A New RGB based Fusion for Forged IMEI Number Detection in Mobile Images

[1]Palaiahnakote Shivakumara, [2]V. Basavaraja, [2]Harsha S. Gowda, [2]D. S. Guru, [3]Umapada Pal and [4]Tong Lu

[1]Faculty of Computer System and Information Technology, University of Malaya, Kuala Lumpur, Malaysia.
Email: shiva@um.edu.my.
[2]Department of Studies in Computer Science, University of Mysore, Mysore, Karnataka, India.
Email: basavarajavyadav@gmail.com, harshasgmysore@gmail.com, dsguruji@yahoo.com.
[3]Computer Vision and Pattern Recognition Unit, Indian Statistical Institute, Kolkata, India. Email: umapada@isical.ac.in.
[3]National Key Lab for Novel Software Technology, Nanjing University, Nanjing, China. Email: lutong@nju.edu.cn

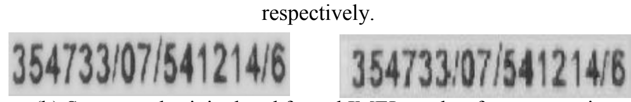
***Abstract*—As technology advances to make living comfortable for people, at the same time, different crimes also increase. One such sensitive crime is creating fake International Mobile Equipment Identity (IMEI) for smart mobile devices. In this paper, we present a new fusion based method using R, G and B color components for detecting forged IMEI numbers. To the best of our knowledge, this is the first work for forged IMEI number detection in mobile images. The proposed method first finds variances for R, G and B images of a forged input image to study local changes. The variances are used to derive weights for respective color components. The same weights are convolved with respective pixel values of R, G and B components, which results in the fused image. For the fused image, the proposed method extracts features based on sparsity, the number of connected components, and the average intensity values for edge components in respective R, G and B components, which gives six features. The proposed method finds absolute difference between fused and input images, which gives feature vector containing six difference values. The proposed method constructs templates based on samples chosen randomly. Feature vectors are compared with the templates for detecting forged IMEI numbers. Experiments are conducted on our own dataset and standard datasets to evaluate the proposed method. Furthermore, comparative studies with the related existing methods show that the proposed method outperforms the existing methods.**

***Keywords*—IMEI number, Color spaces, Fusion, Template mathcing, Forgery detection.**

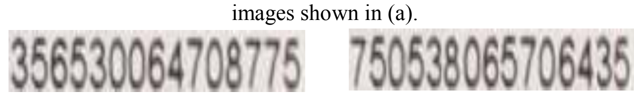
I. INTRODUCTION

In the recent days, new software technologies have been developed to improve living styles of people in the world. At the same time, the same technologies are used for committing crimes, which are also increasing [1]. One such crime is tampering International Mobile Equipment Identity (IMEI) of mobile devices to smuggle and mislead investigation. Example of IMEI numbers are shown in Fig. 1(a), which are marked by green and red color rectangles. In general, skilled persons use advanced software for performing copy-paste or insertion operation to generate fake IMEI numbers as shown in Fig. 1(a), where one can see the original IMEI numbers marked by the green rectangle are copied and pasted on another mobile marked by the red color rectangle. The segmented genuine and forged IMEI number images from Fig. 1(b) are shown in Fig. 1(b), respectively, where we can notice that it is hard to differentiate original and fake IMEI number images with naked eyes. Similarly, one more example for generating fake IMEI numbers by insertion operation is shown in Fig. 1(c), where it is noted that a few numerals are inserted using advanced software. It is observed from Fig. 1(b) and Fig. 1(c) that generated fake IMEI and original numbers appear similar in naked eyes. As a result, tracing lost mobiles through IMEI unique numbers has become hard and challenge for crime branches. Therefore, it is a hot issue for crime police and it is essential to developed system for such crime detection.

(a) Mobile with original and forged IMEI numbers created by copy-paste operation are marked by green and red color, respectively.



(b) Segmented original and forged IMEI number from respective images shown in (a).



(c) Original and forged IMEI number created by insertion operation.

Fig. 1. Illustration for creating forged IMEI numbers using original IMEI numbers printed on mobile images.

