International Journal of Current Engineering and Technology
©2022 INPRESSCO®, All Rights Reserved

E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

Hierarchy SURF Feature Clustering for Image Forgery Detection

Neha Sharma*[*] and Pallavi Gupta

Department of Electronic & Communication Engineering, Global Research Institute of Management and Technology, Haryana, India

Received 20 Nov 2022, Accepted 18 Dec 2022, Available online 20 Dec 2022, **Vol.12, No.6 (Nov/Dec 2022)**

Abstract

Today manipulation of digital images has become easy due to powerful computers, advanced photo-editing software packages and high-resolution capturing devices. Verifying the integrity of images and detecting traces of tampering without requiring extra prior knowledge of the image content or any embedded watermarks is an important research field. Copy move is the most common image tampering technique used due to its simplicity and effectiveness, in which parts of the original image is copied, moved to a desired location and pasted. This is usually done in order to hide certain details or to duplicate certain aspects of an image. This paper is an attempt for surveying the recent developments in the field of Copy move image forgery detection and complete bibliography is presented on blind methods for forgery detection. As the advent and growing popularity of image editing software, digital images can be manipulated easily without leaving obvious visual clues. If the tampered images are abused, it may lead to potential social, legal or private consequences. To this end, it's very necessary and also challenging to find effective methods to detect digital image forgeries. In This works, a fast keypoint based method to detect image copy move forgery is will be used based on the SIFT (scale-invariant feature transform) descriptors, which are invariant to rotation, scaling etc. Results of experiments indicate that the proposed method is valid in detecting the image region duplication and quite robust to additive noise and blurring. For Clustering of Keypoints Clusting algorithm will be used.

Keywords: *Clustering algorithm, Image tampering technique, SIFT etc.*

1. Introduction

Unquestionably, the age we live in exposes us to a great variety of visual stimuli. While in the past we might have had faith in the accuracy of these images, this faith is now being eroded by modern digital technologies. Doctored images are becoming more and more prevalent in a variety of contexts, including tabloid publications, the fashion industry, mainstream media, academic journals, political campaigns, courtrooms, and picture hoaxes that show up in our email inboxes. In order to regain some faith in digital photographs, the area of digital forensics has grown during the past five years. I'll go over the current state of the art in this brand-new, fascinating topic.

The idea of using digital watermarking to verify images has been put forth (see, for example, and for general surveys). This method has the disadvantage that a watermark must be added at the time of recording, limiting its use to digital cameras with certain accessories. In contrast to these methods, passive image forensics techniques work without the need of a watermark or signature. These methods operate under the presumption that while digital forgeries would not leave any visible signs of tampering, they might change an image's underlying data. Approximately five categories may be used to classify the collection of picture forensic tools: 1) pixel-based methods for spotting statistical outliers introduced at the pixel level; 2) format-based techniques that take advantage of statistical correlations brought on by a particular lossy compression scheme; 3) camera-based techniques that take advantage of artifacts brought on by the camera lens, sensor, or on-chip post processing; 4) physically based techniques that explicitly model and detect anomalies in the three-dimensional interaction between physical objects, light, and the camera; and 5) geometric-based techniques that measure objects in the real world.

I'll go through a few exemplary forensic tools from each of these groups. I definitely missed numerous deserving papers in the process. However, it is my goal that this study provides a fair representation of the new field of picture forgery detection.

2. Pixel-Based

The legal system frequently uses a variety of forensic analyses, including forensic identification (using DNA

[*] Corresponding author's ORCID ID: 0000-0000-0000-0000

DOI: https://doi.org/10.14741/ijcet/v.12.6.5

or a fingerprint) as well as forensic deontology, forensic entomology, and forensic geology (using insects and rocks) (soil). All kinds of physical evidence are examined in conventional forensic sciences. The focus in the digital world is on the pixel, which is an image's fundamental building unit. I outline four methods for identifying different types of tampering, each of which examines pixel-level correlations that result from a particular type of tampering directly or indirectly.

