Journal of Innovative Image Processing (ISSN: 2582-4252)
www.irojournals.com/iroiip/

Scam Image Detection on Copy-Move by JPEG Features and Classical Block Matching with Improved Variant

P. Ebby Darney

Associate Professor, Department of Electrical and Electronics Engineering, RajaRajeswari College of Engineering, Bangalore, India

E-mail: darney.pebby@gmail.com

Abstract

Numerous methods have been developed to identify copy-move forgeries, which are among the most often used alteration strategies of digital photographs. The most widely used format of digital photographs is JPEG, which allows for high-rate compression without drastically altering the meaning of the picture. The objective of this work is to develop a system that can automatically identify the forgery type of the suspect image through in a single procedure, without requiring any kind of expert information. A preferable method is to run the same image through multiple algorithms, which saves time and prevents the needless evaluation of multiple detection results, from which it may be difficult to determine the correct output due to the presence of multiple confounding factors. Additionally, it has been shown that the established method is very effective in detecting expert forgeries when the duplicated region is picked in a non-rigid fashion, which is almost hard for the human eye to perform.

Keywords: Copy-move, forgery image, intensity vector, similar matching, coherence vector

1. Introduction

There are many important applications of digital photographs in fields including medical, law, and public relations. Unfortunately, forger may quickly edit and control digital photographs by using a wide variety of image regulatory software tools. With the rise of this programme, issues of photo authenticity and veracity have emerged as a major challenge. This has made studying methods for identifying fake images a priority. The strategies for detecting image fraud may be classified as either active or passive [1-3]. Images in many forms of media dissemination are now widely used. It is often believed that a picture is worth

DOI: https://doi.org/10.36548/jiip.2022.4.001
Received: 07.09.2022, received in revised form: 03.10.2022, accepted: 18.10.2022, published: 01.11.2022

a thousand words when describing an event or a scene. As a result of today's advanced technical landscape, digital photographs play an important part in many different industries, mostly in fields related to military, reporting, health care, and the media. In this age of ever-increasing internet penetration and ever-improving camera, software, and hardware capabilities, a digital picture is increasingly recognised as a key informational resource [4-8].

The availability of high-quality, low-cost hardware and software editing equipment, as well as sophisticated, user-friendly tools, has made picture alteration a breeze in recent years. Every day, image forgery becomes a more pressing issue. The ease with which digital photos may be altered in both their origin and content poses a threat to their security, which has contributed to an increase in the usage of digital image editing tools. Digital image research, an emerging area of study, investigates methods of verifying the credibility of digital photographs [9].

To create a convincing fake photo, all one needs is a computer and some inexpensive editing software. False information may travel at the speed of light over the Internet. As a result, public perception and acceptance may be swayed in ways that have unintended consequences for society. When photographs are used as evidence in court, the situation may become much more dire.

As a result, there is a pressing need for a trustworthy and reliable authentication technique that can determine whether an image is a fake or not. Most forgeries are created using one of two techniques: copy-move or splicing. In the first scenario, undesirable elements are hidden by copying and pasting a portion of an image over other areas of the same picture [10-12].

1.1 Image Forgery

To "forge" an image is to alter a digital photo in such a way that its true meaning is obscured. The need for authenticity and the protection of an image's integrity motivates the search for fakes. Methods include purpose feature matching, adaptive over-segmentation, theme victimization, and the detection of copy-move forgeries. The host picture is split into overlapping rectangular blocks in the block-based forgery detection technique, which would become computationally costly as the size of the image grows. In addition, the image-blocking approach has a poor recall rate due of its uniform shape, which makes it insensitive to even little variations in the forgery regions [13].

1.2 Image Processing

Due to the availability of sophisticated image processing and editing tools, digital photographs may be easily manipulated and edited. It is now feasible to alter a picture significantly, without any visible signs of doing so. It is becoming more important to authenticate digital photos, verify their content, and identify forgeries as digital and video cameras gradually replace their analogue predecessors. This research focuses on methods for identifying poorly edited digital copies and printed copies.