Forgery detection is not a new problem in the field of image processing and computer vision, where one can see many methods for video and general images [2, 3]. However, the scope of the methods is limited to video and general images but not specific forged IMEI number images. Similarly, a few methods addressed the issue of forged text detection in video images, which consider caption texts (edited or superimposed texts) as tampered ones for forgery text detection [4-8]. Though the methods consider text images for forged text detection, it is not sure that how the methods perform for forged IMEI number detection in mobile images. In addition, low contrast, small font and limited digit information make the problem more challenging and interesting in contrast to forged text detection methods [4-8]. Therefore, there is a need for developing a new method for forged IMEI number detection.

978-1-5386-5875-8/18/$31.00 ©2018 IEEE
DOI 10.1109/ICFHR-2018.2018.00074

Since there is no work reported in literature for forged IMEI number detection, we review the methods on fraudulent document detection from document point of view, forgery detection through printer identification and caption text (tampered text in video) detection as these are related methods for the proposed work. Kumar et al. [9] proposed detection of fraudulent alternation in ball point pen strokes. This method explores color and texture features for handwritten documents, especially for bank cheques. Raghunandan et al. [10] proposed Fourier coefficients for fraud handwritten document classification through age analysis. This method studies positive and negative coefficients for analyzing image quality and identifying fraud documents. These methods are limited to handwritten documents but not forged IMEI printed number detection in mobile images. However, recently, Wang et al. [11] proposed a Fourier-residual method for fake printed text detection through printer identification. This method extracts features from residual given by Fourier transform for printer identification. However, the primary goal of this method is to identify printers but not forgery in images. Since the features extracted in the above-mentioned methods are sensitive to character shapes and quality of document images, the same method may not work well for IMEI numbers in mobile images.

In the same way, we also review the methods on caption and scene text separation in video images. Shivakumara et al. [4] proposed the separation of graphics and scene texts in video frames based on the combination of Canny and Sobel edge images along ring radius transform. The performance of the method depends on edge quality. Xu et al. [5] proposed a method for classifying graphics and scene texts by exploring temporal information. However, the method requires full text lines for achieving better results. Roy et al. [6] proposed tampered features for the classification of caption and scene texts. In this method, DCT coefficients are explored to detect tampered information in caption images such that it can be separated from scene texts. In the similar way, Bhardwaj et al. [7] explored tampered features, which represent superimposed texts in video for text detection by separating scene texts from caption ones. Recently, Roy et al. [8] proposed temporal integration for word-wise caption and scene text identification. This method explores temporal information for achieving good results. The main focusses of the method is to classify caption and scene texts in normal video but not forged IMEI number detection in mobile images. Therefore, we can assert that the methods may not perform well for IMEI number images.

It is observed from the above review that most methods consider texts either handwritten, printed or those in video images for forged text detection. None of the methods considers numerals such as IMEI numbers and alpha numerals for forgery detection. In addition, since the above methods consider texts from document or video images, one can expect reasonable font size. In case of IMEI numbers in mobile images, one cannot expect big font as shown in Fig. 1(a). As a result, there are high chances of losing vital information for the above-mentioned methods. Therefore, forged IMEI number detection in mobile images is still a research issue.

Hence, in this work, we focus on forged IMEI number detection in mobile images. It is true that when a text is forged with some operations such as copy-paste and insertion, one can expect some disturbance in the content of the forged image compared to the original one [2, 3]. Based on this observation, inspired by the method [12] where fusion concept has been introduced by studying variations at wavelet decomposition levels for assessing the quality of medical images, we explore the same fusion concept using R, G and B color components through local variations in this work. We believe that studying local variations in R, G and B of the input images help us to extract the difference, which represents forgery caused by some operations. The differences are extracted by estimating the sparsity count of connected components and the average intensity in Canny and Sobel edge images of input and fused images. Therefore, the main contribution here is exploring fusion concept using R, G and B color components and extracting features from fused images for fake IMEI number detection in mobile images.

