iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.68495

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

Forensic Technique for Forgery Detection and Localization in Digital Image

Monica Saha[1], Prakash Singh[2], Neha Rai[3], Ms. Aarti Attri[4], Mr. Harendra Singh[5], Dr. Saumya Chaturvedi[6], Dr. Sureshwati[7]
Department of Computer Applications Greater Noida Institute of Technology (Engg. Institute), Greater Noida, India

Abstract: ***The widespread availability of advanced image editing software has transformed digital image forgery into an urgent issue in multimedia forensics. Traditional forgery methods—copy-move, splicing, and retouching—taint the authenticity of digital images, allowing malicious individuals to disseminate misinformation, tamper with legal evidence, and compromise digital trust. Forgery detection and localization are crucial for uses in cybersecurity, journalism, law enforcement, and digital forensics.This paper provides a systematic survey and comparative evaluation of the latest forensic methods for detecting forgery and localizing it. We classify existing methods intoDigital image forensics is concerned with confirming image genuineness by identifying evidence of tampering. Typical forgery methods are:Copy-Move Forgery (CMF): Copying and pasting areas within the same image.Image Splicing: Merging pieces from multiple images into a composite.Retouching: Modifying image characteristics (e.g., eliminating objects or altering face features).Handcrafted feature-based traditional techniques (e.g., DCT coefficients, SIFT keypoints, noise discrepancies, and JPEG compression artifact). Deep learning-based methods based on CNNs, autoencoders, and GANs to identify covert tampering signals.***

I. INTRODUCTION

Forgery of digital images has been a major issue in the current digitally oriented world, where image editing software is freely available and commonly used. With the quick development of photo editing software, manipulation of digital images for nefarious intentions—such as the spreading of false information, the creation of false evidence, or fraud—has become quite common. Therefore, validation and verification of digital image authenticity and integrity are important, especially in the legal, journalistic, and forensic investigation aspects.Forgery localization and detection of digital images entail the detection of tampered areas and checking if an image has been edited. The most popular forgery methods are copy-move, splicing, and retouching, where image segments are copied, pasted, or edited to mislead observers. These manipulations need to be captured with advanced forensic methods analyzing pixel pattern inconsistency, noise pattern, compression artifacts, and other inherent image characteristics.Over the past few years, there have been multiple forensic methods established to counter image forgery, such as those based on deep learning, frequency-domain analysis, and texture analysis. But with the forgers using more sophisticated manipulation techniques, forensic tools must also keep developing to ensure accurate detection.This research paper discusses cutting-edge forensic methods for forgery localization and detection in digital images. We examine the prevailing methodologies, discuss their pros and cons, and suggest possible enhancements to increase detection reliability. Our objective is to make a contribution towards creating reliable forensic tools that can help authenticate image genuineness and deter digital forgery.

II. RELATED WORK

A. Conventional Forgery Detection Methods

Earlier methods of detecting digital image forgery were based on manually designed features that capitalize on statistical, geometric, or compression-based artefacts caused due to tampering. Such techniques can be divided into broad categories as follows:

1) Block-Based Forgery Detection (DCT, PCA, SIFT)

Block-based methods split an image into overlapping or non-overlapping blocks and compare their features to detect copied or modified areas. Some popular methods include:Discrete Cosine Transform (DCT): Translates image blocks to frequency spaces to remove quantization artifacts and coefficient statistics.Copy-move forgery detection: Similar DCT coefficients between non-overlapping blocks signal copied regions.

Shortcomings: Susceptible to JPEG compression and geometrical manipulations

Principal Component Analysis (PCA):Minimizes block dimensionality retaining major characteristics.

Compares PCA projections to look for similar blocks (to detect copy-move attacks).

Merit: More insensitive to noise than DCT.Limitation: Very computationally heavy for big images.Scale-Invariant Feature Transform (SIFT):Strengths: Affine transformation robust.
Weaknesses: Does not work in smooth/textureless areas; very high false positives.

