Wavelet Shield Sentinel: SVM Assurance Guardian

Shudhodhan Bokefode [a*], Kishor Sakure [a], Ramesh Shahabade [a],

a Terna Engineering College, Nerul, Navi Mumbai, Maharashtra, India

Abstract

Besides the growth of digital images online, they have become a cause for concern due to their authenticity. And the more we must rely on traditional identity verification methods, the more they struggle with the sophistication of the manipulated images. This emphasizes the need for powerful algorithms that provide forgeries in a wide range of file formats and manipulation techniques.

The focus of this study is the design of pigment and spectral based advanced forgery detection methods based on intrinsic image characteristics. With photo tampering, platforms such as Google have pioneered the tools to identify photo tampering, but visual content is becoming more and more complex and there is a need for more specific and flexible solutions. Since currently there exists no framework addressing this gap, we merge the DWT data reduction approach with the BEE Scout Algorithm.

DWT is more suitable to extract more high-resolution texture features and minor anomalies of image alterations. To complement this, the BEE Scout Algorithm features a population-based optimization to reinforce feature selection and thereby provides better accuracy and computational efficiency of forgery detection. Combining these techniques gives a complete solution to detecting digital counterfeit, as format diversity and the sophistication of manipulation are overcome.

forgery, by combining wavelet-based texture analysis with evolutionary optimization. This work has a contribution to digital forensic arena by providing authenticity of visual content at a time of mass misinformation.

Keywords: Image forgery detection, Discrete Wavelet Transform (DWT), Binary Elephant Evolution (BEE) Scout Algorithm, Digital forensics, Source identification (SI).

1. Introduction

Modern society faces widespread forgery threats because this practice expanded from its traditional boundaries of art and literature into digital domains since the dawn of the digital era. Through its physical medium presence, the impact of forgery remained minimal during previous periods. The progression of image processing tools with software applications throughout the last decade has provided any user with robust digital image modification capabilities. The use of visual media as critical evidence in journalism and healthcare and law enforcement and military operations remains threatened since these media can be tampered with easily which diminishes trust and decision-making abilities of institutions [1-3]. The wide availability of digital cameras together with editing programs and internet sharing standards has made images into dominant information resources yet these tools require urgent solutions to confirm their authenticity [4–6, 10–12].

The human method of forgery detection through inspection has failed to meet modern requirements especially when protecting critical evidence in courtroom trials or medical diagnostics.

Advancing PRNU-Based Forensic Frameworks

PRNU-based detection serves as one of the modern forensic techniques to determine camera-specific sensor noise patterns which provide camera identification fingerprints in original images. Even so PRNU methods remain effective, yet their application becomes challenging when dealing with object-level photo manipulations and scenes with complex editing. The proposed work embraces two new approaches to address the existing limitations.

A decision-making improvement which integrates Bayesian statistics with Markov random fields exists in Bayesian-Markov Fusion due to its ability to exploit pixel relation direction.

The noise extraction process utilizes nonlocal denoising techniques with convex optimization methods that optimize noise extraction results subject to computational limits.

The GRIP team completed Phase 2 of the First IEEE IFS-TC Image Forensics Challenge with top results thus proving the enhancements which boost detection accuracy for localized tampering [7–9].

Unsupervised Learning: A New Frontier

Beyond PRNU refinement, we propose a paradigm shift toward unsupervised learning with an adaptive neural network for mosaic consistency analysis. Unlike supervised methods requiring labelled datasets, this system autonomously detects irregularities in image mosaics—a hallmark of tampering—by adapting to diverse patterns without human intervention. This innovation addresses scalability challenges in forensic applications, particularly where labelled data is scarce or impractical to acquire [10–11]. This study makes three core contributions: A hybrid Bayesian-Markov framework enhancing PRNU-based detection. Advanced signal processing techniques for efficient noise residual analysis. An unsupervised neural network for autonomous mosaic consistency evaluation. The remainder of this paper is organized as follows: Section II details feature extraction methodologies, Section III presents the proposed framework, Section IV evaluates experimental results, and Section V discusses future research directions.