3. Cloning

Clone (copy and paste) sections of the image to hide a person or item in the scene are perhaps one of the most used image alteration techniques. Visual cloning detection can be challenging when this is done carefully. Additionally, it is computationally hard to scan through every potential picture position and size since the cloned areas might be of any form and location. The detection of cloned picture portions has been created using two effective computational approaches.

The block discrete cosine transform is used by the authors first (DCT). By combining comparable blocks in an image with the same spatial offset and lexicographically sorting the DCT block coefficients, duplicate areas are identified. In a comparable technique, the authors create a reduced-dimension representation by doing a principal component analysis (PCA) on tiny fixed-size picture blocks. Duplicate areas are once more found by grouping and sorting all of the picture blocks lexicographically. To minimize computing complexity and guarantee that the clone detection is resistant to minute fluctuations in the picture caused by additive noise or lossy compression, both the DCT and PCA representations are used.

4. Literature Survey

Lee, Barry B., et al. (1990) [1] In this study, we assessed the macaque ganglion cells' responsiveness to luminance and chromatic sinusoidal modulation. Tonic ganglion cells of the parvocellular route (P-pathway) were more susceptible to chromatic modulation than were phasic ganglion cells of the magnocellular pathway (M-pathway). Phasic ganglion cells' temporal sensitivity to luminance modulation varied in a way that was consistent with psychophysical findings as retinal illumination decreased. The same held true for chromatic modulation and tonic cells. Together, the findings clearly imply that the physiological substrate for the detection of luminance modulation is formed by M-pathway cells, while the physiological substrate for the detection of chromatic modulation is formed by P-pathway cells. However, at high light levels, responses in the M-pathway, principally resulting from a nonlinearity of cone summing, are likely to be responsible for the incursion of a so-called luminance mechanism at 10 Hz in psychophysical perception of chromatic modulation. Phasic and tonic ganglion cells both reacted to frequencies that are greater than those that may be detected psychophysically. Despite the fact that the corner frequency for the P-pathway is lower than for the M-pathway, this shows that central processes serve as low-pass filters to alter the signals of these cells. The response phase for both cell types was in keeping with their definition as linear filters with a set time delay at various frequencies.

Cortes, Corinna et al. (1995) [2] The support-vector network is a novel learning device for issues involving two groups of objects in this research. Conceptually, the machine implements the idea that input vectors are non-linearly mapped to a very large feature space. A linear decision surface is built in this feature space. High generalisation ability of the learning machine is ensured by special qualities of the decision surface. The support-vector network's principle was previously put into practise for the constrained scenario when training data can be segregated without mistakes. Here, we extend this finding to training data that cannot be separated. Support-vector networks with polynomial input transformations are shown to have high generalizability. We contrast the performance of the support-vector network with a number of traditional learning methods that all participated in an Optical Character Recognition benchmark study.

Zhang, Guangcheng et al. (2004) [3] This research introduces a unique method for face recognition by enhancing classifiers based on statistical local characteristics. To represent the local characteristics of a face picture, the Local Binary Pattern (LBP) histograms [14] are produced from the face image after it has been scanned using a scaled sub-window. By categorising every second pair of face photos as intra-personal or extra-personal, the multi-class issue of face identification is reduced to a two-class problem [9]. As a discriminating characteristic for classifying people as intra- or extra-personal, the Chi square distance between the matching Local Binary Pattern histograms of two facial photographs is utilised. We use AdaBoost algorithm to learn a similarity of all face picture pairings. The FERET FA/FB picture sets were used to test the suggested approach, which produced an impressive identification rate of 97.9%.

Ng, Tian-Tsong et al. (2004) [4] In this work, picture splicing is a straightforward method for cropping and pasting portions from one or more sources. It is a key procedure in digital photomontage, a paste-up created by fusing photos together using software programmes like Photoshop. Several infamous news reporting situations involving the use of fabricated photos contain examples of photomontages. Researchers have lately begun developing new approaches aimed at blind passive detection of picture splicing as part of their hunt for technology solutions for image authenticity. To hasten the developments and support collaborative investigations, however, we require an open data set with diverse content and realistic splicing circumstances, just like the majority of other research groups working with data processing. A data collection of 1845 picture blocks with a constant dimension of 128 pixels by 128 pixels is described in detail in this study. The image blocks are taken from CalPhotos collection [CalPhotos'00] photographs, along with a few supplementary pictures taken with digital cameras. The data set contains roughly the same number of blocks of real and spliced images, which are further broken down into other subcategories (smooth vs. textured, arbitrary object boundary vs. straight boundary).

