ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

# BLOCK BASED IMAGE FORGERY DETECTION TECHNIQUES

**Anil Dada Warbhe [*], Rajiv V. Dharaskar, Vilas M. Thakare**
[*] Department of Computer and Information Technology, MIET, Gondia
Former Director, Disha Education Society (DIMAT - Disha Technical Campus), Raipur, CG
Post Graduate Department of Computer Science, SGB Amravati University, Amravati.

## ABSTRACT

Since the day of an advent of the internet and the World Wide Web digital images started playing an important role in exchanging ideas and sharing the information. Today it's hard to imagine the world of web without digital images right from simple personal web page to giant web applications. Mobile applications like WhatsApp also became the important means of the communication on which very often multimedia content is used to spread the word. But at the same time these digital images are vulnerable in the sense that, it can be easily manipulated to conceal or change the meaning. It could be dangerous, if these forgeries been done with malicious intentions. Hence it's very important to know and prove the authenticity of the digital images. From last few years, research community is contributing towards addressing this issue. In this survey paper we are presenting a review on copy-move forgery detection by dividing the image into the block of particular size and processing these blocks to identify the forgeries.

## INTRODUCTION

The adage such as "A picture is worth a thousand words", is very true in the sense that the picture can communicate the things which even sometimes words can't do effectively. Few decades back, in the era of film cameras, images were used extensively in the print media and it was very much difficult to manipulate the images due to the photography and darkroom developing expertise needed at that time. No doubt the print media is and was a powerful medium to spread a word, but it always lack the power of reaching every individuals sitting in the corner of the worlds as nowadays mobile, websites and the televisions are doing it. Today almost every mobile phone is equipped with a camera and also an image editing software which makes anybody to take pictures and manipulate on a fly and spread it through the Whatsapp like messengers, or social media websites. Hence it is very important that the images that we receive on our mobiles phones, computers through messenger apps or Facebook like social media websites needs to be validated for its reality, integrity and authenticity.

On one hand we have extremely powerful tools and technologies in both generating and processing digital images, there is a severe lack of robust techniques and methodologies for validating the authenticity of these digital images. Due to this asymmetry, digital images appear to be the source of a new set of legal disputes and problems rather than being a solution. Furthermore, combined with the ease with which image processing tools can be obtained and used to modify images in indistinguishable ways, verifying the integrity of digital images proves to be a challenging task. This in turn undermines the credibility of digital images presented as news items, as evidence in a court of law, as part of a medical record or as financial documents since it may no longer be possible to distinguish whether an introduced image can be considered as the original, or a (maliciously) modified version [1].

The tamper detection algorithms pertaining to the digital image forensics are classified as active tamper detection approaches and passive detection approaches. Passive tamper detection approach do not require the knowledge of any prior information about the content [2]. Passive image manipulation detection techniques broadly fall into five categories [3] : 1) pixel-based techniques that detect statistical anomalies introduced at the pixel level; 2) format-based techniques that leverage the statistical correlations introduced by a specific lossy compression scheme; 3) camera-based techniques that exploit artifacts introduced 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 make measurements of objects in the world and their positions relative to the camera. Usually, these forgeries do not leave any visual perceptive clues even though the underlying statistics of an image alter, as a result of which, it becomes difficult to distinguish such images from authenticated ones.

A very common type of forgery is region duplication forgery or copy-move forgery, in which a part of an image itself is copied and pasted into another part of the same image. This is usually done with the intention of disguising some contextual details in an image. These when skilfully done will leave behind no clues of tampering. Hence, need arises to look for effective tools to detect such region duplication forgeries in images.

The tempered image with copy-move forgery contains at least a couple of regions whose contents are identical. Copy-move forgery may be performed by a forger aiming either to cover the truth or to enhance the visual effect of the image. Normal people might neglect this malicious operation when the forger deliberately hides the tampering trace. So we are in urgent need of an effective CMF detection (CMFD) method to automatically point out the clone regions in the image. And CMFD is becoming one of the most important and popular digital forensic techniques currently.

In the literature there are mainly two classes of CMFD algorithms. One is based on block-wise division, and the other on key point extraction. They both try to detect the Copy Move Forgery through describing the local patches of one image. The former first divides the image into overlapping blocks and then finds the CMF by looking for the similar blocks [3].