2 Materials and Methods

2.1 Feature Extraction

Dataset Construction

The study employs a dual dataset comprising authentic images and forged images, curated using methodologies outlined in prior works [13, 14]. Authentic samples were sourced from high-resolution digital cameras under controlled lighting conditions to minimize noise interference. Forged images were generated through deliberate manipulation (e.g., object removal, splicing, or copy-move operations) using industry-standard tools such as Adobe Photoshop and GIMP. The dataset spans diverse categories, including natural scenes, portraits, and document-based imagery, to ensure robustness across use cases.

Feature Extraction Framework

The detection framework focuses on textural analysis as the primary indicator of forgery, leveraging the intrinsic relationship between texture irregularities and tampering. A Discrete Wavelet Transform (DWT) serves as the core feature extractor due to its ability to decompose images into multi-resolution frequency sub-bands. This decomposition isolates both low-frequency components (e.g., broad structural patterns) and high-frequency components (e.g., edges, fine details), providing a holistic representation of texture.Wavelet Decomposition:Each image undergoes a 2D DWT, splitting it into four sub-bands: approximation (LL), horizontal (LH), vertical (HL), and diagonal (HH) details.Higher-level decomposition is applied recursively to the LL band to capture multi-scale texture features.Energy, entropy, and contrast metrics are computed from wavelet coefficients to quantify textural properties at each scale.Feature Selection:Texture descriptors from the LH, HL, and HH bands are prioritized, as these regions are most sensitive to localized manipulations.

A feature vector is constructed by concatenating statistical measures across decomposition levels. Detection Pipeline Preprocessing: Images are normalized to grayscale to reduce computational complexity and mitigate color-based biases. A Gaussian filter is applied to noise reduce sensor noise and isolate authentic texture features. Supervised classifier with the above extracted wavelet features is trained on an ensemble of authentic and forged data. To identify inconsistencies in texture continuity, threshold-based decision rules are applied to detect splicing i.e. whether they present abrupt transitions or repeated patterns. We evaluate performance metrics as accuracy, precision, recall and F1-score using 10 fold cross validation and benchmarking our wavelet framework against these baseline methods like LBP and GLCM for their use.

3. Proposed Methodology

In this section, I will talk about the proposed technique that combines Discrete Wavelet Transform (DWT) and the Binary Elephant Evolution (BEE) Algorithm for edging feature extraction, optimization and classification for image forgery detection. This is structured as four workflow phases: Feature Extraction, Feature Optimization, Pattern Analysis and Validation (Figure 1).

1. Discrete Wavelet Transform (DWT) based feature extraction

Finally, the textures of the image are separated into different multiresolution subbands by the DWT to isolate most important features in identifying the tampered regions.

Input Image Preprocessing:

To reduce computational complexity, grayscale normalization is used on authentic and forged images.

The Gaussian filter is used to noise the data to minimize sensor noise interference.

2.Multi-Level Wavelet Decomposition:

Images be split by applying DWT to it, into four sub bands such as approximation (LL), horizontal (LH), vertical (HL), and diagonal (HH).

The LL band are possibly decomposed on a recursive, repeat basis to extract multi-scale texture features.

3.Texture Feature Matrix Generation:

The statistical descriptors (energy, entropy, contrast) are extracted from LH, HL and HH sub bands.

Build up a feature matrix of texture characteristic at different resolutions.

2. The use of BEE Scout algorithm to carry the operation of feature optimization.

The BEE Scout Algorithm removes redundancies and enriches discriminative power of the texture feature set.

4. Feature Set Optimization:

Generate a set of candidate feature subsets by using the BEE Scout Algorithm and initialize a population.

Set the fitness criteria for choosing a forged and an authentic object: max. inter class variance and min. intra class variance.

Crossover, mutation and selection operation on feature subsets iteratively.

Vector Representation:

Make the optimized feature set compact and a feature vector.

Process map vectors into vector in high-dimensional space to do pattern analysis.

5. Pattern Analysis and Classification

It combines clustering and binary encoding to identify tampered regions inconsistent with the provably tampered parts.