Johnson, Micah K., et al. (2006) [5] Almost all optical imaging techniques in this study introduce a range of aberrations into a picture. For instance, chromatic aberration happens when an optical system is unable to precisely focus light of various wavelengths. According to a first-order approximation, lateral chromatic aberration appears as the expansion or contraction of colour channels relative to one another. This aberration is frequently disrupted and fails to be uniformly present throughout a picture when it is altered. The effectiveness of the computational method we propose for automatically measuring lateral chromatic aberration in spotting digital tampering is demonstrated.

5. Proposed Work

Digital material may now be changed and used in ways that were just not feasible twenty years ago thanks to technology. The technology of the future will almost likely enable us to modify digital material in ways that are currently unthinkable. It will also be more crucial than ever for the science of digital forensics to try to stay up with this technology as it develops.

There is no doubt that new ways will be developed to produce better fakes that are more difficult to identify as we continue to improve tools for uncovering photographic frauds. While certain forensic technologies could be simpler to trick than others, most users won't be able to get around some of them. By simply putting a picture into its original lattice and reinterpolating each colour channel, one may, for instance, restore the colour filter array interpolation after it has been disrupted. On the other hand, a typical photo-editing application makes it difficult to adjust for erratic lighting. An arms race between the forger and the forensic analyst is partly inevitable, much like in the virus/antivirus and spam/antispam games. However, the study of picture forensics has made it more difficult and time-consuming (but never impossible) to produce a fake that cannot be found.

6. Proposed Changes in DCT Forgery Detection

The approach for quantifying step estimate proposed in the current study is histogram-based. The following are the work's key contributions:

- This work establishes a mathematical analysis of the quantization effect during JPEG compression and decompression in contrast to earlier histogram-based methods in order to support the relationship between local maxima of the number of integer quantized forward (IQF) coefficients and the actual quantization step. According to this analysis, the quantity of IQF coefficients may be used as an inherent quantization fingerprint to solve the issue of the history of JPEG compression. A list of candidates for the genuine quantization step can be provided via the IQF fingerprint-based approach.
- To improve accuracy, the work replaces the Laplacian model with the most recent statistical model of DCT coefficients in the estimate process. From the list of possibilities presented by the aforesaid approach, the model is utilised to produce the best estimate of the quantization step.
- To demonstrate the suggested method's great accuracy, it is applied to big picture datasets. Additionally, although some previous approaches fail, the suggested method can accurately estimate the quantization steps for DC coefficients. The strong performance on colour photographs also demonstrates how resistant the suggested technique is to colour noise created by the JPEG compression pipeline. Not to mention, the suggested approach may be used to identify JPEG compression and estimate the secondary quantization table in a double-JPEG compressed picture that has been saved in lossless format.