(a) Original and forged IMEI number images with copy-paste operation

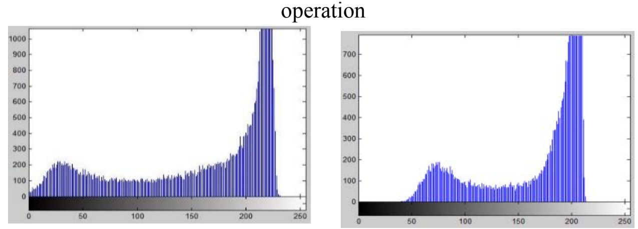

(b) Histogram for the gray values of respective images in (a).

Fig. 2. Distributions of gray pixel values for the original and forged IMEI number images shown in (a).

II. Proposed Methodology

As discussed in the Introduction Section, it is fact that when a forged image is created by operation using any software, the operations introduces distortion at pixel level. It is evident from the illustration shown in Fig. 2, where we perform histogram operation for gray pixels in the original and forged images in Fig. 2(a) as shown in Fig. 2(b). It is observed from Fig. 2(b) that pixel distribution of the original and forged images is different especially for the number of low and high values in the distribution of forged images, which are reduced compared to the distribution of the original image. This is valid because distortion introduced by the operations hinders image quality. As quality deteriorates, the values of pixels reduce. This cue motivated us to propose a method for forged IMEI number image detection in mobile images in this work.

In this work, the segmented original and forged IMEI numbers from mobile images are considered as input for forged image detection. In order to study local variations in details, we propose to divide each color input image into R, G and B components as it helps in extracting minute changes in the content. Inspired by the method [12] where fusion concept has been proposed for studying the quality of medical images of different contrasts with the help of decomposition levels in wavelet domain, we propose to explore the same fusion for the

R, G and B components of the input image in this work. It is noted that when there is no distortion in the input image as the original input one, one can expect the fused image with the same quality or little effect due to operations compared to the input image. On the other hand, for the forged input image, we can expect a fused image with sever effect due to operation in the form of background noisy components and loss of information compared to the input forged image. To extract such observation, the proposed method finds variances in R, G and B and then derives weighs for respective R, G and B components. The weights are convolved with the values of respective input R, G and B images, which gives a fused image. To study the effect of poor and high quality, the proposed method obtains Canny and Sobel edge images for the fused image. It is noted that since Canny does not depend on gradient, it gives fine details for both good and poor quality images, while since Sobel depends on gradient, it gives fine details for good quality images and poor quality images with loss of edges or disconnections. Therefore, we prefer Canny and Sobel for studying quality effect for the fused original and forged images.

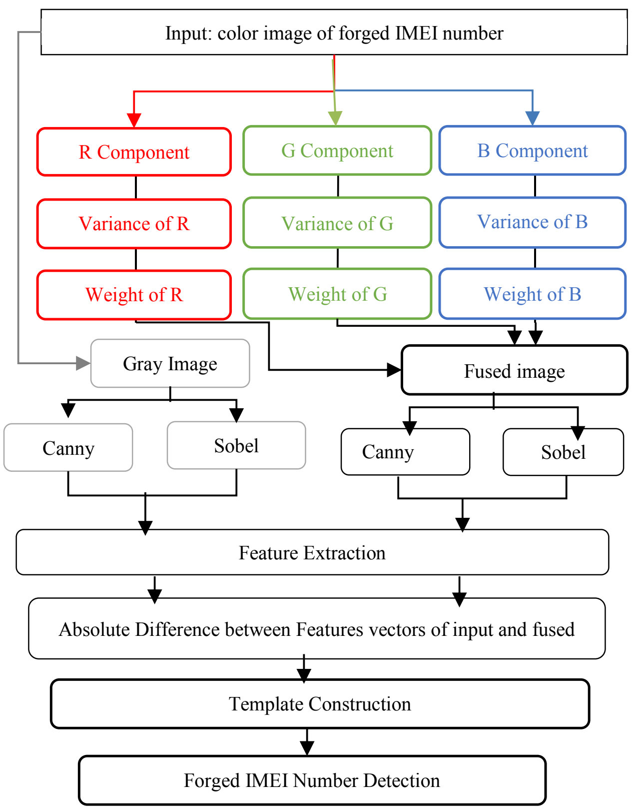
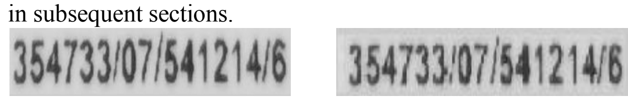


Fig. 3. Block diagram of the proposed method.