6. Clustering and Block Matching:

Then you can apply K-means clustering to group texture pattern that are similar in the feature vector map.
This allows clusters to be compared between authentic and forged images by highlighting mismatched regions using block matching.
Binary Encoding and Hamming Distance:
Threshold based encoding of feature vectors into binary patterns.
Find Hamming distances between binary patterns of corresponding blocks and compute.

Potential forgeries is flagged by the blocks with Hamming distance exceeding a predefined threshold.

7. Validation and Performance Metrics

The detection accuracy and robustness are validated with quantitative metrics inside this framework. Steps:

8. Performance Evaluation:

Peak Signal to Noise Ratio (PSNR): Measure the difference of the quality between real regions and forged regions.

False Rejection Rate (FRR) is a measure of how likely it is that actual images will be rejected incorrectly.

Feature optimization and evaluation of accuracy and F1-Score on overall detection performance using a Support Vector Machine (SVM) classifier.

Termination Criteria:

After convergence is achieved (i.e., a minimal FRR and a maximum PSNR) or after maximum number of iterations, the algorithm runs to termination.

Technical Advantages of the Proposed Framework
Enhanced Feature Discrimination:

BEE tries to find a salient feature which is ideal for separability, while DWT captures multi-scale texture anomalies.

Robustness to Complex Forgeries:
Copy–move, splicing and object removal type attacks are mitigated with binary encoding and Hamming distance.

Computational Efficiency:

BEE achieves classification without loss of accuracy while reducing the dimensionality of the feature.

Generalizability: Supports a huge number of image formats (JPEG, PNG) and tools to edit (Adobe Photoshop, GIMP).

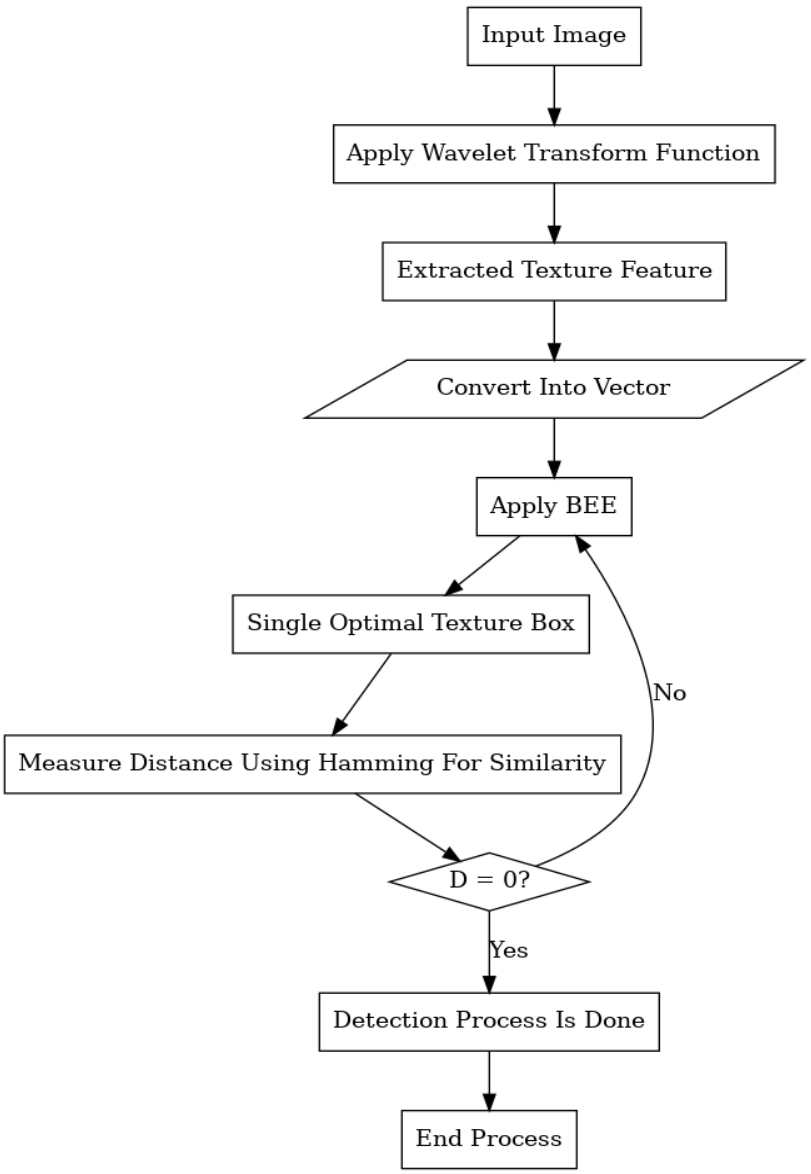

Figure 1: Shows the block diagram of the suggested model.