The paper is organized as follows. In Sec. 2, we present the common workflow shared by different CMFD algorithms in the literature. In Sec. 3, we describe the various block based algorithms and finally the conclusion in section 4.

## WORKFLOW OF COPY MOVE FORGERY DETECTION

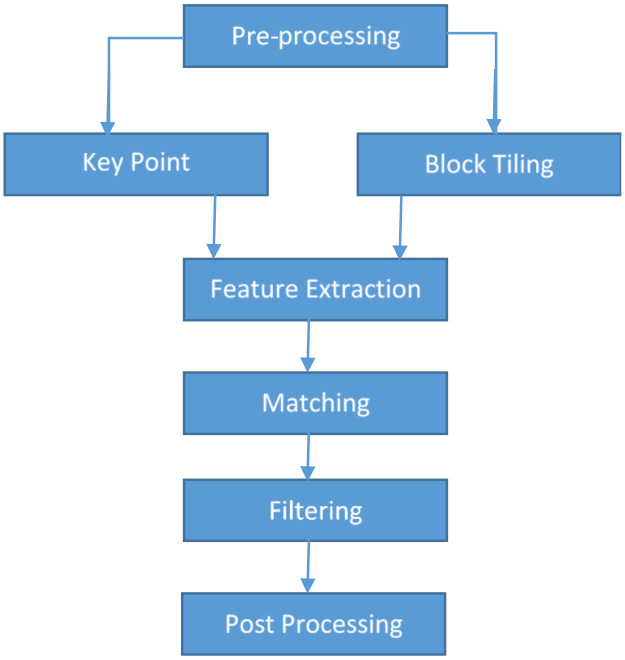

*Fig. 1. Common processing pipeline for the detection of copy-move forgeries*

In last one decade a large number of CMFD methods have been proposed, most of these techniques follow a common pipeline, as shown in Fig.1 Given an original image, there exist two processing alternatives [3].

CMFD methods can either keypoint based or block-based detection approach. In both cases, image can undergo pre-processing. For instance, most methods operate on grayscale images, and as such require that the colour channels be first merged. For feature extraction, block-based methods subdivide the image in rectangular regions. For every such region, a feature vector is computed. Similar feature vectors are subsequently matched. By contrast, keypoint-based methods compute their features only on image regions with high entropy, without any image subdivision. Similar features within an image are afterwards matched. A forgery shall be reported if regions of such matches cluster into larger areas. Both, keypoint- and block-based methods include further filtering for removing spurious matches. An optional post-processing step of the detected regions may also be performed, in order to group matches that jointly follow a transformation pattern [3].

## BLOCK BASED CMFD ALGORITHMS

### 3.1 PCA Based Algorithms

Popescu and Farid [7] proposed A PCA based efficient and robust technique that automatically detects duplicated regions in an image. PCA is used for dimensionality reduction of the image blocks. Duplicate regions are then detected by lexicographically sorting of all the image blocks. PCA results in reduction of the computational cost and the number of computations required are $O(N_t NlogN)$, where $N_t$ is the dimensionality of the truncated PCA representation and N the number of image pixels. Average detection accuracies obtained was 50% when JPEG quality = 95 with block size of 32 x 32 and 100% when JPEG quality = 95 with block size of 160 x 160. Though the algorithm is robust to minor variations in the image due to additive noise or lossy compression, but accuracy degrades for small block sizes and low JPEG qualities.

Mahidian and Saic [25] attempted to improve Popescu's algorithm by adopting blur moment invariants, PCA and kd-tree in their algorithm.

Zimba and Xingming [26] proposed two similar algorithms that were based on DWT and PCA. They aimed at improving the algorithm proposed by Popescu et al. [27] by reducing its computational complexity by first reducing the image size using DWT and, second, by adopting smaller feature vectors. The algorithm is similar to their work in [28], and the only difference is exploiting principal component analysis eigenvalue decomposition (PCA-EVD) as a feature vector. The algorithm could not resist high compression or high noise, especially when the duplicated regions were small.