1.3 The Urgent Need to Identify Digital Fakes

Digital forgeries may be made from a single picture or a collection of photographs with the use of powerful digital image manipulation applications like Photoshop. Figure 1 depicts an instance of digital fraud. The newspaper clipping reveals that three images were used to create the final composite image, depicting the White House, Bill Clinton, and Saddam Hussein. In the first step of making, it seems like the White House in the distance was resized and blurred. Then, parts of the photos of Bill Clinton and Saddam Hussein were spliced onto the one of the White House. Speaker stands equipped with microphones were carefully wheeled in, while taking care to maintain the appropriate lighting and shadows. The example in Figure 1 is a counterfeit that was deliberately made to seem quite authentic.

INTERNET

Spies turn to high-tech info ops

PCs, Internet used for manipulating images, public opinion

ALTERED IMAGE

BY DANIEL VERTON

Federal intelligence agencies are studying ways to use computers and the Internet, rather than just leaflets and radio broadcasts, to shape and disseminate information designed to sway public opinion in the world's hot spots.

As part of its so-called "perception management" program, the intelligence community has for decades created misinformation to trigger political change without direct political or military involvement in countries where the United States has vested interests, such as Iraq and North Korea.

Acting on congressional recommendations to bolster research and development in information technology, intelligence agencies are turning to PCs to develop more sophisticated means of manipulating and delivering digital photos, video clips and recorded sound to portray fictitious events in hopes of provoking desirable

1 2 3

Altered Egos

The top photo, of a fictitious meeting between President Clinton and Saddam Hussein, was generated by digitally altering and combining elements from three photos, shown below the altered image. Intelligence agencies plan to use similar techniques to create images and then disseminate them via the Internet in their efforts to influence events in foreign countries, such as Iraq.

Figure 1. Recent digital image forgery [27]

The only justification for creating a fake copy of a picture is to get access to the previously unavailable material. By adhering a replica of the relevant segment of the manufacturing process over the original, sensitive data in a vision, sensitive information might be concealed. These image adjustments allow for a variety of expressions to be conveyed. These manipulated pictures are often used to prove innocence when none was intended. In the identification of similar actions, since the copied detail is taken from a comparable photograph, manipulating images is a challenging endeavour. Qualities like motion, shading, and surface samples are helpful for the rest of the image. Discovering a forgery becomes a much more laborious task because of the additional steps taken after initial preparation and before the duplicated partition is glued to a new idea [14,15].

1.4 Motivation

Due to the proliferation of digital photographs and the availability of user-friendly photo editing programmes, manipulating photographs is now simpler than ever. This has led to a dramatic surge in the circulation of fake or doctored photos purporting to depict factually inaccurate content. As a result, finding a workable solution to the problem of picture forgery has become urgent. Copy-move forgeries, in which certain objects or portions in a picture are replicated and then moved to another location, is the most prevalent kind of image tampering in digital images. Therefore, forgery detection and localisation are two areas of digital forensics that have received a lot of attention. There are several academic articles dedicated to the topic of image faking.

2. Literature Survey

Copy-move and splicing forgeries may be uncovered with the use of an integrated technique provided by S.S. Ali et al. [15]. Mistakes in identifying the form of forgery will impact the accuracy of the detection. In all tactics, it is not essential to categorise the images into specific forgeries kinds.

E.U.H. Qazi et al. [16], presented a technique based on JPEG blocks. However, there are two major flaws in that research. The first is that the image has to be tweaked through training practice before it can be used to identify other types of fraud. In reality, however, it is impossible to determine the sort of fabrication involved in a suspicious photo. The method also has the drawback of processed images that have undergone very little reduction. In this scenario, the amount and kind of local noise may be utilised as a feature to pinpoint where in

a picture the noise is coming from. Inconsistencies and differences from one place to the next, give additional information beyond BAG to pinpoint the forged area. In order to determine whether or not a photograph is genuine, a function that uses a combination of BAG and noise was developed.