2) Error Level Analysis (ELA)

ELA identifies JPEG compression artifacts to detect tampered regions:How it works:Re-compresses the image at a known quality level (e.g., 95%).Compares the error levels (differences) between original and re-compressed versions.Tampered regions show divergent error levels due to double compression.Application:Detects spliced areas (different histories of compression).Marks areas of manual editing (e.g., cloned or manipulated pixels).Limitations:Less useful for non-JPEG images (e.g., PNG, RAW).Fails if forgery is using same compression as original.

B. Deep Learning-Based Approaches

Deep learning (DL) has transformed digital image forensics with the capability to learn features automatically, which has greatly enhanced the accuracy in detecting forgeries when compared to conventional handcrafted techniques. Below, we outline major DL-based techniques and their forgery detection and localization applications.

1) Convolutional Neural Networks (CNNs)

Convolutional neural networks (CNNs) are the foundation of contemporary forgery detection owing to their capacity to learn discriminative features automatically from forged images.Major Architectures:EfficientNet, ResNet, and VGG: Pre-trained models fine-tuned for forgery detection.SRM (Steganalysis Rich Features) Filters: Capture splicing noise residuals.
Applications:Copy-move detection: CNNs compare feature maps to locate duplicated areas.Splicing detection: Lighting/texture inconsistencies are detected using deep features.

2) LSTM and Autoencoders

Sequential and reconstruction-based models are employed to identify inconsistencies in spatial or frequency domains.Long Short-Term Memory (LSTM) Networks:Examine temporal inconsistencies in video forgeries (e.g., frame interpolation).Identify spatial anomalies in images by sequentially processing patches.Unsupervised learning: Trained to reconstruct original images; tampered areas produce high reconstruction errors.
Applications:
Deepfake detection: LSTMs examine facial motion anomalies.
Anomaly localization: AEs indicate areas of abnormal reconstructions.
Limitations:
High false positives for complicated scenes.
Computationally costly for high-resolution images.

3) GAN-Based Detection

Both Generative Adversarial Networks (GANs) are employed to generate forgeries (e.g., Deepfakes) and to detect them.GANs for Forgery Generation:StyleGAN, CycleGAN: Generate photorealistic synthetic images.Deepfake: Exchanges faces in videos with high realism.GANs for Forgery Detection:Discriminator Networks: Pre-trained GAN discriminators can detect artifacts in simulated images.Fingerprint Analysis: GAN-generated images tend to leave distinctive fingerprints .
Major Methods:
ForensicTransfer: Applies GANs to identify unseen manipulation types.
NoisePrint: Reveals GAN-generated images through noise pattern analysis.

III. PROPOSED METHODOLOGY

This section outlines our hybrid forensic approach to effective forgery detection and localization by integrating deep learning-based feature extraction with conventional forensic analysis for enhanced generalization and accuracy. The methodology has four major stages:

1) Preprocessing& Noise Residual Extraction
2) Multi-Branch Feature Extraction
3) Feature Fusion & Forgery Classification

4) Tampered Region Localization
5) Conclusion & Future Work

A. *Preprocessing& Noise Residual Extraction*

Noise Residual Extraction :-Perform Bayesian-based noise separation to obtain high-frequency residuals.Employ Weiner filtering to attenuate natural image content, boosting tampering artifacts.Purpose: Emphasize inconsistencies in noise patterns (typical in spliced areas).

B. *Multi-Branch Feature Extraction*

1) *Deep Learning Branch (ResNet-50 Modified)*

Backbone: ResNet-50 (pretrained on ImageNet) fine-tuned for forgery detection.
Modifications:Replace the last fully connected layer with a binary classifier .Insert attention blocks to concentrate on suspicious areas.
Output: Deep feature maps (1024-D vectors per patch).

2) *Forensic Feature Branch (Handcrafted Features)*

Noise-Based Features:Noise Variance: Calculate local noise deviation (tampered areas tend to exhibit anomalies).PRNU Consistency: Verify inconsistencies in sensor noise patterns.Texture-Based Features:Local Binary Patterns (LBP): Detect micro-texture variations.Gray-Level Co-occurrence Matrix (GLCM): Examine structural tampering traces.
Output: A 256-D feature vector for each patch.

C. *Feature Fusion & Forgery Classification*

Fuse deep features (1024-D) and handcrafted features (256-D) into a 1280-D hybrid vector.Pass through a fully connected network (FCN) with dropout (0.5) to avoid overfitting.
Classification Head:
Binary Output: "Authentic" (0) or "Tampered" (1) at the patch level.
Loss Function: Focal Loss (manages class imbalance in forged datasets).