Gharibi et al. [29] proposed using texture as a feature in their algorithm. For this purpose, the author used a Gabor filter to extract texture features from image blocks, and then they reduced the feature vector size using PCA. The algorithm is robust to JPEG compression but not to the other image processing operations. Moreover, it depends on several thresholds and initial values.

After creating forgery the forgerer often employ some type of post processing operations to evade the image forgery detection methods. The change of intensity of the copy moved part is such one of the post processing operation. The authors in [30] proposed PCA based approach which is very robust against the change of intensity of the copy moved part. Discrete cosine transform has been used to represent and, and principal component analysis is used to compress the feature vector of overlapping blocks of the image. Features, invariant to local change of intensity are created using down sampling of low frequency DCT coefficients.

The algorithms in this category also have small feature vector sizes and relatively low computation, but they do not show reasonable robustness against the different types of operations.

### 3.2 Discrete Cosine Transform (DCT) based algorithm

Authors in [5] had made first attempt in identifying tampered areas using block based DCT. They have used overlapping blocks and their DCT is then lexicographically sorted to reduce computational burden. They uses two approaches; exhaustive search and auto correlation. The computational complexity of the searching for matching blocks algorithm is $(MN)^2$ while the autocorrelation methods computational complexity is less than $(MN)^2$. The main characteristic of [5] is, though, successfully detect the forged part even when the copied area is enhanced/retouched to merge it with the background and when the forged image is saved in a lossy format; it does not work if the post processing of copy paste region is done.

The authors in [6] also uses block based approach and splits the image into overlapping blocks. It extracts a vector of seven features from each of the blocks for comparison. The first three features are the respective averages of red, blue and green colour components. The other four features are obtained after transforming the image to the YCbCr space – as the Y-component – on the basis of horizontal, vertical and the two diagonal directions. An array consisting of the vector of each block is then lexicographically sorted to carry out the matching .Compared with [7] and [5], this algorithm has lower computational complexity and is more robust against various post region duplication image processing operations.

Zhouchen Lin [8] uses a unique approach for tamper detection using DCT. The author uses DCT coefficients to examine the double quantization effect hidden among them. The method automatically detect tampered regions with additional advantages such as insensitivity to different types of operations such as simple image cut paste, alpha matting and inpainting. The method is capable of fine grained detection at the scale of 8 x 8 DCT blocks and computationally efficient.

Saiqa Khan and Kulkarni [9] uses DCT and the proposed optimized algorithm has a less time complexity than the wavelet and lop polar based algorithm proposed in [10]. Firstly the image is compressed and then it is being divided into overlapping blocks. Blocks are then sorted and duplicated blocks are identified using Phase Correlation as similarity criterion. Due to DWT usage, detection is first carried out on lowest level image representation. This approach drastically reduces the time needed for the detection process and increases accuracy of detection process. The algorithm works effectively even if the noise is added to the image and also at different compression levels of JPEG.

Wang et al. [11] made use of the combination of DWT and DCT. They have first applied DWT and DCT on image blocks separately, then, the resulting coefficients were multiplied to form the eigenvectors. Finally, the similarity of two blocks is measured based on the mean and variance of the distances between the eigenvalues in their corresponding eigenvectors. The algorithm showed good robustness to JPEG compression and additive noise but not to the other types of image processing operations.

Hu. et. al. [12] in their algorithm utilizes grouped DCT coefficients as feature vectors. The unique feature of the algorithm is the criteria used for similarity measure. In the proposed algorithm, the distance between every pair of vectors is sorted instead of the vectors themselves, to reduce the false positive ratio. If the distance between two blocks is less than a threshold, then the blocks are considered to be similar. The algorithm is very simple and robust to noise but not to the other image processing operations.

Cao et al. [13, 14] aimed at reducing the size of the feature vector and adding robustness against post-processing operations. The algorithm, exploits the mean of the DCT coefficients. The image is first converted to grayscale and is then divided into N overlapping blocks. For each block ***b***, DCT is applied, and a circle block is used to represent the coefficients. The circle block is divided into four parts. The feature vector V is obtained by calculating the mean of the coefficient values within each part. Then, all of the feature vectors extracted are lexicographically sorted. The Euclidean distance between each pair of consecutive vectors is calculated. The two blocks are considered to be similar if the corresponding Euclidian distance is less than a chosen predefined threshold. The proposed algorithm not only reduces the features vectors but also shows good endurance to multiple copy move forgeries. The algorithm is robust against blurring and additive noise operation but not to rotation and scaling.