7. Results and Analysis

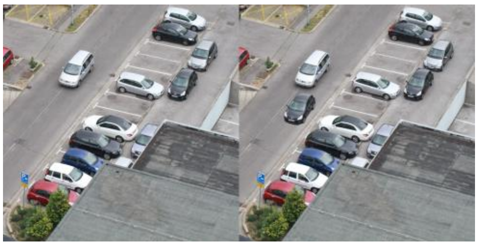

Figure 1: Original and the Forged image from the dataset

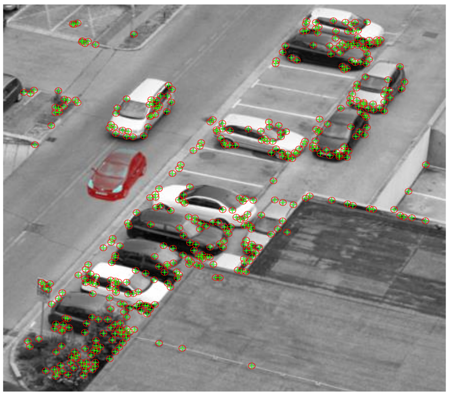

Figure 2: Extracted features form the input image

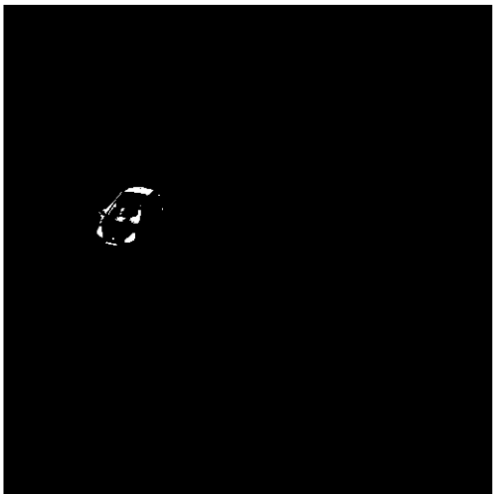

Figure 3: Identified Boundaries of the forged area

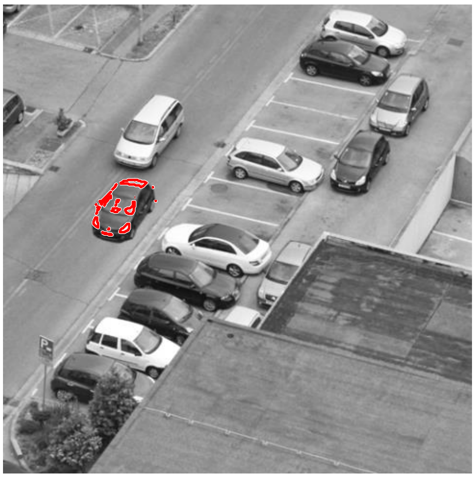

Figure 4: Visualizing forged area in the original image

Table 1: Overall performance numerical values of forgery detection methods

Algorithm	Accuracy	F-measure	Precision	Recall
Proposed	99.4%	99.1%	98.9%	99.4%
IRVM	92.2%	92.2%	96.9%	88.4%
HMM + SVM	89.0%	86.5%	93.4%	82.1%
SVM	84.8%	87.7%	91.6%	78.0%

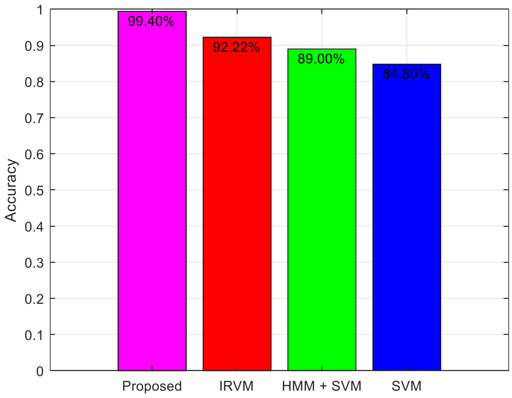

Figure 5: Accuracy of the proposed model compared with IRVM, HMM+SVM and SVM algorithms

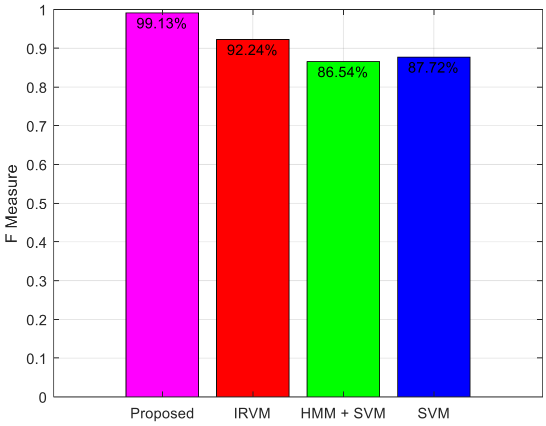

Figure 6: F-Measure of the proposed model compared with IRVM, HMM+SVM and SVM algorithms

