

ISSN: 2321-3914 Volume 3 Issue 2 August 2022 Impact Factor: 10.2 Subject Computer Science

TEXTUAL FEATURE EXTRACTION METHOD USED IN THE COPY-MOVE FORGERY DETECTION APPROACH

Nikita Dubey

Research Scholar

DECLARATION: I AS AN AUTHOR OF THIS PAPER / ARTICLE, HEREBY DECLARE THAT THE PAPER SUBMITTED BY ME FOR PUBLICATION IN THE JOURNAL IS COMPLETELY MY OWN GENUINE PAPER. IF ANY ISSUE REGARDING COPYRIGHT/PATENT/ OTHER REAL AUTHOR ARISES, THE PUBLISHER WILL NOT BE LEGALLY RESPONSIBLE. IF ANY OF SUCH MATTERS OCCUR PUBLISHER MAY REMOVE MY CONTENT FROM THE JOURNAL WEBSITE. FOR THE REASON OF CONTENT AMENDMENT/ OR ANY TECHNICAL ISSUE WITH NO VISIBILITY ON WEBSITE/UPDATES, I HAVE RESUBMITTED THIS PAPER FOR THE PUBLICATION. FOR ANYPUBLICATION MATTERS OR ANY INFORMATION INTENTIONALLY HIDDEN BY MEOR OTHERWISE, I SHALL BE LEGALLY RESPONSIBLE. (COMPLETE DECLARATION OF THE AUTHOR AT THE LAST PAGE OF THIS PAPER/ARTICLE)

Abstract

The problem of fake images has expanded to all corners of the globe and is mostly due to internet entertainment. But, they are also making it possible for an engaged reaction to be offered to overcome it. Modern developments have given this problem both the means and the aid to conquer it. One of these arrangements makes use of sophisticated convolutional learning computations. They have been demonstrated to be effective in preventing visual imitations produced by generative unfriendly networks (GANs). With this type of tactic, the image is altered to the point where it almost disappears as a fake and seems to be identical to the original image. The current evaluation examines the identification of copy-move fabrications utilising a combination handling model made up of an unfavourable model and a significant convolution model. The growing popularity of the web demonstrates how much faster and easier it is to communicate via electronic sight and voice. This implies that this sight and sound may now be manipulated through deception as well. Copy-move duplication is a specific type of forging that frequently includes editing images.

Keywords: Copy-Move, convolution model, Detection, Extraction, Textual Feature

I. INTRODUCTION

The human mind is more strongly influenced by visual images. A image is unquestionably more powerful than many words. We only accept what we can see. Modern data innovation has made digital images widely accessible. There are several tools available for handling



ISSN: 2321-3914 Volume3 Issue 2 August 2022 Impact Factor: 10.2 Subject Computer Science

pictures. Software like Photoshop and Corel Draw may be used to edit images, but the unaided eye cannot notice these changes. In fact, even novices with a very limited understanding of these tools may make modest changes to images. Although most people use these tools to enhance images, they may also be used to make major alterations that result in incorrect translation[1]. Fake photos can be used to deceive people in a variety of contexts, including news stories, magazines, and websites. As a result, numerous methods for thoroughly examining the veracity of images are developed to avoid such circumstances. Although copymove imitation is difficult to spot, it is frequently employed. Several academics promoted different ways to identify copy-move fraud. Computerized picture falsification detection methods may be divided into two categories: dynamic methodology and uninvolved methodology. Dynamic methodologies need previous knowledge about the scene. Dynamic approaches ask for the creation of a watermark or mark while receiving images. Given this requirement, dynamic processes must be used in particular situations. Sometimes inactive methods are referred to as "blind imitation detection" procedures since they don't need any prior knowledge of the image. The five different categories of passive approaches rely on physical science, geometry, physical designs, cameras, source camera ID, and pixels. When photography was first conceptualised, images have been modified and altered. In recent years, a lot of digital image data was altered and used in newspapers, sensational stories, style magazines, court films, and other media. Finding photo misrepresentation is a difficult task because of the many ways that pictures may be altered and the large range of fascinating picture-catching inventions available. The majority of fake detection methods fall into one of two groups: dynamic or inert. Dynamic processes, which are sometimes referred to as nonvisually impaired or intrusive approaches, call for the consolidation of information in the initial image. This fundamental causes the extension of dynamic tactics to be constrained. Some techniques include using the camera's advanced mark and watermarking. Latent approaches, also referred to as non-meddling or blind procedures, don't require any information to be implanted in the electronic image. A digital image can be falsified using a variety of adjustments, including rotation, scaling, resizing, noisy expansion, concealing, and pressure. Copy-move imitation is one type of visual deception in particular.

