Proceedings of the 2nd International Conference on Machine Learning and Automation
DOI: 10.54254/2755-2721/101/20240976

Image splicing detection using integrated LBP and DCT features

Hang Su

School of software, Henan University of Science and Technology, Luoyang, China

211451080624@stu.haust.edu.cn

Abstract. Image splicing is one of the most common techniques used for picture manipulation and forgery. With the advent of user-friendly photo editing software, image splicing has become more prevalent and increasingly difficult to detect. This paper proposes a passive photo splicing detection approach based on Local Binary Patterns (LBP) and Discrete Cosine Transform (DCT) to identify splicing forgeries. The input RGB images are first converted to the YCbCr color space. Subsequently, the chrominance channels, Cb and Cr, are divided into overlapping blocks. Each block's LBP code is then transformed into the DCT domain. For each block, the standard deviation of each DCT coefficient is computed and used as a feature. Support Vector Machine (SVM) is employed as the classifier in a predictive model to determine whether the images have been spliced. To evaluate the proposed approach, two benchmark datasets for photo tampering were utilized. Experimental results indicate that the proposed method outperforms traditional splicing detection techniques in terms of detection accuracy and performance. This enhanced detection capability underscores the potential of combining LBP and DCT features with SVM classification for robust image splicing detection, paving the way for improved digital forensics tools in combating image manipulation.

Keywords: Image Splicing Detection, SVM, LBP, DCT.

1. Introduction

With the increasing usage of electronic devices and advancements in image processing and computer technologies, editing and processing images have become more convenient. Over time, it has become easier to perform and more challenging to detect photo manipulation and forgeries. Despite this, digital photos continue to be widely used in daily life. On one hand, it is now easier than ever to maliciously manipulate digital photographs and spread false information on social media, necessitating users to be more adept at discerning the authenticity of images. On the other hand, ensuring the authenticity of images used for scientific discoveries, courtroom evidence, military intelligence, and similar purposes is critical, as any compromise can have serious repercussions for political and social stability. Consequently, various methods for detecting image tampering and forgery have emerged [1]. Figure 1 illustrates a recent case of image tampering.

Detection techniques for digital photo modification and forgery are broadly classified into active and passive procedures. Active detection approaches involve pre-adding additional information, such as digital watermarks or digital signatures, to photographs to aid detection. However, these methods have significant drawbacks. In contrast, passive detection techniques, also known as blind detection techniques, analyze the properties of digital images without relying on any pre-encoded information or signs. Instead, they assess the image itself to directly determine its validity. Image splicing, the technique of clipping a section from one or more photos and pasting it into a target image without alteration, is a key focus area in passive investigations of digital photo manipulation. This paper proposes a passive detection technique based on learning to identify image splicing forgeries. When images are spliced for forging, sharp edges appear at the boundaries of the pasted region, creating new micro-patterns. This disrupts the local distribution of micro-edge patterns and frequencies. Based on this concept, we propose a method to express such variations using the Discrete Cosine Transform (DCT) and Local Binary Patterns (LBP). Within the LBP domain, discriminative local features are extracted using 2D DCT. Support Vector Machines (SVMs) are then employed for classification.

To demonstrate the effectiveness of the proposed strategy, extensive experiments were conducted on two datasets, with comparisons drawn against several existing techniques. The remaining sections of this paper are structured as follows: Section Two presents related works, Section Three covers the relevant fundamental knowledge, Section Four details the proposed approach, Section Five discusses the experimental analysis, Section Six showcases and discusses the findings, Section Seven compares the proposed method with existing methods, and Section Eight concludes with findings and suggestions for further research..

