihood of event of 1's and 2's is higher than the likelihood of event of 8's and 9's, which is not similarly likely for natural events, [21] which is specified as:

$$P(d) = \log_{10}\left(1 + \frac{1}{d}\right) \quad (6)$$

For instance, in sets that complies with the law, the number 1 shows up as the main significant digit about 30% of the time, while 9 shows up as the main noteworthy digit under 5% of the time. On the off chance that the digits were disseminated consistently, they would each happen about 11.1% of the time.

4.6.2. Localization:

We have selected the multiple region of interest (ROI) in the suspected image and take its DCT. The 8*8 blocks are used to extract the first digits from the de-quantized DCT coefficients of an image. Extract the

first digit components using Benfords' first digit law for the ROI. SVM classifier is trained for the authentic as well as forged blocks comprising of first digits obtained through benfords' law.

V. RESULT AND DISCUSSION

So as to assess the detection results, we made use of images from "Columbia Uncompressed Image Splicing Detection Evaluation Dataset" and "CASIA v1 A Image Tampering Detection Evaluation Dataset". Columbia dataset contains a total of 363 images. Of these, 183 images are authentic whereas 180 images are the spliced. Authentic images are captured utilizing four advanced cameras, they are, Kodak DCS 330, Nikon D70, Canon EOS 350D Rebel XT and Canon G3. Images in this dataset are available in uncompressed format with different sizes varying from 757x568 to 1152x768. Contents of precisely two cameras are contained in each spliced image[22]. CASIA ITDE v1 dataset has a total 1,721 color images with 384 × 256 size of pixels in the JPEG format. Of the total images, 800 images are authentic and 921 images are forged [23].

In this area, we present the capability of the suggested feature (in eq. 4) to classify the images from database. To get more realistic results, a threshold value of 993 is selected as the prime solution for the uncompressed dataset. If the value of noise related feature is lower than the threshold, the image is determined as authentic. Whereas if the value of is higher than specified threshold, the image is considered as suspected. To detect the forged regions in an image, first digits are determined from multiple regions on each authentic and forged image. 70 authentic and 70 spliced images from dataset are used to find first digits using Benfords' law, taking 5 regions each time from the image. This method is based on a SVM classification, taking two distinct cases into account.

In Case 1 SVM classifier is trained using 200 random first digit blocks and testing data is random 10 first digit blocks from within the training data. In Case 2 SVM classifier is trained using 190 random blocks and tested using random 10 first digit blocks which are not included in the training data. One of the cases of considering 10 blocks as testing data is shown in Table 1 and it shows the probability occurrence of first digits. These blocks are randomly chosen from the training data.

The quantitative analysis is done in terms of True Positive (TP), False Positive (FP), True Negative (TN), False Negative (FN), Sensitivity or True Positive Rate (TPR), False Positive Rate (FPR), Accuracy, F-measure and Matthews Correlation coefficient (MCC). The evaluated results are shown in the table 2. So to evaluate the capability of the proposed method we process the TPR, F-measure, Accuracy and MCC.

Table 1: An example of occurrence of first digits in 10 blocks of authentic and spliced images.

First Digits	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Block 1	39	19	6	12	8	8	7	5	7
Block 2	55	21	12	8	7	7	4	5	5
Block 3	30	26	19	11	7	10	5	4	5
Block 4	71	32	23	21	13	11	5	13	8
Block 5	47	28	21	16	12	4	10	12	5
Block 6	19	10	7	7	4	7	2	1	3
Block 7	40	24	22	12	10	13	9	6	5
Block 8	24	17	14	10	6	1	6	4	5
Block 9	39	21	20	7	3	6	1	3	5
Block 10	39	23	26	10	14	5	7	9	8

Table 2: Comparison of various parameters

Cases	TP	FP	TN	FN	TPR	FPR	Accuracy	F-measure	MCC
Case1	5	0	4	1	0.83	0	0.90	0.90	0.82
Case2	5	0	4	1	0.83	0	0.90	0.90	0.82
Case1	4	1	5	0	1.00	0.17	0.90	0.89	0.82
Case2	4	1	5	0	1.00	0.17	0.90	0.89	0.82
Case1	4	1	4	1	0.80	0.20	0.80	0.80	0.60
Case2	4	1	4	1	0.80	0.20	0.80	0.80	0.60
Case1	3	2	5	0	1.00	0.29	0.80	0.75	0.65
Case2	3	2	5	0	1.00	0.29	0.80	0.75	0.65
Case1	4	1	5	0	1.00	0.17	0.90	0.89	0.82
Case2	4	1	5	0	1.00	0.17	0.90	0.89	0.82
Case1	5	0	4	1	0.83	0	0.90	0.91	0.82
Case2	5	0	4	1	0.83	0	0.90	0.91	0.82
Case1	3	2	5	0	1.00	0.29	0.80	0.75	0.65
Case2	3	2	5	0	1.00	0.29	0.80	0.75	0.65

The accuracy rate of Case 1 and Case 2 is 85.71% each. The F-measure evaluated by our proposed method in Case 1 and Case 2 is 0.84.The MCC score is 0.74 for Case 1 and Case 2. Hence, the average F-measure, MCC, and Accuracy of our method is 0.84, 0.74 and 85.71% respectively as shown in table 3.