In the context of double image compression, the research [17] proposed a trustworthy deep learning-based strategy to identify picture forgeries. The model was trained by comparing the original and compressed versions of a picture. The altered concept was re-compressed, and the discrepancy between the two was calculated. Since the forgery's origin is different from the original, the developed portion of the picture stands out. The method was efficient and less bulky than standard methods. Overall, the validation accuracy of 92.23 percent shows that the experiment has produced encouraging findings.

The research [18] suggested a system architecture for object identification and transfer learning that uses ResNet50v2 as a baseline algorithm. Batch normalisation was the first step in the procedure. To optimise the weights, it used an activation function to apply updates. The authors of the research applied a deep learning architecture for the degradation issue.

To identify fakes, Davarazni et al. [19], presented the advanced techniques where the feature vectors were extracted for each block using LBP operations, and then sorted lexicographically. Although effective, the approach was laborious and cannot identify rotation angles for the duplicated sections. The characteristics of each block were lexicographically sorted by Histograms of Oriented Gradients in [9] by Lee et al. Similar block pairings were discovered as duplicates in a picture by comparing their sizes.

In the study [20], the authors presented the techniques based on a fully connected classifier network that can tell the difference between original and edited pictures. The method in [21], presented deep learning for the scam image detection which functions as a regularizer, to effectively hide the impact of image contents and pick up on the alterations that were made. In order to generate discriminative features for SVM classification, it was compared to the proposed CNN-based model on a variety of publicly available datasets.

3. Methodology

Forgery detection methods that rely on rectangular blocks may fail to identify forgeries in which the forgery target is picked freely. A unique mechanism has been devised

in this work to identify such forgery. The suggested method extracts features using a block-based Intensity Coherence Vector (ICV). In contrast to traditional block-based approaches, the suggested method identifies the fabricated areas by superimposing and discriminating between two copies of the suspect picture. With this cutting-edge method, the forgery detection operation's success rate is unaffected by the intensity of the post-processing distortions. High average success rates and steady detection performance against diverse post-processing activities designed to make detecting fraud harder, are the parameters by which the effectiveness of this study is judged into detecting freeform copy-move forgery.

3.1 Matching of the Similar Regions

A necessary condition is that B is an odd integer. In order to implement the suggested method, the suspect picture is first gray scaled, and then partitioned into overlapping square blocks of size B. Each block in the matrix is vectorized, then turned to a row vector. Each of these vectors has a deciding factor removed from the rest of the constituents. And then the absolute values of the numbers are obtained when subtracted. Similarly, sums of basic significance are calculated for other vector characteristics [22]. However, this mask has been adjusted such that all indices are 0. Assigning a value of chosen location, immediately marks the region that was selected on the original picture on the mask that was generated.

3.2 Intensity Coherence Vector

According to the luminance (intensities) of the picture's pixels, they may be categorized as either coherent or incoherent, yielding the image vector [23]. A pixel is considered coherent if it is part of a big, neighbouring group of pixels that all have the same or very comparable brightness, and incoherent otherwise.