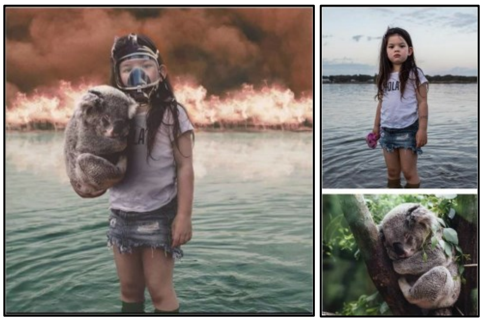

Figure 1. Images related to the Australian bushfire crisis in 2019-2020 (left: spliced image, right: original image) (Photo credit: Original).

2. Related Works

Many passive techniques for detecting picture splicing forgeries have been developed recently. The overview of a few exemplary techniques is given in the paragraphs that follow.

Reference combines an image splicing detection technique centered using Fractal Entropy for Texture Features with an SVM classifier [2]. The accuracy of this technique was 96% on the CASIA TIDE v1.0 [3]. Reference detects picture splicing using a low-dimensional homogeneous feature set generated by principal component analysis [4]. Support vector machines and local binary patterns serve as the foundation for this strategy. Using the Columbia Dataset, the accuracy was 85% [5]. Reference proposes an upgraded Markov features based picture splicing detection method applying SVM to categorization [6]. Using the Columbia Uncompressed Dataset, its approach yielded an accuracy of 94.38% [7]. For a picture splicing detection method centered on LBP and the Illumination-Reflectance model, Reference uses an LDA classifier. Using the CASIA TIDE v2.0, this method's accuracy rate was 94.59% [8].

A technique for detecting picture splicing forgeries based on multi-scale feature priors is presented in Reference [9]. This method combines a feature prior and cyclic residual network module with an external attention mechanism. Using the COLUMBIA, this technique yielded an 88% precision rate. In Reference, an affordable multiscale fusion image-splicing and tamper-detection model is applied [10]. Based on an enhanced MobileNetV2, the suggested Mobile-Pspnet network comprises of a pyramid pooling module and a feature extraction module. The computational complexity and number of parameters are decreased by this approach. On the CASIA dataset and the Columbia Dataset, the precision of this approach was 91% and 96.4%., respectively. All of the above stated approaches differ primarily in how they represent the structural alterations brought about by forgeries. The key to these approaches is how well they capture these shifts. This work presents a method to describe the tampering changes in pictures founded on the incorporation of the DCT and LBP.

3. Relevant Fundamental Knowledge

LBP (Local Binary Pattern) is a texture description approach that represents the local texture qualities of an image by comparing its pixel values with those of its neighboring pixels. The exact phases of LBP are as follows:

Pick the pixel in the middle. Select a circular neighborhood centered on each pixel, with a radius of R. A typical neighborhood dimensions are 3x3.

Review the comparison of the adjacent pixels. Analyze the grayscale values of the P closest neighbors of the center pixel. Mark a pixel as 1 if its grayscale value is more than or equal to the center pixel; if not, mark it as 0. This is the expression for the formula:

$$s(x) = \begin{cases} 0, & x < 0 \\ 1, & x \geq 0 \end{cases} \tag{1}$$

Create the binary blueprint. These defined binary values can be arranged either clockwise or counterclockwise to generate a binary number.

Determine the LBP figure. This binary integer reflects the LBP value of the central pixel; convert it to a decimal number. The following formula may be expressed. The grayscale values of the surrounding pixels are represented by g_p, the center pixel by g_c, and the coordinates of the center pixel by $(x_c\ , y_c)$ [11]:

$$LBP(x_c, y_c) = \sum_{p=0}^{P-1} s\left(g_p - g_c\right) \cdot 2^p \tag{2}$$

Discrete Cosine Transform, or DCT, is mostly utilized for image reduction and feature extraction. It has the ability to convert spatially stored visual data into a frequency domain. The exact phases of DCT are as follows:

Divide the picture into multiple smaller parts, maybe 16 by 16 or 8 by 8.

Apply DCT: Apply DCT to each image block so that the values of the pixels in the domain of space are translated into the frequency domain DCT coefficients.

