Method for detecting altered text in document images

Indian Institute of Information Technology, Allahabad

Mini Project Report

Abstract- In an era where technology strives to enhance human comfort, the rise of various crimes also poses significant challenges. One such critical offense involves the creation of counterfeit International Mobile Equipment Identity (IMEI) numbers for smart mobile devices. This paper introduces an innovative fusion-based method utilizing the R, G, and B color components to detect forged IMEI numbers. As far as our knowledge extends, this work marks the initial endeavor toward detecting forged IMEI numbers in mobile images.

Moreover, this approach incorporates the utilization of the relationship between positive and negative coefficients of Discrete Cosine Transform (DCT) to discern distortions resulting from tampering. By fusing reconstructed images from respective positive and negative DCT coefficients, the Positive-Negative DCT Coefficients Fusion (PNDF) is attained. Leveraging spatial information, the fusion of R, G, and B color channels in input images yields RGB Fusion (RGBF). The fusion operation is then applied to merge PNDF and RGBF, and the amalgamation of Artificial Intelligence leads to the creation of a fused image from the original input. Extracting features from the fused image using histogram analysis results in a feature vector, subsequently employed for classification via a deep neural network.

Evaluation on our dataset and standard datasets demonstrates the effectiveness of the proposed method. Irrespective of image type, our method showcases superior performance compared to existing methodologies.

1-Introduction

Advancements in software technologies have greatly enhanced the quality of life for people worldwide. However, these very technologies are being exploited for criminal activities, leading to a surge in crimes. One such illicit practice involves tampering with the International Mobile Equipment Identity (IMEI) of mobile devices to deceive investigations and smuggle goods. Skilled individuals utilize sophisticated software to execute operations like copy-paste or insertion, resulting in counterfeit IMEI numbers. Existing methods for forgery detection based on printer identification focus on connected component characteristics but lack robustness in detecting altered text. Altered text detection remains challenging, especially in diverse document types. The need for detection arises from potential disturbances introduced during text alteration, such as distortions, pattern irregularities, or pixel-level content misplacement.

2.Proposed methodology

The proposed method in the base research paper aims to detect forged IMEI numbers in mobile images by analyzing pixel-level distortions introduced during image forgery operations. Utilizing color components (R, G, B), the method calculates variances, derives weights, and fuses the components. Canny and Sobel edge images are obtained to study quality variations. Features, including sparsity count, connected components, and average intensity values, are extracted. The absolute difference between input and fused image features yields a vector for forgery detection. Templates constructed from randomly chosen samples enable the detection of forged IMEI numbers by emphasizing differences in information loss and noisy components. Inspired by this methodology and the use case of Discrete Cosine Transforms (DCT) in the field of forgery detection in document images, our proposed methodology combines RGB color information when obtaining the fused image and DCT coefficients to obtain a fused image from an input image. The fusion combines images in the frequency and spatial domains for feature extraction. Next, histogram-based features are extracted from the fused image. The extracted features are then passed to a deep neural network classifier for detecting altered texts.

In the Positive and Negative DCT Coefficient Fusion (PNDF) process, the method initially applies the Discrete Cosine Transform (DCT) to original and altered images, classifying the coefficients into positive, negative, and zero categories. This classification is depicted in Figs. 3(b), 3(c), and 3(d), respectively. Brightness variations in the top-left and right-bottom corners are observed in the positive and negative coefficients of the original image, with a gradual decrease in brightness. Conversely, altered images exhibit scattered bright pixels. High-frequency coefficients represent edges, low-frequency coefficients represent non-edges, and zero coefficients represent background pixels. The distribution of these coefficients is crucial for distinguishing between original and altered images.

2.1. Data Collection and Preparation

We have used IMEI number Dataset. Forged IMEI number detection provides 500 forged and 500 original images. This dataset, which is captured using mobile phone cameras, is challenging because images contain complex backgrounds compared to the other datasets we used.Overall, 2622 images are considered in our experiments.

Image Preprocessing- We have used Weiner filter to reduce Noise and Blurring. Wiener filter can be used in image processing to remove noise and blur while preserving text details by leveraging frequency-based signal estimation and adaptive filtering. Its effectiveness lies in its ability to differentiate between the signal (text) and noise components and apply filtering based on their respective frequency characteristics.