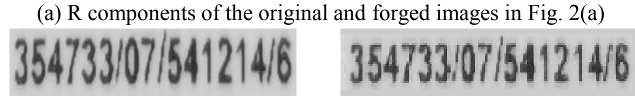
To extract the effect of loss of edges, noisy components, disconnections and low values due to fusion and forgery operations, the proposed method estimates sparsity count, the number of connected edge components, and the average intensity values of edge components, which results in features. Furthermore, the proposed method finds the absolute difference between the features of the fused image and the input image, which results in feature vectors for forged image detection. The whole framework of the proposed method is shown in Fig. 3, where we can see templates are created for the final forged IMEI number detection.

A. Constructing Fused Image using Color Components

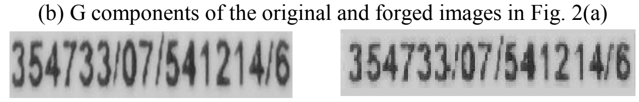
For the input image shown in Fig. 2(a), the proposed method obtains R, G and B components as shown in Fig. 4(a)-Fig. 4(c), respectively. It is noted from Fig. 4(a)-Fig. 4(c) that it is hard to notice the differences between the original and the forged images in different spaces. For each component, the proposed method calculates variance *Var* in row and column wise as defined in Equation (1). The variances of R, G and B are used for deriving weights for respective R, G and B as defined in Equation (2). Finally, the fusion image *S* is estimated by convolving weights with pixels values of the respective of R, G and B components as defined in Equation (3). The effect of fusion using variances and weights of R, G and B is shown in Fig. 4(d), where if we look at closely, the sharpness at edges is reduced for fused forged images compared to fused original images. Similarly, we can see noisy pixels for background of the fused original image compared to the fused forged image. This observation motivates us to extract the quality difference between the original and forged images, which will be discussed in subsequent sections.



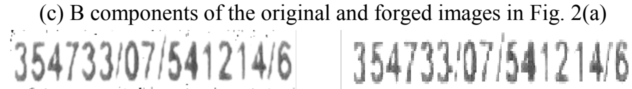
(a) R components of the original and forged images in Fig. 2(a)



(b) G components of the original and forged images in Fig. 2(a)



(c) B components of the original and forged images in Fig. 2(a)



(d) Fused images for respective original and forged images

Fig. 4. Generating of fused images using R, G and B components for the original and forged IMEI number images.

$$Var_K = \sqrt{(RF)^2 + (CF)^2} \quad (1)$$

$$RF = \sqrt{\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=2}^{N}[F(i,j) - F(i,j-1)]^2}$$

$$CF = \sqrt{\frac{1}{MN}\sum_{j=1}^{N}\sum_{i=2}^{M}[F(i,j) - F(i-1,j)]^2}$$

where *k* denotes R, G, B, RF and CF denote variances computed in row and column wise, respectively. F denotes input image, M and N denote the number of row and columns respectively for the window of size 3×3.

$$W_K(x,y) = \frac{Var_K(x,y)}{Var_R(x,y) + Var_G(x,y) + Var_B(x,y)} \quad (2)$$

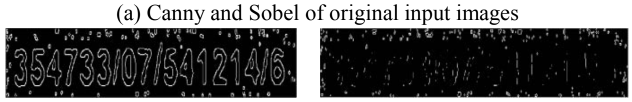
$$S(x,y) = f_R(x,y) * W_R(x,y) + f_G(x,y) * W_G(x,y) + f_B(x,y) * W_B(x,y) \quad (3)$$

Where W denotes weights of R, G, and B components, respectively, and S denotes Fusion of Weight(W_k) with corresponding color components(f_k).