Huang [15] extended and enhanced the work done by [5] in terms of the speed of the processing. Proposed algorithm divides the image overlapping blocks of size B×B. The DCT is applied on each block. The $B^2$ coefficients are quantized by q and then rounded to the nearest integer. The resulting block of coefficients is reshaped with a zigzag scan to a row vector, and then, the vector is truncated to only $P \times B^2$ elements. The algorithm is simple and straightforward, and it has the ability to detect duplicated regions with very good accuracy and sensitivity in spite of the post-processing operations. The authors did not discuss the robustness of their algorithm against geometric transformations.

Lynch [16] proposed an efficient expanding block algorithm primarily using direct block comparison instead of indirect comparisons based on block features.

Sunil Kumar et al. [17] suggested a method by applying PCA on DCT. Discrete cosine transform and principal component analysis have been used to represent and compress the feature vector of overlapping blocks respectively. Features invariant to local change of intensity are created using down sampling of low frequency DCT coefficients. The proposed algorithm is robust against both noise and JPEG compression. It also achieves invariance to illumination, but fails to detect contrast variations. The same authors in [18] uses a novel method for detecting copy move forgery in the contrast changes using binary discrete cosine transform vectors. The image is divided into overlapping blocks and DCT coefficients are calculated for these blocks. And then using the signs of the DCT coefficients, the feature vectors are created from these blocks. The Coefficient of correlation is used to match resulting binary vectors.

The advantage of exploiting DCT as a feature descriptor is the simplicity and the relative reduction in the feature vector size. Usually algorithms in this category show robustness to post processing operations, especially additive noise and JPEG compression, but they cannot resist the geometric operations.

### 3.3 SVD Based Algorithms

Li et al. [31], used singular value decomposition (SVD) for feature vector dimensionality reduction and wavelet transform for duplicated regions detection. Duplicated regions were localized by lexicographically sorting and neighbourhood detecting for all blocks even when the image was highly compressed or edge processed.

The authors in [32] identified the location of copy-move image tampering by applying SVD which served to produce algebraic and geometric invariant feature vectors. The proposed method has lower computational complexity, robust against retouching details and noise.

Ting and Rang-Ding [33] combined SVD with kd-tree in their algorithm. The method is implemented by first extracting SV features, which are invariant to algebraic, geometric changes, and some disturbances. Due to similar texture characteristic between copied and pasted regions, each SV feature vector is represented as a query and is then matched to its nearest neighbours in image. The proposed method is more robust to post image processing, such as scaling, rotation, noise contamination, Gaussian blurring, lossy JPEG compression.

In [34], the authors propose a two-level block matching technique wherein the first-level treatment divides the 8 × 8 fixed-sized overlapping blocks at lower resolutions and apply SVD to reduce the dimensions of the blocks. The resultant blocks are then sorted lexicographically using less cumulative offsets to facilitate block matching. The second level further matches the same blocks with the surrounding overlapping blocks.

In [35], the authors developed an Novel and effective detection algorithm based on SVD and Projection Data whose framework is based on expanding block. SVD is performed on the each block of the image. Choose the dominant features from each block blocks and sort them based on their dominance. The method of expanding block is used for future comparing and matching. The proposed method has stronger robustness to common post-processing attacks such as Gaussian blurring, additive white Gaussian noise, JPEG compression and their mixed operations.

### 3.4 Log-Polar Transform Based algorithms

Myna et al. [10] developed a method for detecting and localizing copy-move forgery using a log-polar coordinates and wavelet transforms. Wavelet transform is used on the input image for dimensionality reduction and then exhaustive search is carried out to identify the similar blocks in the image by mapping them to log-polar coordinates and using phase correlation as the similarity criterion.

Bayram et al. [19] uses the Fourier-Mellin Transform (FMT), which involves a log-polar mapping, to represent image blocks. Bloom-filters are used for block matching to reduce the computational complexity of the overall algorithm. The author exploited FMT as another invariant transform with respect to scale and rotation to allow a better performance of the algorithm when addressing copied regions that are slightly resized and rotated.