The following is the formula for one-dimensional DCT:

$$F(u) = \sum_{a=0}^{N-1} f(a) cos\left[\frac{\pi}{N}\left(a + \frac{1}{2}\right)u\right] \tag{3}$$

The following is the formula for two-dimensional DCT:

$$F(u, v) = \frac{1}{4}\alpha(u)\alpha(v) \sum_{a=0}^{N-1} \sum_{b=0}^{N-1} f(a, b) cos\left[\frac{(2a+1)u\pi}{2N}\right] cos\left[\frac{(2b+1)v\pi}{2N}\right] \tag{4}$$

And

$$\alpha(u) = \begin{cases} \frac{1}{\sqrt{2}}, & u = 0 \\ 1, & u \neq 0 \end{cases} \tag{5}$$

$$\alpha(v) = \begin{cases} \frac{1}{\sqrt{2}}, & v = 0 \\ 1, & v \neq 0 \end{cases} \tag{6}$$

Since the low-frequency components hold most of the visual information, use the DCT coefficients from the low-frequency part for choosing features.

4. Techniques for Detecting Image Splicing

This paper's picture splicing detection technique may be broken down into four key steps: (1) Extract the image's chrominance channels by converting the RGB picture to the YCbCr color system. (2) Divide the chrominance channels into multiple blocks. (3) Extract features from each block. (4) Train and predict using an SVM classifier.

Figure 2 displays the suggested method's flowchart.

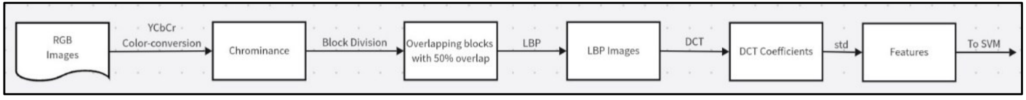

Figure 2. Flowchart (Photo credit: Original).

4.1. Preprocessing the Image

More than any other channel, the chrominance channels are capable of encoding evidence of picture manipulation [12]. Therefore, in this experiment, a color space that is YCbCr is initially created from the RGB picture and the color channels are Cb and Cr. Subsequently, the channels of color Cb and Cr are separated into many picture blocks using extraction.

4.2. Feature Extraction

An picture may be tampered with by splicing it together by copying and pasting the image. The original picture undergoes structural alterations throughout the pasting process. The image's bounds and pasted areas will have different tiny texture patterns, and their edges will have discontinuities. The picture pixels in that area become uncorrelated as a result, and the local frequencies of the image alter [13, 14]. Therefore, the secret to effectively identifying picture alteration is to capture these fundamental changes. LBP is a very useful texture descriptor for images, which may be used to draw attention to and amplify tampering artifacts [15]. Monitoring the alterations in the LBP image's local distribution of frequencies is the next stage. To do this, the LBP picture is first converted to the frequency domain using block-based DCT, and each block's DCT coefficient statistics are then computed.

Drawing on the introduction above, this experiment models the tampering traces in photos using LBP and DCT. Each chrominance component is first split into overlapping blocks with a 50% overlap for localization reasons. Since LBP is an extremely powerful image texture descriptor, it is then applied to each block in this experiment to emphasize and highlight the tampering artifacts introduced in the original image (i.e., sharp edges at the boundaries of the area that was glued and the micro-edges within it) and increase their visibility in the picture. Lastly, to record alterations to the image's local frequency distribution, the LBP-coded block is changed into the sphere of frequencies employing the DCT methodology. A feature vector is created by organizing the matching DCT coefficients' standard deviation.

4.3. Training and Testing Using the SVM Classifier

The classification challenge of picture splicing detection is identifying manipulated and genuine photos. In high-dimensional space, Support Vector Machines (SVM) may find the ideal separation hyperplane that optimizes the margin between various data points. Regression analysis and classification are two applications for this supervised learning model. Therefore, SVM is used for both training and testing in the methods described in this study.