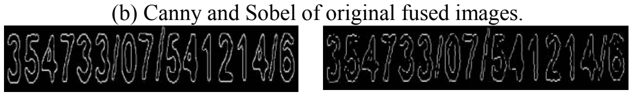
B. Feature Extraction for Forged IMEI Number Detection

As mentioned in the Proposed Methodology Section and the previous section, the proposed method obtains Canny and Sobel edge images for the original-forged input image and original-forged fused images as shown in Fig. 5(a)-Fig. 5(d). It can be seen from Fig. 5(a) and Fig. 5(b) that despite Canny gives fine edges for characters, it also gives noisy pixels for background. At the same time, Sobel loses character shapes for the fused original image. However, Fig. 5(c) and Fig. 5(d) show that for forged input images, Canny gives more noisy edges along with fine edges of characters compared to the original fused image as shown in Fig. 5(b). Note that Sobel gives severe loss of shapes and edges for the fused forged image compared to the original fused image. As a result, one can guess that the difference between Canny original input and its fused version is higher than that between Canny forged input and its fused images. The same conclusion can be drawn from the Sobel of original-forged input and fused images.

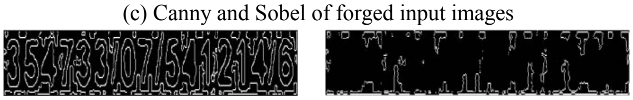
(a) Canny and Sobel of original input images



(b) Canny and Sobel of original fused images.



(c) Canny and Sobel of forged input images



(d) Canny and Sobel of fused forged images.

Fig. 5. Canny and Sobel edge components for original-forged input and fused images.

In order to extract the above reflections in the content of input and fused images of the original and forged images, we propose to estimate the Sparsity Count (SP), Number of Connected Components (CC), and Average Intensity values (AI). The proposed method first finds the centroid for the whole edge image and then counts the number of zeros between the centroid and all the white pixels in edge images as defined in Equation (4). Similarly, to extract the property of loss of edges and additional noisy components in edge images, the proposed method counts the number of connected components in edge images as defined in Equation (5). It is true that when the quality differs, it affects directly for intensity values, which leads to low intensity pixel values. The proposed method computes the average of intensity values of edge pixels in images as defined in Equation (6). This results in three features, namely, *SPc*, *CCc* and *AIc* with respect to Canny edge images and three more, namely, *SPs*, *CCs* and *AIs* with respect to Sobel edge images, which gives a feature vector having six features.

To extract the above distinct property between the original and forged images, the proposed method computes the absolute difference between feature vector of the input and fused images for both the original and forged images. Let *ISPc*, *ISPs*, *ICCc*, *ICCs*, *IAIc*, *IAIs*, and *FSPc*, *FSPs*, *FCCc*, *FCCs*, *FAIc*, *FAIs* be the counts of *SP*, *CC*, *AI* of input images with respect to Canny and Sobel, and fused images with respect to Canny and Sobel edge images, respectively. The absolute difference between the input and fused images, say, *CD1*, *CD2*, *CD3*, *SD1*, *SD2*, *SD3* are calculated as defined in Equation (7), which gives feature vector containing six difference values. As per experiments, it is noted that the proposed feature vector gives clear difference between the original and forged images. Therefore, we calculate the average of feature vectors for 50 images chosen randomly from respective sets of the original and forged images of our database. This is considered as templates for a set of original and forged images as shown in Fig. 6 for separating forged IMEI number images from the original images. It is noticed from the templates in Fig. 6 that higher values for original images and lower values for forged images. This is due to the loss of information in case of forged images and more noisy components in case of the original images.

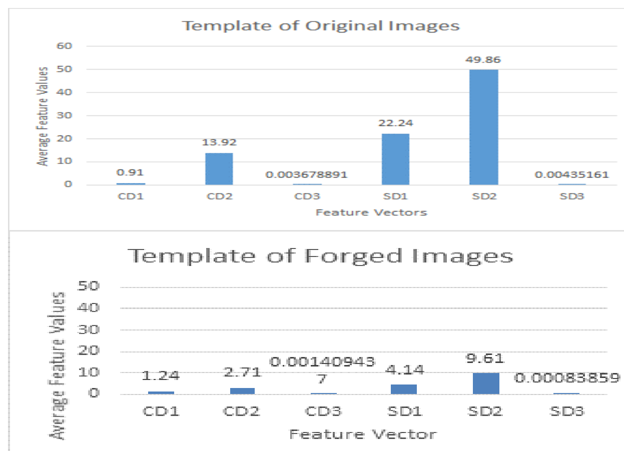


Fig. 6. Templates construction for average feature vectors of original and forged images.