The development of computerised images as a reliable source of data is due to advancements in imaging technology. The wide range of picture control systems now available raises



ISSN: 2321-3914 Volume 3 Issue 2 August 2022 Impact Factor: 10.2 Subject Computer Science

concerns about the validity of photos. The goal of visual substance fabrications is to stage the changes so that they are difficult to spot with the unaided eye and then use these items for evil [2]. For instance, a legal analysis conducted in 2001 following the 9/11 attack revealed that some accounts of Osama bin Laden being loaded into a canister via virtual entertainment were false. Similar to how a picture of a tiger in the wild in 2007 forced people in Shanxi, China, to recognise the existence of tigers. The criminological evaluation, however, revealed that the tiger was a "paper tiger." Similar to this, it was discovered in 2008 that a government photograph showing four Iranian long-range missiles had been altered due to the duplication of one rocket. Hence, the adage "reality may be stranger than fiction" is now untrue. Finding methods to guarantee the accuracy of the images is crucial in this regard, especially in proofloped applications. Web-based entertainment is experiencing an increase in the popularity of the hotly contested topic known as "counterfeit news," which is defined as data that has been altered to reflect a specific plan. For some people, web-based entertainment has replaced traditional news sources as their primary news source. In order to encourage the creation of fake news, altered images are frequently shown together with the reports they are associated with. The ability to spread false information has increased recently for two main reasons: first, the cost of critical image creation technology (such as mobile phones and digital cameras) has decreased; and second, image editing software is presently widely available owing to opensource hardware and software. Nowadays, anyone with a smartphone or computerised camera, as well as internet access to the necessary programming, may efficiently and moderately edit images in any situation. Because to internet connectivity, the photos may also be transferred across an almost infinite number of platforms, where they can subsequently be further edited using specialised symbolic software (like Photoshop) using capabilities like grafting, painting, or copy-move falsifications.

II. REVIEW OF LITREATURE

The primary characteristic of copy-move phoney is the similarity of the copied fix and the stalled fix. Hence, comprehensive hunt is one approach of imitation detection Yadav, Preet 2016 Nevertheless; the method isn't practical due to its complicated processing requirements.

In any case, the majority of detection methods are founded on the link that the reordered region was shown to have. Only uninvolved detection algorithms are discussed here Bayram



ISSN: 2321-3914 Volume 3 Issue 2 August 2022 Impact Factor: 10.2 Subject Computer Science

2017Fridrich et al. developed a block matching strategy in consideration of the discrete cosine change (DCT). In this approach, the picture's covering bits were separated into quantized DCT coefficients, which were then used as features. [3] After lexicographically organising the data, duplicated segments were constructed with an eye towards quality comparison.

An important benefit of adopting DCT is that the majority of the energy is focused on a small number of DCT coeficients. Popescu et al2016 .'s Head Part Examination (PCA) was used in this technique to reduce the number of factors, creating a system similar to Fridrich's. The number of features that were supplied was only around 50% of Fridrich's. The method's drawback is that it doesn't work when the cloned locale is rotated or scaled differently.

Li et al. 2018 developed an organised neighbourhood strategy utilising Specific Worth Decay and Discrete Wavelet Change (DWT) (SVD). The DWT reduces aspect, which speeds up the entire cycle, but this method uses a lot of Computer power because it takes a while to calculate the SVD. Hao-Chiang Hsu et al. [4] suggested using feature extraction using the Gabor ilter to consider characteristics in order to differentiate copy-move extortion.