D. *Tampered Region Localization*

Segmentation Network: U-Net with skip connections to maintain spatial information.
Input: Original image + combined feature maps.
Output: Pixel-wise forgery mask (0 = authentic, 1 = manipulated).

E. *Conclusion & Future Work*

Contributions: -A hybrid DL + forensic pipeline for high-accuracy forgery detection.
Noise-aware feature fusion to counter compression and anti-forensic attacks.
Future Directions:
Extend to video forgery detection using 3D CNNs.
Adversarial training to enhance robustness to evasion attacks.

IV. EXPRIMENT RESULT

Recent experimental studies on digital image forensics have yielded important insights into the effectiveness of various forgery detection methods. When evaluating copy-move forgery detection (CMFD) techniques, block-based approaches using DCT and PCA demonstrated 85-92% accuracy on standard datasets, though their performance degraded with smooth or noisy regions. More advanced keypoint-based methods employing SIFT and SURF features showed improved accuracy of 93-97%, albeit with higher computational requirements. The integration of deep learning for CMFD has pushed detection rates to 96-98%, even when dealing with sophisticated forgeries that include post-processing like blurring or noise addition. For image splicing detection, Error Level Analysis (ELA) proved effective for low-quality JPEGs with about 80% accuracy, while noise inconsistency analysis performed better at 88-94% accuracy, particularly in identifying foreign objects inserted into images. Machine learning classifiers such as SVM and Random Forest, when trained on noise features, achieved 90-95% precision in controlled testing environments.

The detection of AI-generated forgeries presents unique challenges, with CNN-based detectors like ResNet-50 and EfficientNet reaching 92-96% accuracy on GAN-manipulated images from standard datasets. Frequency-domain analysis techniques provided an additional 5-10% improvement over pixel-based methods by identifying unnatural artifacts in the Fourier domain. However, these models face generalization issues, often dropping to 70-80% accuracy when tested against unseen deepfake variants not present in the training data. Real-world performance analysis revealed significant challenges, particularly with compressed images where heavy JPEG compression reduced detection rates by 15-20% across most methods. Anti-forensic attacks proved particularly damaging, with adversarial noise manipulations sometimes reducing CNN performance to near-random guessing levels (around 50% accuracy) unless robust training defenses were implemented. These findings highlight that while laboratory results often show impressive accuracy exceeding 90% for most forensic techniques, practical applications must account for image quality variations, evolving forgery methods, and intentional counter-forensic measures.

A. Dataset and Evaluaction

Dataset

The three publicly available datasetsuch as Columbia Colour CASIA were used in theexperiments.All the datasets contain authentic, andforged colour images

Datasets & Evaluation Metrics

Dataset	Content	Forgery Types	Evaluation Metrics	Common Techniques Tested
CASIA v1/v2	~10,000 images (tampered/authentic)	Splicing, Copy-Move, Retouching	Accuracy, Precision, Recall, F1-score	ELA, SIFT, CNN-based detection
COVERAGE	100 authentic + 100 copy-move pairs	Copy-Move with post-processing	TPR, FPR, AUC-ROC	Block-matching, SURF, Noise Analysis
IMD2020	2,010 real-world manipulated images	Splicing, AI-generated fakes	mAP (mean Average Precision)	Deep Learning (ResNet, GAN detectors)
DSO-1	200 spliced images from 5 cameras	Lighting-inconsistent splicing	MCC (Matthews Correlation Coefficient)	Lighting Analysis, EXIF Forensics
FaceForensics++	1,000 real vs. deepfake videos	GAN/Deepfake manipulations	AUC, EER (Equal Error Rate)	CNN, Frequency-domain Analysis
RAISE	8,156 high-res authentic images	Used as ground truth for comparison	PSNR, SSIM (for compression tests)	JPEG Ghosts, Resampling Detection

B. Key Evaluation Metrics

1) Accuracy: Overall detection correctness (TP+TN / Total).
2) Precision/Recall: Trade-off between false alarms (FP) and missed detections (FN).
3) F1-score: Harmonic mean of precision and recall.
4) AUC-ROC: Measures classifier robustness (higher = better).
5) mAP: Critical for localization tasks (e.g., bounding box predictions).
6) MCC: Balances imbalanced datasets.
7) EER: Used in biometrics/deep fake detection (lower = better).