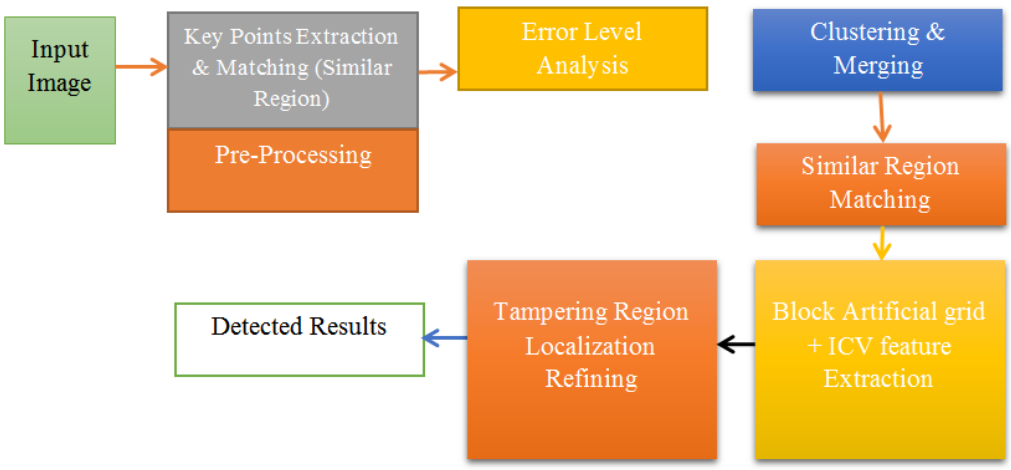

Figure 2. Proposed hybrid block matching technique

The power coherence measures the number of neighbouring pixels that have the same or very comparable brightness levels over wide areas. The presence of coherent sections has been interpreted as a block's fingerprint. Figure 2 contains the block of hybrid block matching techniques.

3.3 Measurements for similar region in the matrix

To begin, the neighbouring locations that are similar are identified. After averaging one picture and superimposing it on the other, overlapping areas are calculated. At this point, it is anticipated that two objects, one of which is a duplicate of the other, will overlap. Aside from that, the absolute value is calculated as the difference between the two objects' areas being equal. This allows for immediate acquisition of a differential picture. Following this, a two-dimensional filtering strategy is performed to this differential picture in an effort to remove any remaining noise. The regions on the differential picture where neighbouring pixels have values below the forgery phenomena are then identified [24].

It has become vital to analyse the efficacy of this algorithm using many metrics. It is not required to distinguish between the copied and pasted areas in order to employ the copy-move forgery detection techniques [25].

4. Comparative Observations

It is ensured that this study would clearly show whether or not the proposed method retains its stability when the distorted forgery is further processed. Table 1 and Figure 3 shows the experimental results obtained, which demonstrate that this method maintains a consistent performance regardless of the JPEG quality level, in contrast to the traditional approaches.

Table 1. Results obtained

Method	Block Matching size				Performance Metrics		Overall Efficacy
	8x8		12x12				
	TP	FP	TP	FP	Accuracy	Precision	
Transformation Technique	0.69	0.3	0.58	0.4	78.2%	75%	79%
Hybrid Bilateral Technique	0.75	0.21	0.63	0.33	82.1%	84.3%	83%
Proposed Hybrid Block Matching ICV Method	0.93	0.03	0.95	0.01	96.6%	95.3%	98%

These false positive, and true positive rates are all above average, and the accuracy rates are rather high, regardless of whether the JPEG compression operation is performed with a variety of quality factors, a Gaussian filtering operation, or a mix of the two. It must be noted that some of the increases and decreases agree with the findings of this detection approach.