$$SP = \begin{cases} S+1 & \textit{if no white pixel in the path} \\ 0 & \textit{otherwise} \end{cases} \quad (4)$$

$$CC = \begin{cases} C+1 & \textit{if a edge componet is connected} \\ 0 & \textit{otherwise} \end{cases} \quad (5)$$

$$AI = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} f(i,j) \quad (6)$$

Where *SP* denotes sparsity count, *CC* denotes connected component count, *AI* denotes average intensity, *M*, *N* denote the number of row and columns of the image and *f*(*i*, *j*) is image.

$$CD1 = |ISPc - FSPc|,\ CD2 = |ICCc - FCCc|,$$
$$CD3 = |IAIc - FAIc|,\quad SD1 = |ISPs - FSPs|, \quad (7)$$

$$SD2 = |ICCs - FCCs|, \;\; SD3 = |IAIs - FAIs|$$

III. Experimental results

Since the proposed forged IMEI number detection is the first work as per our knowledge, we create our own dataset by segmenting IMEI number manually from different mobile images. The segmented IMEI number is used for creating forged IMEI numbers with the help of Adobe Photoshop. For creating fake IMEI numbers, we use the popular operation called copy-paste and insertion [2, 3] as discussed in the Introduction Section. IMEI numbers in a mobile image are copied and pasted onto another mobile image. Similarly, we perform insertion operation to edit the original numbers, replace the original numbers with new numbers, and delete numbers. A number which, involves the above operation is considered as forged data, otherwise, it is considered as the original data. As experienced, creating fake images is not easy because it needs background color correction, choosing suitable font, font size and shape, which appear the same as the original. Therefore, the created dataset contains 100 original and 100 forged images for experimentation.

To prove the effectiveness of the proposed method, we consider standard datasets, namely, datasets of Roy et al. [6] and Bharadwaj et al. [7], which consist of caption and scene texts in video for evaluation. In these datasets, caption text is considered as forged one because it is edited (superimposed text) while scene text is considered as the original text because it is a part of an image. Since IMEI numbers appear the same as caption and scene texts except numerals and characters, we believe the considered above two datasets are the benchmark for evaluating the effectiveness of the proposed method. Roy et al.'s [6] dataset consists of 500 caption and 500 scene texts. Bharadwaj et al.'s [7] dataset consists of 150 low resolution (Set-1) and 150 high-resolution images (Set-2). This dataset is used to test the ability of the proposed method to work on both low and high-resolution images. Note that Bharadwaj et al.'s dataset does not provide scene texts because its main objective is to detect only caption texts by extracting tampered features of caption texts in video. Overall, we consider 1500 images for experimentation, which includes 200 from our dataset, 1000 from Roy et al. and 300 from Bharadwaj et al.

To show the superiority to existing methods, we implement the following state-of-the-art methods for comparative study. Roy et al. [6] proposed a method for caption and scene text classification based on DCT coefficients. This method extracts tampered features of caption texts by studying DCT coefficients. Bharadwaj et al. [7] proposed a method for detecting caption texts in video by exploring tampered features in compress domain. Kumar et al. [9] proposed a method for fraudulent document detection by studying color and texture features for forged handwritten texts. The main reason to consider the above three methods for comparative study is that the primary objective of the above methods is to use distortion created by forgery as the main basis for developing methods. In addition, Roy et al. use frequency domain for forged text detection, Bharadwaj et al. use compress domain for forged text detection, and Kumar et al. use color and texture features for forged text detection. However, the proposed method uses fusion concept and statistical features of edge components for forged text detection.

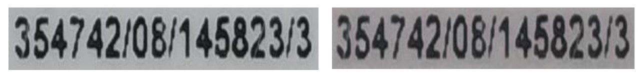
To evaluate the performance of the proposed and existing methods, we use standard measures, namely, Recall (R), Precision (P) and F-measure (F) as defined in Equation (8)-Equation (10).

$$P = \frac{T_p}{T_p + F_p} \tag{8}$$

$$R = \frac{T_p}{T_p + F_n} \tag{9}$$

$$F = 2 * \frac{P * R}{P + R} \tag{10}$$

Here, T_p signifies the total number of correctly detected forged images, F_p signifies the total number of the original images mistakenly detected as forged, and F_n is the total number of forged images, which are incorrectly missed.