The specific procedure is as follows: first, the LBP and DCT features of the training set images are extracted using the aforementioned methods and then sent to the SVM for instruction. The predictive model is established using cross-validation, which yields the SVM's optimum parameters. The next step is to determine if the photos under investigation have been spliced by feeding the LBP and DCT features that were retrieved from the test set images into the SVM for classification. Experimental Analysis

This section will introduce the dataset used in this experiment and describe the experimental procedure.

5. Experimental Analysis

The experimental approach and dataset utilized in this experiment will be introduced in this section.

5.1. Experimental Data

COLUMBIA and CASIA TIDE v1.0 were used in this investigation.

There are a total of 1721 photos in the CASIA TIDE v1.0, of which 800 are genuine and 921 are tampered with. Every image is in JPG format, and it can be found in two sizes: 384 x 256 and 256 x 384.

There are 363 photos altogether in the COLUMBIA, 180 of which are tampered with and 183 of which are genuine. The images are in the TIFF or BMP format and range in size from 757x568 to 1152x768.

Figures 3 and 4 provide selections of photos from the two datasets. Table 1 presents detailed data on these two datasets.

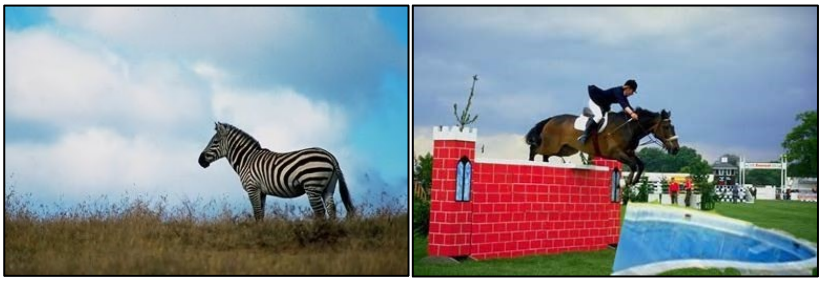

Figure 3. A selection of photos from the CASIA TIDE v1.0 (left: authentic image, right: tampered image) (Photo credit: Original).

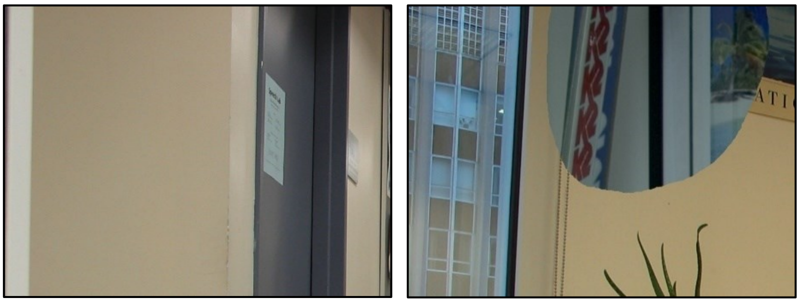

Figure 4. A selection of photos from the COLUMBIA (left: authentic image, right: tampered image) (Photo credit: Original).

Table 1. Experimental Datasets.

Dataset	Image Count Authentic Images	Tampered Images	Total Images	Image Formats	Image Sizes
CASIA TIDE v1.0 Dataset	800	921	1721	Jpg	384×256, 256×384
COLUMBIA Dataset	183	180	363	tif, bmp	757×568 to 1152×768

Five-fold cross-validation was employed in this work. Every one of the dataset's remaining four subgroups was alternately utilized as both the testing and training sets after five subsets were chosen at random. This process was used to obtain the optimal parameters that resulted in the highest cross-validation accuracy. The Spyder platform was used to experiment with each set of results ten times, and the average of the outcomes was used to determine the final result.

5.2. Evaluation Metrics

Four metrics were included in this experiment to assess the model.