Leida Li et al. 2019 developed a method for detecting copy-move fabrication using neighbourhood double pattens. M.Qiao et al. 2019 utilised curvelet measurements to identify copy-move extortion after the image was divided into different covering blocks. Examples of local visual characteristics that can withstand various mathematical transformations, such as turn, obstacles, mess, and scale, are SRF, Filter, and GLOH.

As a result, they are frequently used to tell between picture fabrications. Hwei-Jen Lin et al. (2018) introduced a block-based method with radix sort for quick copy-move phoney detection to increase computational productivity. Nevertheless, this strategy only works well against JPEG pressure attacks and Gaussian clamour. Amerini et al. (2011) discuss how to differentiate copy-move deception using a filter-based technique.

III. PROPOSED METHODOLOGY



ISSN: 2321-3914 Volume3 Issue 2 August 2022 Impact Factor: 10.2 Subject Computer Science

The DCT and Gaussian RBF component PCA with squared blocks are used in this work to identify copy-move extortion. As it is a continual practise in picture duplicating to continuously expose the fabricated images to various post handling procedures, the adaptability against distinct post handling duties, like pressure, concealing, scaling, and clamour, is the justification for adopting the DCT for block portrayal. As a result, fraud detection becomes extremely difficult. Notwithstanding the DCT's strong opposition to the aforementioned modifications, there are a few circumstances in which the block representations obtained from the DCT will be acceptable. For instance, if turn activity is used over the created districts, the outcomes of the DCT depictions will also be affected. We employ Gaussian RBF bit PCA over them to get over this restriction since DCT recurrence coefficients, in contrast to PCA, are revolution invariant. One further defence against using section PCA with DCT is provided by nonlinear RBF piece PCA with direct DCT. As a result, it increases the diversity of the feature depiction and also seems like a better option than PCA, which is also direct in nature like DCT. [5] Also, because Gaussian RBF bits must only have piece values in the range of 0 to 1, they are mathematically simpler due to the fact that they have fewer hyper borders.

a) Framework of the Proposed Algorithm.

The information presented above sheds light on the CMFD design seen in Figure 2. The steps of the recommended CMFD approach are as follows:

- (1) Dividing the greyscale picture into blocks that overlap and have predetermined sizes.
- (2) Applying DCT to every deleted block.
- (3) Extracting the Gaussian RBF kernel PCA-based features from each DCT square block.
- (4) Comparable block matching pairings.
- (5) Removing the isolated block and ejecting the duplicated sections

b) Pre-processing and Blocks Extraction.



ISSN: 2321-3914 Volume 3 Issue 2 August 2022 Impact Factor: 10.2 Subject Computer Science

The suggested approach is applied to greyscale images using the computation. As a result, a colour input image I of size HW is first converted into a greyscale image using

I = 0.229R + 0.587G + 0.114B

As a result, the tones red, green, and blue are each represented separately in figure I by R, G, and B. A window of size just one pixel is moved from the top left corner to the bottom right corner of picture I after it has been converted to greyscale to get the covering blocks. [6] As seen in, each block is referred to as Brc, where r and c denote the block's specific line and section beginning regions.

$$Brc(x, y) = f(x + c, y + r)$$

where $x, y \in \{0, ..., Brc - 1\}, r \in \{1, ..., H - h + 1\}$, and $c \in \{1, ..., W - w + 1\}$. Thus, *I* can be divided into N overlapping blocks as shown in

 $\mathbf{N} = (H - h + 1) \times (W - w + 1)$

c) Block Representation Details

In our execution, each block has a size of HW, where h and w have opposite upsides of 16. Block Bi is subjected to the DCT, producing a coefficients lattice C with a comparable size. Next the Gaussian RBF component PCA is used to further alter this network. The first 10 educationally important components may be recovered using (16), and these components are then utilised to create the feature vector for the block depiction. [7] We chose these 10 fundamental components since there are many blocks and the curse of dimensionality, which increases computation time, force us to limit the size of the feature vector. Another explanation is that the rule part inquiry uses a symmetrical straight change, which makes it appear as though the major head part has the most fluctuation, according to some projections, and that the second-most significant difference has the highest change, etc. As the feature components in our execution, the 10 crucial components that provide the finest data are chosen.