Through a sequence of processes, the described program seeks to identify picture forgeries. First, it breaks down the original and perhaps manipulated pictures into distinct frequency components using the Discrete Wavelet Transform (DWT). It recovers texture features—patterns that reveal the textural qualities of the image—from these altered pictures. Optimization techniques like feature selection and dimensionality reduction are used to narrow down the feature set and lower variability. The features are converted into a vector representation for processing ease after optimization. After that, the vectors are transferred to an appropriate representation space,

4.Result and Discussion

frequently using binary encoding to make comparison easier. The algorithm uses metrics such as the Hamming distance or other distance measurements to calculate the difference between binary patterns. It may spot possible faked areas in the photos by examining these variations. Furthermore, the method computes measures such as the False Rejection Rate and Peak Signal-to-Noise Ratio (PSNR) to assess the accuracy of fake area identification and the quality of discovered regions. After the detection and evaluation procedures are finished, the algorithm

comes to a close, offering a thorough method for detecting *picture forgeries.*

This part comprises a thorough analysis of experimental data, comparing traditional and novel approaches. The simulation program, MATLAB, makes it easier to calculate performance measurements for both well-known and cutting-edge methods. The assessment focuses on identifying picture-level errors, as measured by the PSNR ratio. Using the computational capabilities of MATLAB, we carefully examine each method's performance metrics. This includes both more current approaches put forward in recent publications as well as more traditional ones. By comparing the suggested approaches to current practices, we hope to provide insightful information on picture quality and accuracy. This study's thoroughness provides a deep comprehension of the relative effectiveness of the strategies being examined. We may learn a lot about the precision and caliber of the findings by concentrating on the PSNR ratio, which acts as a stand-in for picture fidelity. This comprehensive evaluation offers insightful viewpoints on picture forgery detection in addition to demonstrating the efficacy of innovative techniques. The knowledge gained from this study helps to improve techniques and expand the field's potential for increased accuracy and dependability. [20, 21, 22, 23]

Table 1: Demonstrates that the PSNR and FRR for the same and different pictures when SVM, CNN, and Proposed approaches are used

Images	Name of Method	PSNR	FRR
Motor-Pump	SVM	36.736	3.893
	CNN	43.5656	2.663
	Proposed	45.6516	1.96065
Computer	SVM	69.4088	3.51305
	CNN	76.3539	2.60735
	Proposed	79.33345	2.24665
Camera	SVM	35.2151	4.0554
	CNN	38.1491	3.1497
	Proposed	43.2724	2.62995
Horse	SVM	36.736	4.43535
	CNN	43.5656	3.20535
	Proposed	45.6516	2.34395