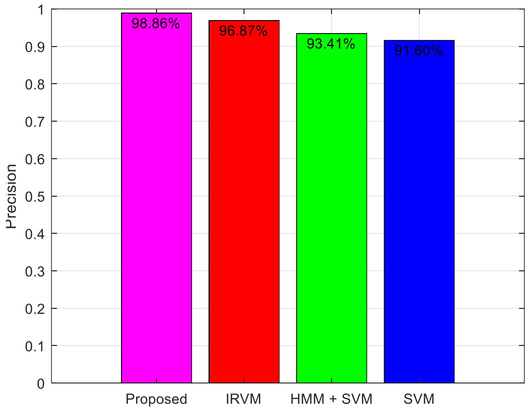

Figure 7: Precision score of the proposed model compared with IRVM, HMM+SVM and SVM algorithms

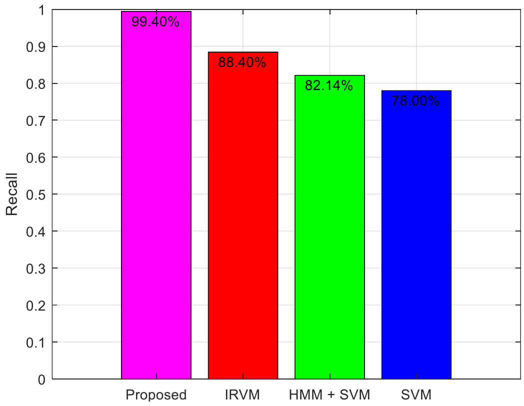

Figure 8: Recall Score of the proposed model compared with IRVM, HMM+SVM and SVM algorithms

Conclusion and Future Scope

The method for estimating a quantization step from a given picture is proposed in this paper. The work proposes a quantization fingerprint—the number of integer quantized forward coefficients—by analysing the quantization effect during the JPEG compression and decompression pipeline. It also provides a mathematical justification to demonstrate the relationship between local maxima of that measure and the actual quantization step. Based on the quantization fingerprint and the statistical model of DCT coefficients presented in our earlier research, the estimate technique was created. Numerical tests on a sizable picture database demonstrate the applicability of the suggested strategy. The high estimation accuracy for a wide range of photos with various image contents, image sizes, and quality parameters is the suggested method's main strength. Additionally, although some previous approaches fail, the suggested method can accurately estimate the quantization steps for DC coefficients. Applying the suggested approach to actual colour JPEG photographs obtained from various camera models/brands emphasises how accurate it is. The resilience of the proposed approach against colour noise created during the JPEG compression process is demonstrated by the good performance on colour pictures. The suggested technique takes longer than existing ones while having higher estimation accuracy performance. This flaw results from the use of a numerical optimization approach for ML estimate of the DCT model parameters. The suggested approach also demonstrates its accuracy in additional real-world forensic situations, such as the estimate of the secondary quantization table in a double-JPEG compressed picture stored in lossless format and the detection of JPEG compression. This strategy could be investigated in more forensic circumstances in the future. By examining the properties of double-JPEG compression and determining the relevant version of the IQF fingerprint, this technique may be extended for the detection of double-JPEG compression existence and estimate of the principal quantization table in a double-JPEG compressed picture. Due to the strong efficiency of the suggested approach for JPEG compression identification on small-size pictures, the second forensic application uses discrepancies in JPEG compression history among various regions of the image under examination to identify and pinpoint copy-paste forgeries. As various manufacturers create their own compression schemes, picture origin identification is another forensic application that seeks to confirm if the image in issue was captured by a certain source (camera equipment, model, brand).

References

[1] Lee, Barry B., Joel Pokorny, Paul R. Martin, Arne Valbergt, and Vivianne C. Smith. "Luminance and chromatic modulation sensitivity of macaque ganglion cells and human observers." JOSA A 7, no. 12 (1990): 2223-2236.

[2] Cortes, Corinna, and Vladimir Vapnik. "Support-vector networks." Machine learning 20, no. 3 (1995): 273-297.