Qiumin et al. [20] employed log-polar fast Fourier transform (LPFFT). LPFFT is based on a nearly log-polar system where conversion to log-polar coordinates only involves 1-D Fourier transform and interpolation operations. It is also rotation and scale invariant and with lower computational complexity of $O(n^2 \log n)$ where n is block size.

Sergio and Asoke [21] focuses on automated detection and localization of duplicated regions affected by reflection, rotation and scaling in images. To perform an efficient search, overlapping blocks of pixels are mapped to 1-D descriptors derived from log-polar map.

Li and Yu [22] extended the work performed by Bayram et al. [19], which is based on FMT. As Bayram's algorithm is not rotation invariant, the authors aimed at enhancing it to allow it to handle duplicated regions of any rotation angle. The image is first divided into overlapping blocks, and the Fourier transform is applied to image blocks. The resulting magnitude values are resampled into log-polar coordinates and are then quantized to form feature vector f. The duplicated blocks are detected by means of generating hash feature vectors h using a simple hash algorithm, where the hash values are used to compare the corresponding blocks. The experimental results showed that the algorithm can detect arbitrarily rotated (up to 90º), slightly scaled, JPEG-compressed copy-move forgery. However, the algorithm is not robust against high levels of scaling, noise, or blurring.

Wu et al. [23] proposed their algorithm using a log-polar Fourier transform (LPFT). Unlike Bayram's algorithm [19], in which a log-polar mapping is performed in the Fourier domain; Wu's algorithm performs a log-polar transform (LPT) on every circular region in the image domain and then takes the 2D Fourier transform of the LPT results. In this algorithm, the image is first converted into a grayscale and is divided into overlapping blocks. The LPT of the inscribed circle of each block is then computed. The Fourier transform of the LPT is computed, and the *K* results of the LPFT, which are denoted as a set of *V* vectors, are considered for the matching step. The matching step is performed by calculating the maximum of the normalized cross-spectrum G between each pair of *V* values. The results showed that the algorithm has robustness against scaling and rotation. However, the algorithm is not robust against post-processing operations.

Recently, Wu et al. [24] improved their LPFT-based algorithm to a Log-Polar Fractional-Fourier Transform (LPFFT)-based algorithm. The fractional-Fourier transform is a generalization of a Discrete Fourier transform with less computation complexity and is based on a pseudo-polar grid.

### 3.5 Texture and Intensity Based Algorithms

Langille and Gong [36] has performed the early work in this category. Authors proposed a method segmenting an input image into blocks and search for blocks with similar intensity pattern using matching technique. The authors has used a k-dimentionsl tree to address the computational complexity.

Ardizzone et al. [37] proposed detecting copy-move regions by analysing a bit-plane representation of an image. In their algorithm, the n-bit grayscale image is first split into n different planes. Starting from a selected plane and proceeding toward the most significant planes, each plane is divided into m  m blocks. Each block is reshaped into an array of m2 bits. This array is zero padded, to make its size a multiple of 8. Bits from the array are converted into characters using ASCII code and are then used for the matching step.

Luo et al. [38] proposed a copy–move forgery-detection method that uses overlapping blocks of the image and then compare the block similarity using seven intensity-based characteristic features. Though it uses lexicographic sorting yet the algorithm has a less computational complexity as compared to [5] and [7].

Lin et al. [39] used average intensities of blocks along with a radix sort that aimed at reducing the time of the computation.

## CONCLUSION

In most of the block based copy-move forgery detection technique the pre-processing is done on the images. In most of the algorithms this pre-processing is converting the colour image into the grayscale by merging the colour channels. It is noted that in most of the block based CMFD methods the forgery detection is precise and accurate but the computational complexity is very much high.

## REFERENCES

[1] Xiao-qiang Zhou; Hai-yan Zeng and Man-jia Hu, "A Mathematical Approach to Detect Tampered Images," in Journal of Mathematics and Informatics Vol. 1, 2013-14, pp. 94-99, 2014.

[2] Anil Dada Warbhe et al, "An Active Approach based on Independent Component Analysis for Digital Image Forensics", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 2201-2203.