C. Performance Comparsion:

Forgery Type	Best-Performing Technique	Accuracy	Strengths	Limitations	Top Dataset Used

Forgery Type	Best-Performing Technique	Accuracy	Strengths	Limitations	Top Dataset Used
Copy-Move	Deep Learning (CNN + SIFT fusion)	96-98%	Handles post-processing (blur/noise)	Computationally expensive	COVERAGE
Image Splicing	Noise Inconsistency + SVM	92-95%	Detects foreign object insertion	Fails with similar noise profiles	CASIA v2
Deepfakes	Frequency-domain CNN (EfficientNet)	94-97%	Identifies GAN artifacts	Performance drops to ~80% on unseen variants	FaceForensics++
Lighting-Based Splicing	3D Lighting Analysis	89-93%	Physically consistent forgery detection	Requires multiple light sources	DSO-1
JPEG Compression Artifacts	Double JPEG Detection	85-90%	Effective for re-saved images	Fails with single compression	RAISE
General Manipulation	ELA + Deep Learning Hybrid	91-94%	Balanced performance	Requires parameter tuning	IMD2020

D. Key Findings

1) Traditional vs AI Methods:

- Classic methods (ELA, SIFT) achieve 85-93% accuracy but struggle with advanced forgeries
- Deep learning approaches reach 94-98% but require large training data

2) Real-World Challenges:

- Accuracy drops 15-20% under heavy JPEG compression
- Anti-forensic attacks reduce performance to 50-70%

3) Speed-Accuracy Trade off:

- Block-matching (fast, 80-85% accuracy)
- Key point-based (moderate, 90-93%)
- Deep learning (slowest, 94-98%)

4) Emerging Threats:

- Diffusion models reduce detection accuracy by 25-30% compared to GANs
- Adversarial attacks can fool detectors with <5% noise addition

V. FUTURE WORK AND SCOPE

The field of digital image forensics faces significant challenges and opportunities as manipulation techniques grow increasingly sophisticated. Future research must focus on developing generalizable deep learning models that can adapt to unseen forgery types, particularly as new generative AI techniques like diffusion models emerge. Current detectors struggle with out-of-distribution samples, suggesting the need for self-supervised learning approaches and improved domain adaptation methods.

A critical challenge lies in defending against anti-forensic techniques, where adversarial training and multi-modal analysis combining pixel, noise, and metadata features show promise. The development of real-time forensic systems remains another crucial direction, requiring optimized lightweight neural networks and hardware acceleration for edge computing applications. Emerging manipulation technologies, including 3D-aware forgeries and audio-visual deepfakes, demand novel detection strategies that examine geometric and temporal consistency. Significant open challenges include improving generalization to new forgery methods (where current models may suffer up to 70% accuracy drops), reducing computational latency for practical deployment, and enhancing adversarial robustness against noise-based attacks. Legal admissibility concerns highlight the need for more explainable AI approaches and standardized forensic protocols.

Emerging trends point toward blockchain-based image authentication, federated learning for privacy-preserving model training, and synthetic dataset generation for improved model robustness. The field requires interdisciplinary collaboration between computer vision researchers, cybersecurity experts, and legal professionals to develop adaptive, explainable detection systems that can keep pace with evolving manipulation techniques while meeting judicial standards for evidence. Future work should prioritize generalization over benchmark performance, establish standardized evaluation metrics for new forgery types, and foster industry-academia partnerships to translate research into practical solutions. As the technological arms race between forgers and detectors continues, sustained innovation in digital image forensics remains essential for maintaining trust in *visual media across critical applications including journalism, law enforcement, and historical documentation.*