The exact details of the assessment measures are as follows:

Accuracy. The proportion of correct projections made relative to all predictions is known as accuracy. $(TP: True\ Positive, TN: True\ Negative, FN: False\ Negative, FP: False\ Positive.)$

$$Accuracy = \frac{TP+TN}{TP+TN+FN+FP} \tag{7}$$

Precision. Precision is described as the percentage of actual positive outcomes among all samples that were predicted to be positive.

$$Precision = \frac{TP}{TP+FP} \tag{8}$$

Recall. The percentage of real positive samples among all actual affirmative examples that were accurately predicted is known as recall.

$$Recall = \frac{TP}{TP+FN} \tag{9}$$

F1 Score. A balanced indicator of both metrics' performance is the F1 Score. It is the accuracy and recall harmonic average.

$$F1\,Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{10}$$

5.3. Experimental Parameters

Numerous factors, including color channels, block division kinds and sizes, and LBP parameters, are part of the model utilized in this experiment. Numerous studies were conducted on the CASIA TIDE v1.0 and COLUMBIA, looking at different parameter combinations to find the optimal set of variables for the best outcomes. The results of the studies showed that chrominance channels, 16x16 not overlapping blocks, and LBP parameters the value of R=8 and P=1 produced the best results. Thus, the aforementioned parameters were used in this study to execute the final experiment and acquire findings.

6. Results and Discussion of the Experiment

The experimental findings on two datasets—CASIA TIDE v1.0 and COLUMBIA—will be covered in this section.

Experimental Results Using COLUMBIA.

Table 2 displays the experimental findings on the COLUMBIA.

Table 2. Experimental Outcomes on the COLUMBIA.

Using Dataset	Accuracy	Precision	Recall	F1 Score
COLUMBIA	94.06%	94.14%	94.07%	94.10%

6.1. Experimental Results Using CASIA TIDE v1.0

The findings from the CASIA TIDE v1.0 experiment are displayed in Table 3.:

Table 3. Experimental Outcomes on the CASIA v1.0.

Using Dataset	Accuracy	Precision	Recall	F1 Score
CASIA TIDE v1.0	97.68%	97.77%	97.58%	97.67%

6.2. Ablation Study

The experimental results demonstrate that using LBP and DCT feature extraction on both datasets yields consistently good results, thereby proving the reliability of the experiments. This study also used methods that extract features using only one of these approaches, i.e., utilizing either LBP features or DCT features alone, in order to investigate the efficacy of combining LBP and DCT. Table 4 displays the outcomes of utilizing LBP alone, DCT alone, and their combination.

Table 4. Results of Different Feature Selection Approaches.

Features	Accuracy
LBP	86.34%
DCT	90.68%
LBP and DCT	94.06%

It is evident that better outcomes were obtained when LBP and DCT were combined.

7. Comparison with Existing Methods

The Accuracy is compared in this part with a few current techniques. Table 5 presents the findings.

Table 5. Comparison with Other Methods.

Methods	Accuracy
Base on Texture Features with Fractal	96%
Based on improved Markov features	94.38%
based on Illumination-Reflectance model and LBP	94.59%
Proposed method	97.68%

The experimental results show that this study's outcomes are better than those of certain other approaches currently in use.

8. Conclusion

This paper proposes a method for detecting image splicing based on the integration of Local Binary Patterns (LBP) and Discrete Cosine Transform (DCT) features. The process begins by converting the RGB input image to the YCbCr color space, where the Cb and Cr color channels are divided into overlapping blocks. Each block's LBP code is then transformed into the DCT domain. The standard deviation of each DCT coefficient for each block is calculated and used as a feature. An SVM classifier is employed for classification. The proposed method was thoroughly evaluated using two benchmark datasets: CASIA TIDE v1.0 and COLUMBIA. The results demonstrated the effectiveness of the combined DCT and LBP approach, achieving accuracies of 94.06% and 97.68% on these datasets, respectively. These outcomes surpass several existing methods, underscoring the robustness of the proposed strategy.