ISSN: 2321-3914 Volume 3 Issue 2 August 2022 Impact Factor: 10.2 Subject Computer Science

Methods	Feature	Feature length
Fridrich et al.	DCT	2.3
Bayram et al.	FMT	4.5
Popescu and Farid	PCA	6.5
Huang et al.	Improved DCT	7.2
Proposed technique	DCT and KPCA	8.3

 Table 1: Comparison of computational complexity

d) Forgery Detection

Finding duplicated districts that are not covering and where the comparability file between the locales (feature vectors) is below a certain limit is the goal of the CMFD. The concept of counterfeit images, which undergo post-processing procedures, is what inspired the use of location-based constraints; the likelihood that they would have identical characteristics is virtually nonexistent. [8] The blocks should not cross or overlap, and the comparability file should not be greater than a predetermined threshold, are the two requirements placed on the cloned block detection method for CMFD.

The matching between non-overlapping blocks, which is the basic condition of the CMFD, is achieved by using the shift distance requirements. For this, we should anticipate that the orientations of the top left corners of the two blocks that each feature vector fVi and fVj separately address are (xi, yi) and (xj, yj).

$$\forall \sqrt{\left(x_i - x_j\right)^2} + \left(y_i - y_j\right)^2 \ge N_t$$

If the two feature vectors satisfy proviso (18), we shall take that into consideration when determining the likeness record to satisfy the CMFD's statement (2). Thus, the Euclidean distance is used as



ISSN: 2321-3914 Volume 3 Issue 2 August 2022 Impact Factor: 10.2 Subject Computer Science

$$d(fv_{i}, fv_{i}) = \sqrt{\sum_{k=1}^{10} (fv_{ik} - fv_{ik})^{2}} < d_{t}$$

The method creates a realistic dark guide to handle the effects of fraud detection, and the sections that are thought to be copies are highlighted as the best outcome.

e) Morphological Operation

The size of the primary component has no bearing on the morphological opening and closing duties that are done to IO without excluding any suitable characteristics to display the calculation's final detection result. [9] Next, using an initial activity with a primary component of size 33, the small and unneeded blocks of IO are deleted, and the gaps in the highlighted regions of I are filled using an end activity with an underlying component of size 88.

f) Computational Analysis

For the system's obvious display, we are taking on a few common documentations that are mentioned in the processing message. Assume that there are N absolute blocks, each of which were initially hw and is now nn in size. H = w = 16. In the initial stage, we process the 2D discrete cosine change for a single block in O(n log n)-time. After registering the DCT for a single block, we use the O(n2)-fast Gaussian RBF component PCA. [Hence, the number of machine instructions required to calculate the features for a single block is O(n2 + n log n), and as a result, we are only interested in the problem with the highest consider time complexity. [10] The feature lattice Mkpc is produced in O(Nn2) time when the block portrayal approach is used to N. After that, Mkpc does lexicographical arrangement, which requires O(N log N) processing time. N being more than n or even n2, O(Nn2 + N log N) is the time required to run the machine rules (N log N). Block correlation is required by the approach, which has a substantial impact on the calculation's temporal complexity. As a result, the temporal complexity of the computation is still O(N log N), but the total quantity of machine instructions needed is O(N(n log n + n2) + N log N + N).

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS



ISSN: 2321-3914 Volume3 Issue 2 August 2022 Impact Factor: 10.2 Subject Computer Science

The trial findings from the suggested approach are provided in this section. An Intel 1.70 GHz Core i5 computer processor, MATLAB 2011, and Adobe Photoshop are used to carry out the research on a plate structure. The effectiveness of the suggested technique is assessed using two datasets. Greyscale images with a resolution of 128 by 128 pixels from the DVMM Columbia College collection were used. The images in the second dataset, which includes images with 256 by 256 and 512 by 512 pixel resolutions, were downloaded from the Internet. Where necessary, we establish the boundary parameters for the analysis to include B (the current block), size h w = 16 16, dt (the comparability distance between vectors) = 0.0015, Nn (the number of columns to look at), Nt (the block distance limit), and Nc (the number of head parts). The supplemental portions include interesting facts regarding the examination.