(a) Original and forged samples images of our dataset with copy-paste operation

(b) Original (scene) and forged (caption) images of Roy et al. [6] dataset.

(c) Forged images (caption text) of low and high resolution of Bharadwaj et al [7] dataset.

Fig. 7. Sample successful results of the proposed method

Sample original and forged images of each database are shown in Fig. 7, where it can be seen that the proposed method detects original and forged images successfully for different datasets. It is observed from Fig. 7 that the proposed method is robust to low and high resolutions, low and high contrast and blur. More important is that the proposed method works well irrespective of content such as numeral, character, font, font size and color. This is because the proposed method does not involve any content specific features for forged text detection. Therefore, we can conclude that the proposed method is generic in nature and can be extended to texts of different scripts, handwritten, signatures, etc. The quantitative results of the proposed and existing methods are reported in Table I, Table II and Table III for our dataset, Roy et al.'s and Bharadwaj et al.'s datasets, respectively. It is observed from Table I, II and Table III that the proposed method is better than the existing methods for all the datasets except Roy et al.'s dataset. Besides, the proposed method scores consistent results for all the three different datasets. However, for Roy et al.'s dataset, Roy et al.'s method scores the best recall for the original images but it is the worst at precision compared to the propose method. The main reason of the existing method for poor results on our dataset and other dataset is that the methods proposed content specific features and the methods are limited to mixed characters and numeral but not alone numerals. On the other hand, as mentioned in the above, the proposed method uses generic features for forged text detection. When we compare the results among the different existing methods, Kumar et al.'s method scores poor results as its scope is limited to handwritten but not texts in video and mobile images. However, Roy at al.'s and Baharawaj et al.'s methods are developed for forged text detection in video. Hence, we can conclude that the proposed method outperforms the existing methods.

Table I. Performance of the proposed and existing methods on our dataset (IMEI number).

Methods	Original			Forged		
	R	P	F	R	P	F
Proposed	**0.73**	**0.82**	**0.77**	**0.85**	**0.75**	**0.80**
Roy et al. [6]	0.67	0.64	0.65	0.63	0.65	0.64
Bhardwaj [7]	0.58	0.60	0.59	0.62	0.59	0.60
Kumar et al. [9]	0.43	0.42	0.42	0.41	0.41	0.41

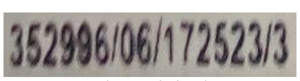
Table II. Performance of the proposed and existing methods on Roy et al. [6] dataset (Caption and Scene text)

Methods	Original (scene)			Forged (caption)		
	R	P	F	R	P	F
Proposed	0.54	**0.96**	0.69	**0.98**	**0.68**	**0.80**
Roy et al. [6]	**0.75**	0.71	**0.73**	0.63	0.68	0.65
Bhardwaj [7]	0.56	0.46	0.51	0.40	0.51	0.45
Kumar et al. [9]	0.55	0.44	0.48	0.39	0.50	0.44

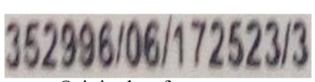
Table III. Performance of the proposed and existing methods on Bharadwaj et al. [7] dataset (Caption of text of low and high resolution)

Methods	Set-1(Low resolution)			Set-2(High resolution)		
	R	P	F	R	P	F
Proposed	**0.73**	**0.70**	**0.72**	**0.80**	**0.74**	**0.76**
Roy et al. [6]	0.62	0.58	0.60	0.66	0.63	0.64
Bhardwaj [7]	0.64	0.62	0.63	0.68	0.65	0.67
Kumar et al. [9]	0.41	0.37	0.39	0.45	0.40	0.43

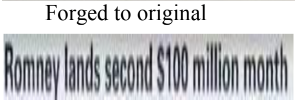
Sometimes, when the input IMEI number or text image are affected by too blur, low contrast and multiple adverse factors, the proposed method fails to detect forged texts correctly as shown in Fig. 8, where we can see misclassified images for each database. Therefore, there is a scope for future work.