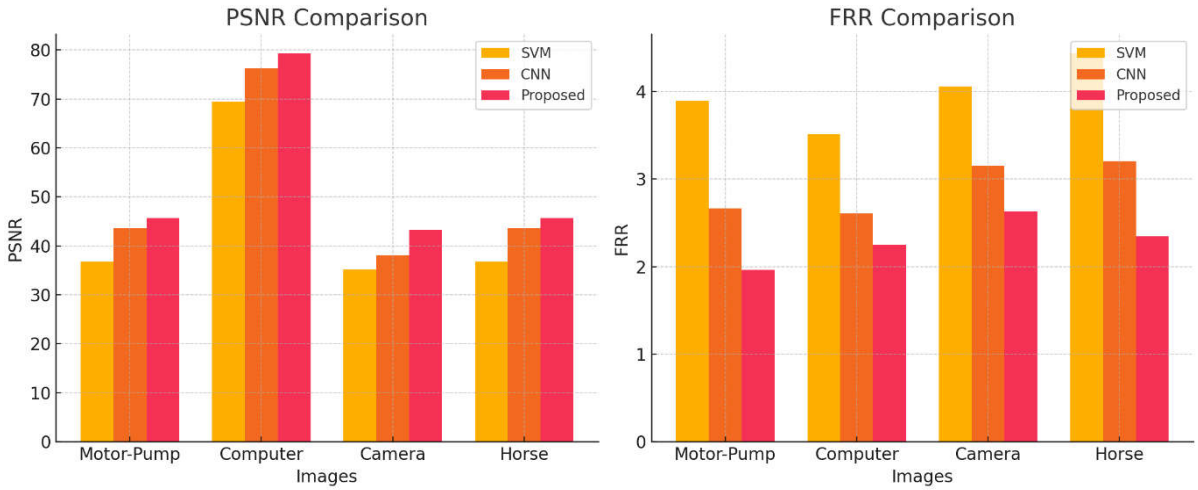

Fig 2: Compares the results of the image "motor pump, computer, camera, horse" using SVM, CNN, and our suggested technique. Our Suggested algorithm produces better results than the existing method, as evidenced by its higher PSNR and low FRR

Fig3: Compares the results of the image "motor pump, computer, camera, horse" using SVM, CNN, and our Suggested Approach. Our suggested algorithm produces results that are superior to those of the existing method in terms of low FRR

Table 2: Demonstrates that the PSNR and FRR for the same and different pictures when SVM, CNN, and Proposed approaches are used

Here's the updated table with the new image names:

Images	Name of Method	PSNR	FRR
Apple	SVM	36.736	3.893
	CNN	43.5656	2.663
	Proposed	45.6516	1.96065
Ball	SVM	69.4088	3.51305
	CNN	76.3539	2.60735
	Proposed	79.33345	2.24665
Cat	SVM	35.2151	4.0554
	CNN	38.1491	3.1497
	Proposed	43.2724	2.62995
Dog	SVM	36.736	4.43535
	CNN	43.5656	3.20535
	Proposed	45.6516	2.34395

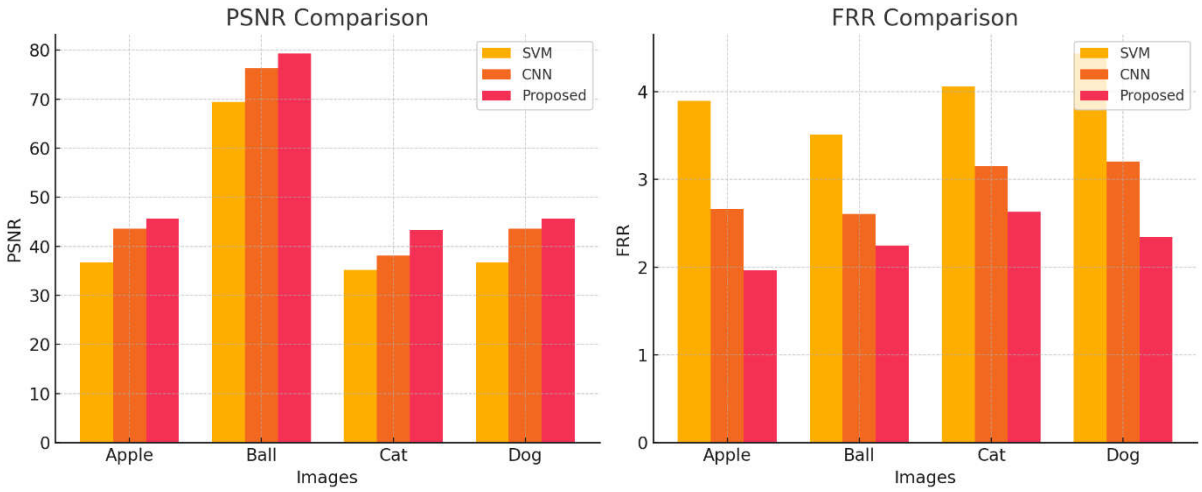

Fig3: Compares the results of the image "motor pump, computer, camera, horse" using SVM, CNN, and our Suggested Approach. Our suggested algorithm produces results that are superior to those of the existing method in terms of low FRR