[3] H. Farid, "A Survey of Image Forgery Detection," Signal Processing Magazine, vol. 26, no. 2, pp. 16–25, Mar. 2009.

[4] Christlein, V.; Riess, C.; Jordan, J.; Riess, C.; Angelopoulou, E., "An Evaluation of Popular Copy-Move Forgery Detection Approaches," Information Forensics and Security, IEEE Transactions on, vol.7, no.6, pp.1841, 1854, Dec. 2012.

[5] Fridrich, A. Jessica, B. David Soukal, and A. Jan Lukáš. "Detection of copy-move forgery in digital images." in Proceedings of Digital Forensic Research Workshop. 2003.

[6] Luo, Weiqi, Jiwu Huang, and Guoping Qiu. "Robust detection of region-duplication forgery in digital image." Pattern Recognition, 2006. ICPR 2006. 18th International Conference on. Vol. 4. IEEE, 2006.

[7] Popescu A, Farid H. Exposing digital forgeries by detecting duplicated image regions. Technical Report TR2004-515. Department of Computer Science, Dartmouth College; 2004.

[8] Lin, Zhouchen, et al. "Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis." Pattern Recognition 42.11 (2009): 2492-2501.

[9] Khan, Saiqa, and Arun Kulkarni. "Robust method for detection of copy-move forgery in digital images." Signal and Image Processing (ICSIP), 2010 International Conference on. IEEE, 2010.

[10] Myrna, A. N., M. G. Venkateshmurthy, and C. G. Patil. "Detection of region duplication forgery in digital images using wavelets and log-polar mapping." Conference on Computational Intelligence and Multimedia Applications, 2007. International Conference on. Vol. 3. IEEE, 2007.

[11] X. Wang, X. Zhang, Z. Li, S. Wang, A DWT-DCT based passive forensics method for copy-move attacks, in: 2011 Third International Conference on Multimedia Information Networking and Security, 2011, 304–308.

[12] J. Hu, H. Zhang, Q. Gao, H. Huang, An improved lexicographical sort algorithm of copy-move forgery detection, in: Proceedings – 2nd International Conference on Networking and Distributed Computing, ICNDC 2011, (2011), pp. 23–27.

[13] Y. Cao, T. Gao, L. Fan, Q. Yang, A robust detection algorithm for region duplication in digital images, Int. J. Digit. Content Technol. Appl. 5 (6) (2011) 95–103.

[14] Y. Cao, T. Gao, L. Fan, Q. Yang, A robust detection algorithm for copy-move forgery in digital images, Forensic Sci. Int. (0) (2011).

[15] Y. Huang, W. Lu, W. Sun, D. Long, Improved DCT-based detection of copy-move forgery in images, Forensic Sci. Int. 3 (2011) 178–184.

[16] G. Lynch, F.Y. Shih, H.M. Liao, An efficient expanding block algorithm for image copy-move forgery detection, Inf. Sci. 239 (2013) 253–265.

[17] Sunil, Kumar, Desai Jagan, and Mukherjee Shaktidev. "DCT-PCA based method for copy-move forgery detection." ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol II. Springer International Publishing, 2014.

[18] Kumar, Sunil, J. V. Desai, and Shaktidev Mukherjee. "Copy Move Forgery Detection in Contrast Variant Environment using Binary DCT Vectors." International Journal of Image, Graphics and Signal Processing (IJIGSP) 7.6 (2015): 38.

[19] S. Bayram, H.T. Sencar, N. Memon, An efficient and robust method for detecting copy-move forgery, in: Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, 2009, pp. 1053–1056.

[20] Qiumin W, Shuozhong W, Xinpeng Z. Log-polar based scheme for revealing duplicated regions in digital images. IEEE Signal Process Lett 2011;18(10):559–62.

[21] Sergio B, Asoke N. Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics. Signal Process 2011;91:1759–70.

[22] W. Li, N. Yu, Rotation robust detection of copy-move forgery, in: Proceedings –International Conference on Image Processing, ICIP, 2010, pp. 2113–2116.

[23] Q. Wu, S. Wang, X. Zhang, Detection of image region-duplication with rotation and scaling tolerance, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 6421, 2010, pp. 100–108, LNAI.