2.2. Positive and negative DCT coefficient fusion (PNDF)

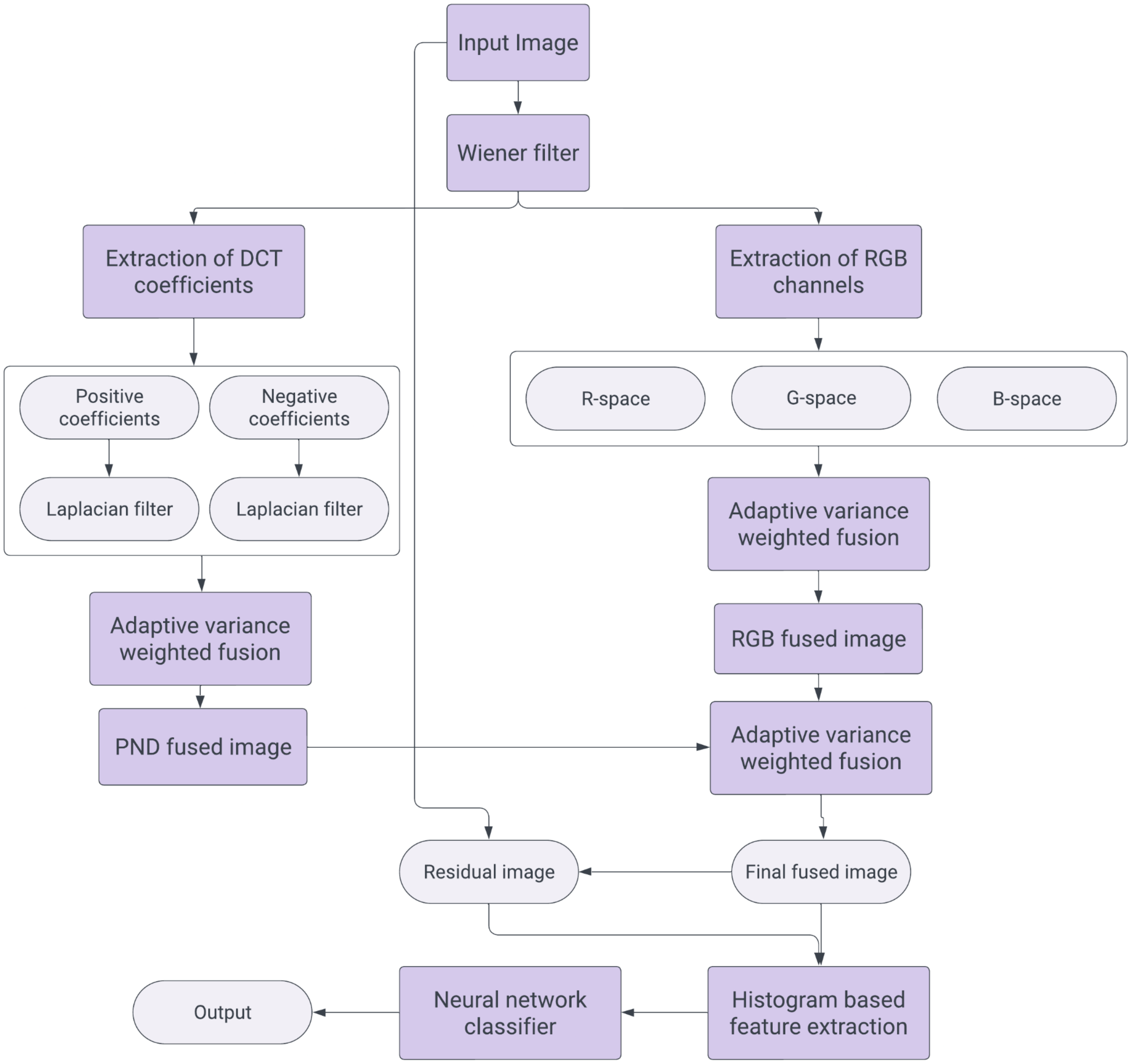
The method then reconstructs images based on the positive and negative coefficients, resulting in brighter representations for the original images compared to altered ones. To enhance differences between original and altered texts, Laplacian filtering is applied separately to positive and negative coefficient images. Inspired by a fusion operation used in medical image enhancement, the method performs a similar fusion operation for the Laplacian-filtered positive and negative coefficients. Before fusion, variances are calculated for each window over the Laplacian-positive and negative images, serving as weights for the fusion process. This fusion, denoted as PNDF, enhances text pixels in original images but does not significantly affect altered text. The fusion operation sharpens text pixels in original images, highlighting differences between original and altered texts. The fusion process effectively enhances text pixels in original images. In contrast, altered images, with randomly changed pixel values, exhibit an impact on variance during fusion. The overall effect is, emphasizing the sharpening of text pixels in original images compared to altered ones.