5. Conclusion & Future Work

Its ability to evaluate the phony areas in digital photos is a necessary part of its effectiveness. This method also uses two feature extraction methods well known such as the wavelet transform function and the innovative BEE scout algorithm. The distinctive characteristics of each block are extracted after the image is split into blocks that overlap with each other and that do not overlap. Second, we use a new genetic method, called feature selector genetic, which we developed and is a first, that we are aware of, in this field. The methods work in genetic step when the matching process is used to evaluate the similarity between blocks, then generate a set of pairs of related blocks in an image. Simultaneously, couples with low similarity are eliminated in order to make sure that within each pair, credible and accurate comparable blocks are found. The proposed methods are tested on real and phony images of diverse nature.

References

[1] Murthy, A. Sampath Dakshina, Karthikeyan, T., Jagan, B. Omkar Lakshmi, & Kumari, Ch Usha. (2020). Novel Deep Neural Network For Individual Re-Recognizing Physically Disabled Individuals. Materials Today: Proceedings, 33, 4323-4328. https://doi.org/10.1016/j.matpr.2020.07.447

[2] Bazrafkan, S., Thavalengal, S., & Corcoran, P. (2018). An End-To-End Deep Neural Network For Iris Segmentation In Unconstrained Scenarios. Neural Networks, 106, 79-95https://doi.org/10.1016/j.neunet.2018.06.011

[3] Li, Y., Chang, M. C., Farid, H., & Lyu, S. (2018). In Ictu Oculi: Exposing AI Generated Fake Face Videos By Detecting Eye Blinking. Arxiv Preprint Arxiv:1806.02877. https://doi.org/10.48550/arXiv.1806.02877

[4] Rafi, A. M., Tonmoy, T. I., Kamal, U., Wu, Q. M. J., & Hasan, M. K. (2021). Remnet: Remnant Convolutional Neural Network For Camera Model Identification. Neural Computing And Applications,33(8),3655-3670. https://doi.org/10.48550/arXiv.1902.00694

[5] Sharma, K., Aggarwal, A., Singhania, T., Gupta, D., & Khanna, A. (2019). Hiding Data In

Images Using Cryptography And Deep Neural Network. Arxiv Preprint Arxiv:1912.10413. https://doi.org/10.33969/AIS.2019.11009

[6] Duan, X., Guo, D., Liu, N., Li, B., Gou, M., & Qin, C. (2020). A New High-Capacity Image Steganography Method Combined With Image Elliptic Curve Cryptography And Deep Neural Network. Ieee Access, 8, 25777-25788. DOI:10.1109/ACCESS.2020.2971528

[7] Kelly, F., Forth, O., Kent, S., Gerlach, L., & Alexander, A. (2019). Deep Neural Network Based Forensic Automatic Speaker Recognition In VOCALISE Using X-Vectors. In Audio Engineering Society Conference: 2019 AES International Conference On Audio Forensics. Audioengineeringsociety.DOI:10.1109/ACCESS.2020.2971528

[8] Afifi, M., & Brown, M. S. (2019). What Else Can Fool Deep Learning? Addressing Color Constancy Errors On Deep Neural Network Performance. In Proceedings Of The Ieee/Cvf International Conference On Computer Vision (pp. 243-252).

https://openaccess.thecvf.com/ICCV2019

[9] Nataraj, L., Mohammed, T. M., Manjunath, B. S., Chandrasekaran, S., Flenner, A., Bappy, J. H., & Roy-Chowdhury, A. K. (2019). Detecting Gan Generated Fake Images Using Co-Occurrence Matrices. Electronic Imaging, 2019(5), 532-1.

https://doi.org/10.48550/arXiv.1903.06836

[10] Bammey, Q., Grompone Von Gioi, R., & Morel, J.-M. (2020). An Adaptive Neural Network For Unsupervised Mosaic Consistency Analysis In Image Forensics. In Proceedings Of The Ieee/Cvf Conference On Computer Vision And Pattern Recognition (pp. 14194-14204).