Table 3: Detection results as compared to previous methods

Methods	F-measure	MCC	Accuracy
Proposed	**0.84**	**0.74**	**85.71%**
[13]	0.61	0.48	-
[17]	-	-	99.5%
[18]	-	-	98.33%
[19]	0.51	0.39	-
[24]	0.45	0.21	-
[25]	0.53	0.35	-
[26]	0.47	0.23	-
[27]	0.52	0.41	-
[28]	0.57	-	-
[29]	-	-	76.52%
[30]	-	-	82.32%
[31]	-	-	80.58%

VI. CONCLUSION

In the proposed technique, detection of Splicing forgery has been proposed. This technique is based on the consideration of local interactions between noise channels. Local noise based features are compared over small regions of a test image to determine the forgery. The features are obtained using Benford‟s law by taking first digits of DCT coefficients, which are further provided to the SVM classifier for training and then classification of the region of interest as forged. Our technique has produced better results in comparison to the existing techniques. In future, further research may be done for automatic detection of forged pixels in an image, and accuracy of the proposed method can be improved. Technique may be further extended to detect forgery in heavily compressed images.

REFERENCES

[1] C. Kaur and N. Kanwal, "An Analysis of Image Forgery Detection Techniques," vol. 7, no. June, pp. 486–500, 2019, doi: 10.19139/soic.v7i2.542.

[2] A. Piva, "An Overview on Image Forensics," vol. 2013, 2013.

[3] S. K. Mankar and P. A. A. Gurjar, "Image Forgery Types and Their Detection : A Review," vol. 5, no. 4, pp. 174–178, 2015.

[4] H. Farid, "Creating and Detecting Doctored and Virtual Images : Implications to The Child Pornography Prevention Act," no. 2000.

[5] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey," *Digit. Investig.*, vol. 10, no. 3, pp. 226–245, 2013, doi: 10.1016/j.diin.2013.04.007.

[6] K. Asghar, Z. Habib, and M. Hussain, "Copy-move and splicing image forgery detection and localization techniques : a review," *Aust. J. Forensic Sci.*, vol. 0618, pp. 1–27, 2017, doi: 10.1080/00450618.2016.1153711.

[7] J. Lukáš and J. Fridrich, "Estimation of Primary Quantization Matrix in Double Compressed JPEG Images."

[8] J. Goo, H. Tae, H. Park, Y. Ho, M. Il, and K. Eom, "Quantization-based Markov feature extraction method for image splicing detection," *Mach. Vis. Appl.*, 2018, doi: 10.1007/s00138-018-0911-5.

[9] S. Milani, M. Tagliasacchi, S. Tubaro, S. Milani, M. Tagliasacchi, and I. Processing, "APSIPA Transactions on Signal and Information Processing Transactions on Signal and Information Processing : Discriminating multiple JPEG compressions using fi rst digit features Discriminating multiple JPEG compressions," no. December 2014, pp. 0–10, 2015, doi: 10.1017/ATSIP.2014.19.

[10] X. Pan, "Exposing Image Forgery with Blind Noise Estimation," pp. 15–20, 2011.

[11] "TOWARDS LEARNED COLOR REPRESENTATIONS FOR IMAGE SPLICING DETECTION Benjamin Hadwiger , Daniele Baracchi † , Alessandro Piva † , Christian Riess urnberg Dipartimento di Ingegneria dell ' Informazione , Universit `," pp. 8281–8285, 2019.

[12] T. Ng, S. Chang, and Q. Sun, "Blind detection of photomontage using higher order statistics," 1845.

[13] R. Salloum, Y. Ren, and C. J. Kuo, "Image Splicing Localization Using A Multi-Task Fully Convolutional Network (MFCN) arXiv : 1709 . 02016v1 [cs . CV] 6 Sep 2017," pp. 1–19, 2017.

[14] A. M. Das and S. Aji, *A Fast and Efficient Method for Image Splicing Localization Using BM3D Noise Estimation*. Springer Singapore.