2.3. RGB color channels fusion (RGBF)

In this study, our objective is to devise a robust method for detecting alterations at the character level, inspired by the importance of color information in forgery detection (Reference 12). We explore the RGB color space to strengthen the previously discussed approach. The proposed method fuses the RGB color space, resulting in a fused image denoted as RGBF. This fusion enhances edges for characters in original images and blurs edges for characters in altered images. Further, the method fuses positive and negative DCT coefficients (PNDF) with RGBF to generate final fused images. A residual image is obtained by subtracting the fused image from the input image. The effectiveness of the fusion operation is highlighted, where histograms are computed for original and altered images, revealing differences in PNDF, RGBF, PNDF+RGBF, and residual images. The proposed method considers each histogram bin as a feature vector, resulting in 75 (50 + 25) feature vectors extracted for detecting altered text in document images.

2.4. CNN for altered text detection

Motivated by the discriminative power of deep neural networks, the 75 extracted feature vectors are input into the neural network depicted in Fig. 7 to detect altered text in document images. The architecture employs the ReLU activation function for all layers, a dropout rate of 0.2 (except in the final layer, which uses the Sigmoid activation), and Batch Normalization in intermediate layers for faster training and improved weight initialization. Using the Adam optimizer with a learning rate of 0.01 and binary cross-entropy loss function, the architecture is trained for 100 epochs with a batch size of 8 (N=8).



3.Literature Review

S.No	Paper title	Year	Methodology used	Accuracy
1	DCT-phase statistics for forged IMEI numbers and air ticket detection	2020	Phase spectrum using the Discrete Cosine Transform (DCT).	70
2	A New RGB Based Fusion for Forged IMEI Number Detection in Mobile Images	2018	Fusion-based approach using R, G and B color components.	64
3	A new forged handwriting detection method based on Fourier spectral density and variation	2019	Using variation in Fourier spectral density	58
4	Automated Forgery Detection in Multispectral Document Images using Fuzzy	2018	Using Fuzzy C-means Clustering	61

	Clustering			
5	Analysis of Copy Move Image Forgery Detection Using Histogram of Orientated Gradient	2018	Automatic Image Forgery detection using HOG	75

3. Experimental results

Methods	IMEI Dataset
Kundu et al[4]	58.0
Wang et al[5]	78.8
Shivakumara et al[2]	84.3
Base Paper[3]	74.8
Proposed Approach	77.45

4.Conclusion

The scope of feedback for the project on Detecting Altered Text in Document Images encompasses various aspects, including technical improvements, user experience enhancements, and considerations for broader deployment. Here are key areas for feedback

1. Technical Accuracy and Performance: - Evaluate the accuracy of the Proposed model in providing relevant and correct answers for unseen data and text Images. But for too blurry and noisy images our model may get confused and this is a challenging part of our work.

2. However, when alteration is done at the text line level instead, the performance degrades. This provides a topic for future research, where we plan to employ context information through the use of natural language models.

5.References

[1] L. Nandanwar et al., "A Conformable Moments-Based Deep Learning System for Forged Handwriting Detection," in IEEE Transactions on Neural Networks and Learning Systems, 2022, doi: 10.1109/TNNLS.2022.3204390.

[2] Nandanwar, Lokesh & Shivakumara, Palaiahnakote & Kanchan, Swati & Basavaraja, Venkappanavara & Guru, Devanur & Pal, Umapada & Lu, Tong & Blumenstein, Michael. (2021). DCT-phase statistics for forged IMEI numbers and air ticket detection. Expert Systems with Applications. 164. 114014. 10.1016/j.eswa.2020.114014.
[3] Shivakumara, Palaiahnakote & Basavaraja, Venkappanavara & Gowda, Harsha & Guru, Devanur & Pal, Umapada & Lu, Tong. (2018). A New RGB Based Fusion for Forged IMEI Number Detection in Mobile Images. 386-391. 10.1109/ICFHR-2018.2018.00074.
[4] Kundu, Sayani & Shivakumara, Palaiahnakote & Grouver, Anaica & Pal, Umapada & Lu, Tong & Blumenstein, Michael. (2020). A New Forged Handwriting Detection Method Based on Fourier Spectral Density and Variation. 10.1007/978-3-030-41404-7_10.
[5] Z. Wang, P. Shivakumara, T. Lu, M. Basavanna, U. Pal and M. Blumenstein, Fourierresidual for printer identi¯cation, in Proc. ACPR (2017), pp. 1114–1119.