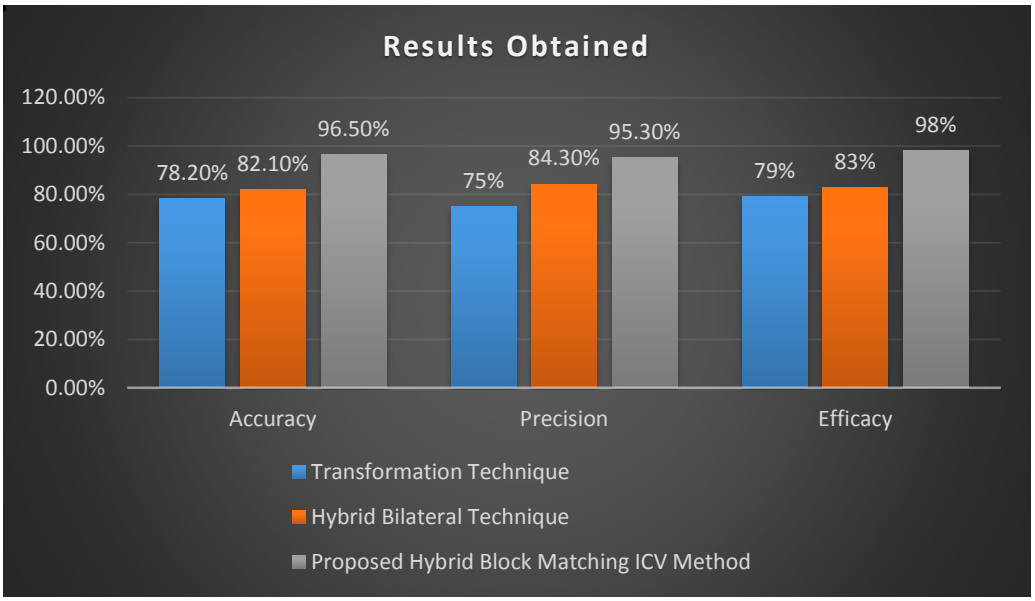

Figure 3. Graphical representation of the results obtained

Trials are conducted on the forged photos using numerous versions of the postprocessing processes, despite the fact that none of the previous research did so. In other words, its efficacy is shown over a spectrum of experimental conditions by comparing its success and failure rates to those of previous investigations. It is also important to note that, it was unable to replicate the positive outcomes shown in the aforementioned research [18-26] when the traditional block-matching approach was used.

5. Conclusion

This research article has focused on debunking the two most common forms of photo tampering: copy-move and splicing forgery; for example, highlight the regions in question. In addition, it is related to other blocks; however, unlike other methods, a fresh and original mathematical methodology has been used to identify free-form copy-move fraud by focusing on immediately detecting the full suspect region. To identify areas where authentication has been compromised, a unified approach based on the Intensity Coherence Vector has been suggested. The picture quality score was employed as a coefficient in this technique and was

used to build characteristics such as JPEG block fake grids and local noise differences. The experimental findings verify the good quality and compression ratio of the images generated by this method. It is believed that the proposed approach has an edge over similar algorithms in the market and can be used in a wider variety of contexts. The next phase of this research is to put the suggested approach to the test on a larger dataset of photographs of varying formats.

References

[1] Soad Samir, Eid Emary, Khaled Elsayed, Hoda Onsi, Copy-Move Forgeries Detection and Localization Using Two Levels of Keypoints Extraction, Journal of Computer and Communications, Vol.7 No.9, September 2019, DOI: 10.4236/jcc.2019.79001.

[2] A. Kashyap, R. S. Parmar, M. Agrawal, and H. Gupta, "An Evaluation of Digital Image Forgery Detection Approaches," arXiv preprint arXiv:1703.09968, 2017.

[3] N. K. Gill, R. Garg, and E. A. Doegar, "A review paper on digital image forgery detection techniques," in Computing, Communication and Networking Technologies (ICCCNT), 2017 8th International Conference on, 2017, pp. 1-7.

[4] T. M. Mohammed, J. Bunk, L. Nataraj, J. H. Bappy, A. Flenner, B. Manjunath, et al., "Boosting Image Forgery Detection using Resampling Detection and Copy-move analysis," arXiv preprint arXiv:1802.03154, 2018.

[5] O. Mayer and M. C. Stamm, "Accurate and Efficient Image Forgery Detection Using Lateral Chromatic Aberration," IEEE Transactions on Information Forensics and Security, 2018.

[6] H. A. Alberry, A. A. Hegazy, and G. I. Salama, "A fast SIFT based method for copy move forgery detection," Future Computing and Informatics Journal, vol. 3, no. 2, pp. 159-165, 2018.

[7] A. Novozámský and M. Šorel, "Detection of copy move image modification using JPEG compression model," Forensic science international, vol. 283, pp. 47-57, 2018.

[8] A. Parveen, Z. H. Khan, and S. N. Ahmad, "Blockbased copy–move image forgery detection using DCT," Iran Journal of Computer Science, vol. 2, no. 2, pp. 89-99, 2019.

[9] J. A. Redi, W. Taktak, and J.-L. Dugelay, "Digital image forensics: a booklet for beginners," Multimedia Tools and Applications, vol. 51, no. 1, pp. 133–162, 2011.