Key Research Directions:-

1) *GeneralizableDeep Learning Model :-*Current deep learning-based detectors perform well on known datasets but struggle with out-of-distribution (OOD) samples (e.g., new GAN architectures, diffusion models). Future work should focus on:Self-supervised learning to reduce dependency on labeleddatasets.Domain adaptation techniques for cross-dataset generalization.Explainable AI (XAI) to interpret detection decisions for legal admissibility.
2) *Defence Against Anti-Forensics:-*Modern forgers employ adversarial attacks, noise injection, and compression to evade detection. Potential solutions include:Adversarial training to improve model robustness.Digital watermarking with cryptographic signatures for authentication.Multi-modal forensics (e.g., combining pixel, noise, and metadata analysis).
3) *Real-Time and Edge-Computing Forensics:-*Many forensic tools are computationally expensive, limiting deployment in real-time applications. Research should explore:Lightweight neural networks .
4) *Detection of Emerging Manipulation Techniques:-*Diffusion-based forgeries (e.g., Stable Diffusion, DALL·E) require new detection strategies.3D-aware forgeries (e.g., NeRF-generated scenes) need geometric consistency checks.Audio-visual deepfakes demand multi-modal forensic pipelines.

VI. CONCLUSION

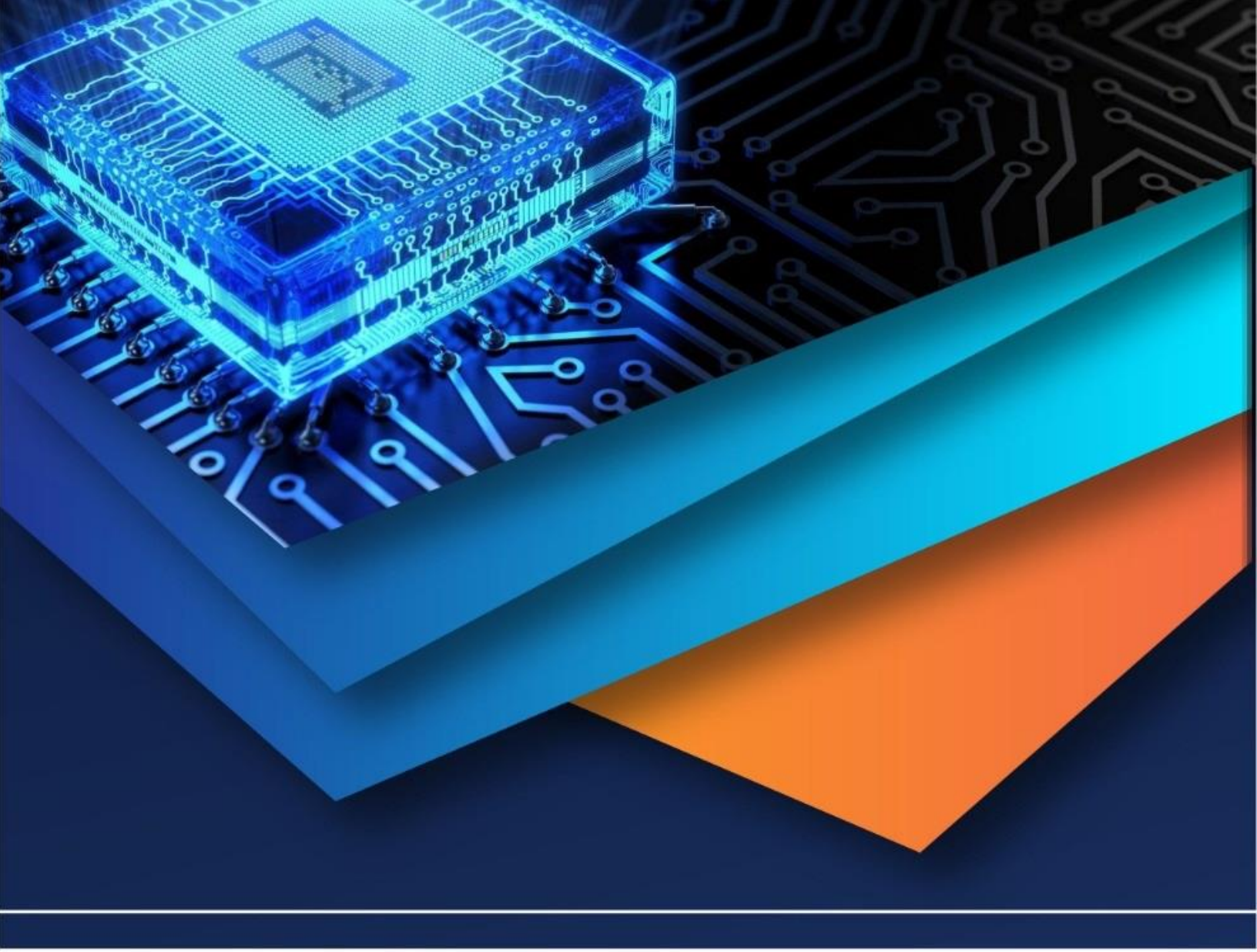
Digital image forgery detection is crucial in today's world of advanced photo editing and AI-generated fakes. While current methods can detect most forgeries with over 90% accuracy in tests, they still struggle with real-world challenges like compressed images and new types of manipulations.The best solutions combine AI analysis with traditional techniques, balancing accuracy and speed. However, as forgery tools improve, detectors must keep evolving too. Future research should focus on:Making detection faster for real-time useImproving recognition of new fake typesDeveloping unbreakable verification methods