a) Performance Evaluation

Overall, the most important characteristic of a detection approach is its capacity to distinguish between authentic and fake pictures. Additionally, the ability to precisely locate the phoney location is a crucial piece of evidence that may be used to debunk digital impersonations. In this way, the effectiveness of our approach is assessed at two different levels: at the image level, where we emphasise if the detected picture is indeed a fashioned picture, and at the pixel level, where we assess how clearly the formed segments can be found. To demonstrate the accuracy of the suggested technique at the picture level, the accuracy calculation "p" shows the likelihood that a supposedly fraudulent item is indeed an imitation, and the review "r" denotes the possibility that a produced image is discovered:

$$p=\frac{T_P}{T_p+F_P}$$

$$r = \frac{T_P}{T_p + F_n}$$

where TP is the total number of fake images that were successfully identified, FP is the total number of real photos that were mistakenly identified as fake, and Fn is the total number of fake photos that were missed.

b) Effectiveness Testing



ISSN: 2321-3914 Volume3 Issue 2 August 2022 Impact Factor: 10.2 Subject Computer Science

In order to determine if the suggested computation is enough, the primary analysis for recognising copy-move imitation is focused on pictures where the created region is supposed to be another section of the picture.

Any post-handling that has ever been done to the images used in this study has never been done. Dataset I had images in grayscale that were 128 pixels by 128 pixels, which we selected. The first, generated, and final images are arranged from left to right in Figure 1 to show the examination's detection finds. Figure 3 demonstrates the abundance of similar and challenging-to-identify areas. In any event, the constructed localities were successfully identified by the programme. In the next test, we selected a few variety images from dataset-II with 512 by 512 pixel aspects. [11] The first, fashioned, and final images in Figure 2 display the results of the detection and are arranged from left to right. Figure 2 demonstrates how the fake items are all inconsistent, but the programme was able to identify them with accuracy.

	$w = 5 \delta = 0.5$		$w = 5 \delta = 1$	
	24	40X40	24X24	40X40
	X24			
Precision	2.362	1.256	2.365	3.695
(p)				
Recall	2.598	1.968	3.584	4.589
(r)				
TPR	3.452	2.485	3.999	5.369
FPR	4.235	3.562	4.523	6.256

Table 1: Results of detection with Gaussian blending



ISSN: 2321-3914 Volume3 Issue 2 August 2022 Impact Factor: 10.2 Subject Computer Science



Figure 1: Results of detection with Gaussian blending

c) Robustness and Accuracy Test of the Algorithm

Free / Unpaid

Peer Reviewed

National

Multidisciplinary

A forger often uses picture-altering programmes to his best ability to create a fashioned image. In order to accomplish some goal, a forger persistently uses post-processing techniques including concealing, disturbance, and pressure to create incoherent falsified photographs. Another type of picture treatment is called different copy-move phonies, in which there are numerous duplicated segments.

In this section, these factors are taken into consideration. We also provide a few examples to show the precision and strength of the computation. Nevertheless, Figures 2 do not provide comparison preliminary results when presenting the discoveries of fake detection. The guidelines for identifying different copymove fakes are provided in Figure 2.

In order to objectively assess the accuracy and potency of the suggested technique, 100 real photos from the two databases are explored to create produced images. With a chosen real image as a starting point, a square segment with a size of 24×24 pixels is copied from an unreliable position and pasted onto a nonoverlapping area to create four convincingly realistic fake images. [12] Using the same method as before, four more tempered images are created for the selected image using the squared area of size 40 40 pixels. As a result, the 800-picture collection of fake images is created for the chosen real photos. These fake and real images are subsequently ruined using postprocessing techniques including Gaussian concealing, AWGN, and JPEG pressure. Tables 2-4 summarise the findings and discuss the calculation's accuracy and adaptability at the pixel level.