[10] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 1099–1110, 2011.

[11] N. Warif, A. Wahab, M. Idris, R. Ramli, R. Salleh, S. Shamshirband, K. Choo, Copy-move forgery detection: survey, challenges and future directions. J. Netw. Comput. Appl. 75, 259–278 (2016)

[12] M. Zandi, A. Mahmoudi-Aznaveh, A. Talebopur, Iterative copy-move forgery detection based on a new interest point detector. IEEE Trans. Inf. Forensics Secur. 11(11), 2499–2512 (2016)

[13] M. Ikhalyel, M. Hariadi, K.E. Pummama, A study of copy-move forgery detection based on segmentation. IJCSNS Int. J. Comp. Sci. Netw. Secur. 18(7), 27–32 (2018)

[14] J. Zheng, Y. Liu, J. Ren, T. Zhu, Y. Yan, H. Yabf, Fusion of block and keypoints based approaches for effective copy-move image forgery detection. Multidim. Syst. Sign. Process. 24(4), 989–1005 (2016)

[15] S.S. Ali, I.I. Ganapathi, N.S. Vu, S.D. Ali, N. Saxena, N. Werghi, Image Forgery Detection Using Deep Learning by Recompressing Images, Electronics 11(3), 403 (2022).

[16] E.U.H. Qazi, T. Zia, A. Almorjan, Deep LearningBased Digital Image Forgery Detection System, Appl. Sci., 12, 2851 (2022).

[17] S. Nath, R. Naskar, Automated image splicing detection using deep CNN learned features and ANN-based classifier, Springer-Verlag London ltd., part of springer nature (2021).

[18] Y. Rao, J. Ni, Deep learning local descriptor for image splicing detection and localization, IEEE access, vol. 8 (2020).

[19] R. Davarazni, K. Yaghmaie, S. Mozaffari, Copy-move forgery detection using multiresolution location binary patterns. Forensic Sci. Int. 231(1), 61–72 (2013)

[20] Eman I. Abd El-Latif, A. Taha, Hala H. Zayed, A passive approach for detecting image splicing using Deep Learning and Haar Wavelet Transform, Arabian journal for science and engineering, vol. 6 (2020).

[21] S. Saleem, A. Dilawariand U.G. khan, Multimedia Forensic: An approach for splicing detection based on deep visual features, 2019 international conference on robotics and automation in industry (ICRAI) (2019).

[22] Y. Rao, J. Ni, A deep learning approach to detection of splicing and copy-move forgeries in images, 2016 IEEE international workshop on information forensics and security (WIFS) (2016).

[23] E. Ardizzone, A. Bruno, G. Mazzola, Copy-move forgery detection by matching triangles of keypoints. IEEE Trans. Inf. Forensics Secur. 10(10), 2084–2094 (2015).

[24] Zhang, Zhongping & Zhang, Yixuan & Zhou, Zheng & Luo, Boundary-based image forgery detection by fast shallow CNN, conference: computer vision and pattern recognition Doi: 10.11.09/ICPR (2009).

[25] C.M. Pun, X.C. Yuan, X.L. Bi, Image forgery detection using adaptive oversegmentation and feature points matching. IEEE Trans. Inf. Forensics Secur. 10(8), 1705–1716 (2015).

[26] J. Li, X. Li, B. Yang, X. Sun, Segmentation-based image copy-move forgery detection scheme. IEEE Trans. Inf. Forensics Secur. 10(3), 507–518 (2015).

[27] Gill, Navpreet & Garg, Ruhi & Doegar, Amit. (2017). A review paper on digital image forgery detection techniques. 1-7. 10.1109/ICCCNT.2017.8203904.

Author's biography

P. Ebby Darney is working as an Associate Professor in the Department of Electrical and Electronics Engineering, RajaRajeswari College of Engineering, Bangalore, India. His area of research includes Image Processing, Artificial Intelligence, Control Systems, Radio Networks, and cloud computing.