[3] Zhang, Guangcheng, Xiangsheng Huang, Stan Z. Li, Yangsheng Wang, and Xihong Wu. "Boosting local binary pattern (LBP)-based face recognition." In Advances in biometric person authentication, pp. 179-186. Springer Berlin Heidelberg, 2004.

[4] Ng, Tian-Tsong, Shih-Fu Chang, and Q. Sun. "A data set of authentic and spliced image blocks." Columbia University, ADVENT Technical Report (2004): 203-2004.

[5] Johnson, Micah K., and Hany Farid. "Exposing digital forgeries through chromatic aberration." In Proceedings of the 8th workshop on Multimedia and security, pp. 48-55. ACM, 2006.

[6] Sokolova, Marina, Nathalie Japkowicz, and Stan Szpakowicz. "Beyond accuracy, F-score and ROC: a family of discriminant measures for performance evaluation." In Australasian Joint Conference on Artificial Intelligence, pp. 1015-1021. Springer Berlin Heidelberg, 2006.

[7] Hsu, Yu-Feng, and Shih-Fu Chang. "Detecting image splicing using geometry invariants and camera characteristics consistency." In Multimedia and Expo, 2006 IEEE International Conference on, pp. 549-552. IEEE, 2006.

[8] Shi, Yun Q., Chunhua Chen, and Wen Chen. "A natural image model approach to splicing detection." In Proceedings of the 9th workshop on Multimedia & security, pp. 51-62. ACM, 2007.

[9] Zhang, Zhen, Jiquan Kang, and Yuan Ren. "An effective algorithm of image splicing detection." In Computer Science and Software Engineering, 2008 International Conference on, vol. 1, pp. 1035-1039. IEEE, 2008.

[10] Dong, Jing, Wei Wang, Tieniu Tan, and Yun Q. Shi. "Run-length and edge statistics based approach for image splicing detection." In International Workshop on Digital Watermarking, pp. 76-87. Springer Berlin Heidelberg, 2008.

[11] Farid, Hany. "Image forgery detection." IEEE Signal processing magazine 26, no. 2 (2009): 16-25.

[12] Mahdian, Babak, and Stanislav Saic. "A bibliography on blind methods for identifying image forgery." Signal Processing: Image Communication 25, no. 6 (2010): 389-399.

[13] Chih-wei Hsu, Chih-chung Chang , Chih-jen Lin, A practical guide to support vector classification, (2010).

[14] Wang, Wei, Jing Dong, and Tieniu Tan. "Image tampering detection based on stationary distribution of Markov chain." In Image Processing (ICIP), 2010 17th IEEE International Conference on, pp. 2101-2104. IEEE, 2010.

[15] Zhao, Xudong, Jianhua Li, Shenghong Li, and Shilin Wang. "Detecting digital image splicing in chroma spaces." In International Workshop on Digital Watermarking, pp. 12-22. Springer Berlin Heidelberg, 2010.

[16] Shivakumar, B. L., and Lt Dr S. Santhosh Baboo. "Detecting copy-move forgery in digital images: a survey and analysis of current methods." Global Journal of Computer Science and Technology 10, no. 7 (2010).

[17] Huang, Di, Caifeng Shan, Mohsen Ardabilian, Yunhong Wang, and Liming Chen. "Local binary patterns and its application to facial image analysis: a survey." IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) 41, no. 6 (2011): 765-781.

[18] Hussain, Muhammad, Summrina Kanwal Wajid, Ali Elzaart, and Mohammed Berbar. "A comparison of SVM kernel functions for breast cancer detection." In Computer Graphics, Imaging and Visualization (CGIV), 2011 Eighth International Conference on, pp. 145-150. IEEE, 2011.

[19] Muhammad, Ghulam, Muhammad Hussain, and George Bebis. "Passive copy move image forgery detection using undecimated dyadic wavelet transform." Digital Investigation 9, no. 1 (2012): 49-57.

[20] Zhang, Yujin, Chenglin Zhao, Yiming Pi, and Shenghong Li. "Revealing image splicing forgery using local binary patterns of DCT coefficients." In Communications, Signal Processing, and Systems, pp. 181-189. Springer New York, 2012.