ISSN: 2321-3914 Volume3 Issue 2 August 2022 Impact Factor: 10.2 Subject Computer Science

The results shown in Tables 2-4 demonstrate that a larger copied zone would enhance detection execution. Table 2 demonstrates that the computation works well when the images are hidden by Gaussian concealing. In any case, when the images are of poor quality (w=5, =1) and contain a little amount of falsification (24 24 pixels), our method only misses 14 out of 800 frauds (r = 0.980).

Items	SNR - 35 dR		SNR –	$40 \mathrm{dR}$
items	SINK = 35 ub		SINK = 40 uD	
	24 ×	40 ×	24 ×	40 ×
	24	40	24	40
Precision	3.62	2.36	3.35	4.23
(p)				
Recall	4.25	3.56	4.36	5.36
(r)				
TPR	5.36	4.25	5.23	6.23
FPR	6.23	5.63	6.23	7.25

Table 2: Detection results with AWGN.



Figure 2: Detection results with AWGN.



ISSN: 2321-3914 Volume 3 Issue 2 August 2022 Impact Factor: 10.2 Subject Computer Science

Q = 80		Q = 90	
24×24	40 × 40	24×24	40 × 40
3.62	4.22	5.36	4.66
4.25	5.36	5.96	5.89
5.89	6.88	6.02	6.88
6.89	7.36	7.23	9.23
	Q = 80 24 × 24 3.62 4.25 5.89 6.89	$Q = 80$ 24×24 40×40 3.62 4.22 4.25 5.36 5.89 6.88 6.89 7.36	$Q = 80$ $Q = 90$ 24×24 40×40 24×24 3.62 4.22 5.36 4.25 5.36 5.96 5.89 6.88 6.02 6.89 7.36 7.23

 Table 3: Detection results with JPEG compression

Table 3 shows that the method also performed well with AWGN-misshaped images. [13] According to Table 3, the suggested approach is also capable of accurately identifying produced segments in images that have been simply packed and have a quality component of 80 or 90.

According to the most recent analysis, the suggested method differs from DCT-based, PCAbased, FMT-based, and further refined DCT-based techniques. For this, we selected 100 real, 512×512 pixel photos and created 400 fashioned images from them. In order to create two very unique fake photos, a square segment of 48×48 pixels is copied from an uneven place and pasted into a no-covering zone.

V. CONCLUSION

Experts looked at several picture-faking techniques. Before copy-glue fabrication detection techniques, we evaluated them. The suggested method makes use of DWT and Filter. DWT consolidates the image data before only cycling the pertinent data thereafter (low requency data). The Filter shown strength. The repeated portion is rotated or enlarged before being set, thus the suggested technique detects picture duplication in any case. For a data set of 100 images, the overall accuracy was 94%. (50 real photos and 50 created images). In this, both based strategies and feature-based tactics have been examined. The cell automata is a completely clever approach, even if some arrangements of features, such as DCT/DWT coefficients, PCA (Head Part Examination), or Zernike minutes, are thought to be used in



ISSN: 2321-3914 Volume3 Issue 2 August 2022 Impact Factor: 10.2 Subject Computer Science

block-based techniques[14]. Block-based computations are useful for locating copied segments, but their accuracy when used on objects that have been mathematically altered is still lacking. To get around this problem, feature-based approaches are used to match features in the image. In this, the cloned segment-applicable scaling, turn, mutilation, and mix adjustments have been investigated.

VI. FUTURE SCOPE

The suggested method may be tested in the future on various images, and feature vectors can be extracted by using a surface feature extraction technique. Moreover, comparison features may be applied to several aspects of image management, such as example recognition, medical imaging, face identification, and others, to spot misrepresentation. [15] Future study may include expanding the preparation dataset, evaluating the effects of additional hyperparameters on classifier performance, and combining a feature extraction stage based on deep learning with a stage of image pre-handling that makes use of space change (such DFT, DCT, and DWT).