[24] Q. Wu, S. Wang, X. Zhang, Log-polar based scheme for revealing duplicated regions in digital images, IEEE Signal Proc. Lett. 18 (10) (2011) 559–562.

[25] Mahdian B, Saic S. Detection of near-duplicated image regions. In: Computer recognition systems 2Advances in soft computing, vol. 45. 2007. p. 187–95.

[26] M. Zimba, S. Xingming, DWT-PCA (EVD) based copy-move image forgery detection, Int. J. Digital Content Technol. Appl. 5 (1) (2011) 251–258.

[27] A.C. Popescu, H. Farid, Exposing digital forgeries by detecting traces of resampling, IEEE Tran. Signal Proc. 53 (2) (2005) 3948–3959.

[28] M. Zimba, S. Xingming, Fast and robust image cloning detection using block characteristics of DWT coefficients, Int. J. Digital Content Technol. Appl. 5 (7) (2011) 359–367.

[29] F. Gharibi, J. Ravanjamjah, F. Akhlaghian, Z. Azami B., J. Alirezaie, Robust detection of copy-move forgery using texture features, in: 2011 19th Iranian Conference on Electrical Engineering, ICEE 2011, 2011.

[30] Sunil, Kumar, Desai Jagan, and Mukherjee Shaktidev. "DCT-PCA based method for copy-move forgery detection." ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol II. Springer International Publishing, 2014.

[31] Li G, Wu Q, Tu D, Sun S. A sorted neighbourhood approach for detecting duplicated regions in image forgeries based on DWT and SVD. In: Proc. International conference on multimedia & Expo 2007. p. 1750–3.

[32] Kang, XiaoBing, and ShengMin Wei. "Identifying tampered regions using singular value decomposition in digital image forensics." Computer Science and Software Engineering, 2008 International Conference on. Vol. 3. IEEE, 2008.

[33] Z. Ting, W. Rang-Ding, Copy-move forgery detection based on SVD in digital image, in: Proceedings of the 2009 2nd International Congress on Image and Signal Processing, CISP'09, 2009.

[34] Yang, Qing-Chu, and Chung-Lin Huang. "Copy-move forgery detection in digital image." Advances in Multimedia Information Processing-PCM 2009. Springer Berlin Heidelberg, 2009. 816-825.

[35] Liu, Feng, and Hao Feng. "A Novel Algorithm for Image Copy-move Forgery Detection and Localization based on SVD and Projection Data." International Journal of Multimedia & Ubiquitous Engineering 9.9 (2014).

[36] Langille, Aaron, and Minglun Gong. "An efficient match-based duplication detection algorithm." Computer and Robot Vision, 2006. The 3rd Canadian Conference on. IEEE, 2006.

[37] Ardizzone, Edoardo, and Giuseppe Mazzola. "Detection of duplicated regions in tampered digital images by bit-plane analysis." Image Analysis and Processing–ICIAP 2009. Springer Berlin Heidelberg, 2009. 893-901.

[38] W. Luo, J. Huang, G. Qiu, L. Weiqi, H. Jiwu, Q. Guoping, Robust detection of region duplication forgery in digital image, in: Proceedings of the 18th International Conference on Pattern Recognition, vol. 04, 2006, pp. 746–749.

[39] H.-J. Lin, C.-W. Wang, Y.-T. Kao, Fast copy-move forgery detection, WSEAS Trans. Sig. Proc. 5 (5) (2009) 188–197.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

## AUTHOR BIBLIOGRAPHY

| | |
|---|---|
| | **Anil Dada Warbhe**<br>Assistant Professor at MIET, Gondia, and Research Scholar, SGBAU, Amaravati, Maharashtra |
| | **Dr. Rajiv V. Dharaskar**<br>Former Director, Disha Education Society (DIMAT - Disha Technical Campus), Raipur, CG<br>Former Director, MPGI Group of Institutions Integrated Campus, Nanded<br>Former Professor and Head, PG Department of Computer Science and Engineering, G H Raisoni College of Engineering, a TEQIP II benefited Autonomous Institute, Nagpur. |
| | **Dr. Vilas M. Thakare**<br>Professor and Head in Computer Science, Faculty of Engineering & Technology, Post Graduate Department of Computer Science, SGB Amravati University, Amravati. |