Future research will focus on exploring alternative detection methods and extending their application to other areas of image tampering detection, such as copy-move forgery detection. Additionally, experiments will be conducted using larger and more diverse datasets to further validate the method's efficacy.

References

[1] Thakur, R., & Rohilla, R. (2020). Recent advances in digital image manipulation detection techniques: A brief review. Forensic Science International, 312, 110311. https://doi.org/10.1016/j.forsciint.2020.110311.

[2] Al-Azawi, J., Al-Saidi, M. G., Jalab, N. A., Ibrahim, R. W., & Baleanu, D. (2021). Image splicing detection based on texture features with fractal entropy. Computational Materials and Continua, 69(3), 3903-3915. https://doi.org/10. 32604/cmc. 2021.020368.

[3] Dong, J., Wang, W., & Tan, T. (2013). CASIA Image Tampering Detection Evaluation Database. Paper presented at the 2013 IEEE China Summit & International Conference on Signal and Information Processing (ChinaSIP), July 6-10, 2013, Beijing, China. https://doi.org/10.1109/ChinaSIP. 2013. 6491686.

[4] Das, D., Naskar, R., & Chakraborty, R. S. (2023). Image splicing detection with principal component analysis generated low-dimensional homogeneous feature set based on local binary pattern and support vector machine. Multimedia Tools and Applications, 82(17), 25847-25864. https://doi.org/10. 1007/s11042-023-14658-w.

[5] Ng, T.-T., Chang, S.-F., & Sun, Q. (2004). ADVENT Technical Report: A data set of authentic and spliced image blocks.

[6] Liu, J., Li, X., & Jiang, C. (2020). Research on image stitching detection based on improved Markov features. Information Technology & Cyber Security, 39(2), 13-18. https://doi.org/10.19358/j.issn.2096-5133.2020.02.003.

[7] Hsu, Y. F., & Chang, S. F. (2006). Detecting image splicing using geometry invariants and camera characteristics consistency. Paper presented at the 2006 IEEE International Conference on Multimedia and Expo, July 9-12, 2006.

[8] Niyishaka, P., & Bhagvati, C. (2020). Image splicing detection technique based on illumination-reflectance model and LBP. Multimedia Tools and Applications, 80(2), 2161-2175. https://doi.org/10.1007/s11042-020-09707-7.

[9] Lv, J., Lu, W., Wang, M., Liu, Y., Shi, K., Huang, H., & Zhao, H. (2022). Image stitching tamper detection based on multi-scale feature prior. China Science and Technology Papers, 17(11), 1267-1275. https://doi.org/10.3969/j.issn. 2095-2783.2022.11.014.

[10] Zhao, D., & Tian, X. (2022). A multiscale fusion lightweight image-splicing tamper-detection model. Electronics, 11(16). https://doi.org/10.3390/ electronics 11162621.

[11] Kaur, N., Nazir, N., & Manik. (2021). A review of local binary pattern based texture feature extraction. Paper presented at the 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), September 3-4, 2021.

[12] Alahmadi, A. A., Hussain, M., Aboalsamh, H., Muhammad, G., & Bebis, G. (2013). Splicing image forgery detection based on DCT and local binary pattern. Paper presented at the 2013 IEEE Global Conference on Signal and Information Processing, December 3-5, 2013.

[13] Shi, Y. Q., Chen, C., & Chen, W. (2007). A natural image model approach to splicing detection. Paper presented at the Proceedings of the 9th Workshop on Multimedia & Security, Dallas, Texas, USA. https://doi.org/10.1145/ 1288869. 1288878.

[14] Zhang, Y., Zhao, C., Pi, Y., & Li, S. (2012). Revealing image splicing forgery using local binary patterns of DCT coefficients. Paper presented at the International Conference on Communications, Signal Processing, and Systems.

[15] Shen, K., & Chen, X. (2023). Enhanced local binary mode and its image texture feature extraction. Computers and Simulation, 40(6), 260-267. https://doi. org/10. 3969/j.issn.1006-9348.2023.06.048.