REFERNCES

- I. Amerini, L. Ballan, R. Caldelli, A.D. Bimbo, G. Serra, A sift-based forensic method for copy-move attack detection and transformation recovery. IEEE Trans. Inf. Forensics Secur. 6(3), 1099–1110 (2011)
- 2. J.C. Lee, C.P. Chang, W.K. Chen, Detection of copy-move image forgery using histogram of orientated gradients. Inf. Sci. 321, 250–262 (2015)
- 3. J.W.G. Wang, J. Liu, A. Zhang, Y.W. Dai, Z.Q. Wang, Fast and robust forensics or image region-duplication forgery. Acta Automat., Sinica 35(12), 1488–1495 (2009)
- 4. L. Li, S. Li, H. Zhu, X. Wu, Detecting copy-move forgery under affine transforms for image forensics. Comput. Electr. Eng. 40(6), 1951–1962 (2014)
- 5. M. Al-Qershi Osamah, B.E. Khoo, Passive detection of copy-move forgery in digital images: state-of-the-art. Forensic Sci. Int. 23(1), 284–295 (2013)
- 6. R. Davarazni, K. Yaghmaie, S. Mozaffari, Copy-move forgery detection using multiresolution location binary patterns. Forensic Sci. Int. 231(1), 61–72 (2013)



ISSN: 2321-3914 Volume 3 Issue 2 August 2022 Impact Factor: 10.2 Subject Computer Science

- S. Bravo-Solorio, A.K. Nandi, Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics. Signal Process. 91(8), 1759– 1770 (2011)
- 8. S.J. Ryu, M. Kirchner, M.J. Lee, H.K. Lee, Rotation invariant localization of duplicated image regions based on Zernike moments. IEEE Trans. Inf. Forensics Secur. 8(8), 1355– 1370 (2013)
- 9. S.J. Ryu, M.J. Lee, H.K. Lee, in Information Hiding. Detection of copy-rotate-move forgery using Zernike moments (Springer-Verlag, Berlin, 2010), pp. 51–65
- 10. X. Pan, S. Lyu, Region duplication detection using image feature matching. IEEE Trans. Inf. Forensics Secur. 5(4), 875–867 (2010)
- X. Wang, X. Zhang, Z. Li, S. Wang, in 3rd Int. Conf. on Multimedia Information Networking and Security. A DWT-DCT based passive forensics method for copy-move attacks (2011), pp. 304–308
- 12. Y. Huang, W. Lu, W. Sun, D. Long, Improved DCT-based detection of copy-move forgery in images. Forensic Sci. Int. 206(3), 178–184 (2011)

Author's Declaration

I as an author of the above research paper/article, hereby, declare that the content of this paper is prepared by me and if any person having copyright issue or patent or anything otherwise related to the content, I shall always be legally responsible for any issue. For the reason of invisibility of my research paper on the website/amendments /updates, I have resubmitted my paper for publication on the same date. If any data or information given by me is not correct I shall always be legally responsible. With my whole responsibility legally and formally I have intimated the publisher (Publisher) that my paper has been checked by my guide (if any) or expert to make it sure that paper is technically right and there is no unaccepted plagiarism and the entire content is genuinely mine. If any issue arise related to Plagiarism / Guide Name / Educational Qualification /Designation/Address of my university/college/institution/ Structure or Formatting/ Resubmission / Submission / Copyright / Patent/ Submission for any higher degree or Job/ Primary Data/ Secondary Data Issues, I will be solely/entirely responsible for any legal issues. I have been informed that the most of the data from the website is invisible or shuffled or vanished from the data base due to some technical fault or hacking and therefore the process of resubmission is there for the scholars/students who finds trouble in getting their paper on the website. At the time of resubmission of my paper I take all the legal and formal responsibilities, If I hide or do not submit the copy of my original documents (Aadhar/Driving License/Any Identity Proof andAddress Proofand Photo) in spite of demand from the publisher then my paper may be rejected or removed from the website anytime and may not be consider for verification. I accept the fact that as the content of this paper and the resubmission legal responsibilities and reasons are only mine then the Publisher (Airo International Journal/Airo National Research Journal) is never responsible. I also declare thatif publisher finds any complication or error or anything hidden or implemented otherwise, my paper may be removed from the website or the watermark of remark/actuality may be mentioned on my paper. Even if anything is found illegal publisher may also take legal action against me

Nikita Dubey