[15] N. Thanh, P. J. Lee, and G. K. C. Park, "Efficient image splicing detection algorithm based on markov features," 2018.

[16] P. S. Abhijith and P. Simon, *Improved Blurred Image Splicing Localization with KNN Matting*. Springer Singapore, 2019.

[17] A. K. Jaiswal and R. Srivastava, "A technique for image splicing detection using hybrid feature set," *Multimed. Tools Appl.*, vol. 79, no. 17–18, pp. 11837–11860, 2020, doi: 10.1007/s11042-019-08480-6.

[18] N. Y. Hussien, R. O. Mahmoud, and H. H. Zayed, "Deep learning on digital image splicing detection using cfa artifacts," *Int. J. Sociotechnology Knowl. Dev.*, vol. 12, no. 2, pp. 31–44, 2020, doi: 10.4018/IJSKD.2020040102.

[19] C. Destruel, V. Itier, O. Strauss, and W. Puech, "Color noise-based feature for splicing detection and localization," *2018 IEEE 20th Int. Work. Multimed. Signal Process.*, pp. 1–6.

[20] J. A. Redi, W. Taktak, and J. Dugelay, "Digital image forensics : a booklet for beginners," no. October 2010, pp. 133–162, 2011, doi: 10.1007/s11042-010-0620-1.

[21] B. Patil, M. E. Student, S. Chapaneri, and D. Jayaswal, "Improved Image Splicing Forgery Localization with First Digits and Markov Model Features," 2017.

[22] "DETECTING IMAGE SPLICING USING GEOMETRY INVARIANTS AND CAMERA CHARACTERISTICS CONSISTENCY Department of Electrical Engineering Columbia University."

[23] P. O. Box, "CASIA IMAGE TAMPERING DETECTION EVALUATION DATABASE Jing Dong , Wei Wang and Tieniu Tan Institute of Automation , Chinese Academy of Sciences," pp. 422–426, 2013.

[24] D. Cozzolino, G. Poggi, and L. Verdoliva, "Splicebuster: A new blind image splicing detector," *2015 IEEE Int. Work. Inf. Forensics Secur. WIFS 2015 - Proc.*, no. November, 2015, doi: 10.1109/WIFS.2015.7368565.

[25] S. Lyu, X. Pan, and X. Zhang, "Exposing Region Splicing Forgeries with Blind Local Noise Estimation," *Int. J. Comput. Vis.*, vol. 110, no. 2, pp. 202–221, 2013, doi: 10.1007/s11263-013-0688-y.

[26] P. Ferrara, T. Bianchi, A. De Rosa, A. Piva, and S. Member, "Image Forgery Localization via Fine-Grained Analysis of CFA Artifacts," vol. 7, no. 5, pp. 1566–1577, 2012.

[27] B. Mahdian and S. Saic, "Using noise inconsistencies for blind image forensics," *Image Vis. Comput.*, vol. 27, no. 10, pp. 1497–1503, 2009, doi: 10.1016/j.imavis.2009.02.001.

[28] J. V. C. I. R, C. Pun, B. Liu, and X. Yuan, "Multi-scale noise estimation for image splicing forgery detection q," *J. Vis. Commun. Image Represent.*, vol. 38, pp. 195–206,

2016, doi: 10.1016/j.jvcir.2016.03.005.
[29] J. Dong, W. Wang, T. Tan, and Y. Q. Shi, "Run-Length and Edge Statistics Based Approach for Image Splicing Detection Run-length and edge statistics based approach for image splicing detection," no. April 2014, pp. 0–12, 2008, doi: 10.1007/978-3-642-04438-0.
[30] W. Chen, Y. Q. Shi, and W. Su, "Image splicing detection using 2-D phase congruency and statistical moments of characteristic function," vol. 6505, pp. 1–8, 2017.
[31] Z. He, W. Sun, W. Lu, and H. Lu, "Digital image splicing detection based on approximate run length," *Pattern Recognit. Lett.*, vol. 32, no. 12, pp. 1591–1597, 2011, doi: 10.1016/j.patrec.2011.05.013.

Author Profile

Amandeep Kaur received the B.E. degrees in Computer Science and Engineering in 2016. My areas of interest are image processing, machine learning.

Navdeep Kanwal is currently working at department of Computer Science and Engineering at Punjabi University Patiala. Skills and Expertise are Video Processing, Image Processing, Signal Processing.

Dr. Lakhwinder Kaur is currently working at department of Computer Science and Engineering at Punjabi University Patiala. Skills and Expertise are Video Processing, Image Processing, Signal Processing.