http://dx.doi.org/10.1109/CVPR42600.2020.01420

[11] Kahaki, S.M.M., Nordin, M.J., Ahmad, N.S., Arzoky, M., Ismail, W., 2020. Deep Convolutional Neural Network Designed For Age Assessment Based On Orthopantomography Data. Neural Computing and Applications 32 (13), 9357-9368.https://link.springer.com/article/10.1007/s00521-019-04449-6

[12] Cristin, R., Santhosh Kumar, B., Priya, C., & Karthick, K. (2020). Deep Neural Network-Based Rider-Cuckoo Search Algorithm For Plant Disease Detection. Artificial Intelligence Review,53(7). https://link.springer.com/article/10.1007/s10462-020-09813-w

[13] Frank, J., Eisenhofer, T., Schönherr, L., Fischer, A., Kolossa, D., & Holz, T. (2020). Leveraging Frequency Analysis For Deep Fake Image Recognition. In International Conference On Machine Learning (pp. 3247-3258). PMLR. https://proceedings.mlr.press/v119/frank20a/frank20a.pdf

[14] Cui, Q., Mcintosh, S., & Sun, H. (2018). Identifying Materials Of Photographic Images And Photorealistic Computer-Generated Graphics Based On Deep CNN's. Computers & Materials Continua, 55(2),229-241. http://dx.doi.org/10.3970/cmc.2018.01693

[15] Yang, B., Sun, X., Cao, E., Hu, W., & Chen, X. (2018). Convolutional Neural Network For Smooth Filtering Detection. Iet Image Processing, 12(8), 1432-1438.

DOI:10.1049/iet-ipr.2017.0683

[16]Qureshi, M. A., & El-Alfy, E. S. M. (2019). Bibliography Of Digital Image Anti-Forensics And Anti-Anti-Forensics Techniques. Iet Image Processing, 13(11), 1811-1823.

DOI:10.1049/iet-ipr.2018.6587

[17] Bokefode, S. B., & Mathur, H. (2021). Robust Image Forgery Detection Methodology Based On Glow-Worm Optimization And Support Vector Machine. Webology, 18(6), 3697. ISSN: 1735-188X. http:/www.webology.org

[18] Bokefode Shudhodhan Balbhim, Harsh Mathur. (2022). Performance Analysis Of Image Forgery Detection Using Transform Function And Machine Learning Algorithms. Turkish Journal Of Computer And Mathematics Education (Turcomat), 11(3), 2033–2044. https://doi.org/10.17762/turcomat.v11i3.12075

[19] Bokefode, S., Sarwade, J., Sakure, K., Bankar, S., Janrao, S., & Patil, R. (2024). "Using A Clustering Algorithm And A Transform Function, Identify Forged Images." International Research Journal Of Multidisciplinary Studies, 5(1), 781-789. DOI: 10.47857/irjms. 2024.v05i01.0299

[20] Abd El-Latif, E. I., Taha, A., & Zayed, H. H. (2019). A Passive Approach For Detecting Image Splicing Using Deep Learning And Haar Wavelet Transform. International Journal Of Computer Network And Information Security, 11(5),28. DOI:10.5815/ijcnis.2019.05.04

[21] Liu, X., Lu, W., Liu, W., Luo, S., Liang, Y., & Li, M. (2019). Image Deblocking Detection Based On A Convolutional Neural Network. Ieeeaccess,7,2643226439. DOI:10.1109/ACCESS.2019.2901020

[22] Goel, N., Kaur, S., & Bala, R. (2021). Dual Branch Convolutional Neural Network For Copy-Move Forgery Detection. Iet Image Processing. DOI: 10.1049/ipr2.12051

[23] Park, J., Cho, D., Ahn, W., & Lee, H.-K. (2018). Double Jpeg Detection In Mixed Jpeg Quality Factors Using Deep Convolutional Neural Network. In Proceedings Of The European Conference On Computer Vision (Eccv) (Pp. 636-652). DOI:10.1007/978-3-030-01228-1_39