Forged to original

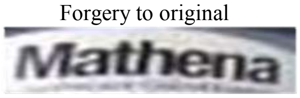


Original to forgery



Forgery to original


Original to forgery



Forged images are misclassified as original (scene text) of Baharadwaj dataset.

Fig. 8. Sample unsuccessful results of the proposed method for different databases. Row-1 andRow-2 denote the sample unsuccessful of our dataset and Roy et al. dataset, respectively.

IV. Conclusion and Future Work

This paper presents a new method for forged IMEI number detection in mobile images. The method explores a new fusion concept through variance and weights estimation for the respective color components, which results in fused images. The features based on sparsity, the number of connected components, and the average intensity of edge components in Canny and Sobel edge images of fused images are proposed. The relationship between the features of fused images and their input images helps us to separate forged IMEI numbers from the original ones. Experimental results on our dataset and two standard datasets along with the comparative study with the existing methods show that the proposed method outperforms the existing methods. Since the proposed concept is generic, it can be extended to other applications in the near future.

Acknowledgment

The work was supported by the Natural Science Foundation of China under Grant No. 61672273 and No. 61272218, the Science Foundation for Distinguished Young Scholars of Jiangsu under Grant No. BK20160021, and Scientific Foundation of State Grid Corporation of China (Research on Ice-wind Disaster Feature Recognition and Prediction by Few-shot Machine Learning in Transmission Lines).

References

[1] C. Chen, J. Ni, Z. Shen and Y. Q. Shi, "Blind forensic of successive geometric transformations in digital images using spectral method: Theory and applications", IEEE Trans. Image Processing, Vol. 26, No. 6, pp 2811-2823, 2017.

[2] C. M. Pun, X. C. Yuan and X. L. Bi, "Image forgery detection using adaptive over segmentation and feature point matching", IEEE Trans. IFS, Vol. 10, No. 8, pp 1705-1716, 2015.

[3] F. Yang, J. Li, W. Lu and J. Weng, "Copy-move forgery detection based on hybrid features", Engineering Applications of Artificial Intelligence, pp 73-83, 2017.

[4] P. Shivakumara, N. V. Kumar, D. S. Guru and C. L Tan, "Separation of graphics (superimposed) and scene text in videos", In Proc. DAS, pp 344-348, 2014.

[5] J. Xu, P. Shivakumara, T. Lu, T. Q. Phan and C. L. Tan, "Graphics and Scene Text Classification in Video", In Proc. ICPR, pp 4714-4719, 2014.

[6] S. Roy, P. Shivakumara, U. Pal, T. Lu and C. L. Tan, "New Tampered Features for Scene and Caption Text Classification in Video Frame", In Proc. ICFHR, pp 36-41, 2016.

[7] D. Bhardwaj, V. Pankajakshan, "Image Overlay Text Detection Based on JPEG Truncation Error Analysis", IEEE Signal Process. Lett. pp 1027-1031, 2016.

[8] S. Roy, P. Shivakumara, U. Pal, T. Lu and A. W. B. A. Wahab, "Temporal integration of word-wise caption and scene text identification", In Proc. ICDAR, pp 350-355, 2017.

[9] R. Kumar, N. R. Pal, B. Chanda and J. D. Sharma, "Forensic detection of fraudulent alterations in ball point pen strokes", IEEE Trans. IFS, Vol. 7, No. 2, pp 809-820, 2012.

[10] K. S. Raghunandan, P. Shivakumara, B. J. Navya, G. Pooja, Navya, N. Prakash, G. H. Kumar. U. Pal and T. Lu, "Fourier coefficients for fraud handwritten document classification through age analysis", In Proc. ICFHR, pp 25-30, 2016.

[11] Z. Wang, P. Shivakumara, T. Lu, M. Basavanna, U. Pal and M. Blumenstein, "Fourier-residual for printer identification", In Proc. ICDAR, pp 1114-1119, 2017.

[12] X. Xu, Y. Wang and S. Chen, "Medical image fusion using discrete fractional wavelet transform", Biomedical Signal Processing and Control, 27, pp 103-111, 2016.