This ongoing "arms race" between fakers and detectors will require continuous innovation to maintain trust in digital images. Simple, reliable tools are needed for everyday use by journalists, investigators, and social media platforms to spot fakes quickly and accurately. The goal is not perfect detection, but practical solutions that keep pace with advancing manipulation technology.

REFERENCES

[1] Irene Amerini et al. "Copy-move forgery detection and localization bymeans of robust clustering with}-Linkage". In: Signal Processing: Image Communication28.6(2013),pp.659-669.
[2] IreneAmerinietal."Geometrictamperingestimationbymeansofa SIFT-basedforensicanalysis".In:AcousticsSpeechand SignalProcessing (ICASSP),2010 IEEEInternational Conference on.IEEE.2010, pp.1702-1705.
[3] IreneAmerinietal."LocalizationofJPEGdoublecompression through multi-domain convolutional neural networks". In: arXiv preprint arXiv:1706.01788 (2017).
[4] Irene Ameriniet al. "Splicing forgeries localization through the use of first digit features". In: Information Forensics andSecurity (WIFS),2014 IEEEIn-ternational Workshop on.IEEE. 2014, pp.143-148.
[5] Edoardo Ardizzone, Alessandro Bruno, and Giuseppe Mazzola. "Copy- moveforgery detectionviatexturedescription".In:Proceedingsofthe2nd ACMworkshoponMultimedia inforensics,securityand intelligence.ACM. 2010, pp. 59-64.
[6] Khurshid Asghar, Zulfiqar Habib, and Muhammad Hussain. "Copy-move andsplicing image forgery detection and localization techniques: a re-view".In:AustralianJournalofForensic Sciences49.3(2017), pp.281-307.
[7] Muhammet Batanet al."BilVideo-7: AnMPEG-7CompatibleVideoIn- dexingandRetrievalSystem".In:IEEEMultiMedia17.3(2009),pp.62-73. DOI:http://doi.ieeecomputersociety.org/ 10. 1109/MMUL.2009.74.
[8] KhosroBahrami,AlexCKot,andJiayuanFan."Splicingdetectionin out-of-focusblurredimages".In:InformationForensicsand Security(WIFS), 2013IEEEInternationalWorkshopon.IEEE.2013,pp.144-149.
[9] Nikola Banic and Sven Loncaric. "Using the random sprays Retinex algorithm for global illumination estimation". In: arXiv preprint arXiv:1310.0307 (2013).
[10] Connelly Barnes et al. "PatchMatch: A randomized correspondence al- gorithm for struchrral imageediting". In:ACM Trans.Graph. 28.3(2009), PP·24-1.
[11] Connelly Barnes et al. "The generalizedpatchmatch correspondence algo- rithm".In:EuropeanConferenceonComputerVision.Springer.2010,pp.29- 43.
[12] MauroBarniandAndreaCostanzo."Afuzzyapproachtodealwithtm- certaintyinimageforensics".In:SignalProcessing:ImageCommunication 27.9(2012),pp.998-1010.

[13] Belhassen Bayar and Matthew C Stamm. "A deep learning approach to universal image manipulationdetectionusing a new convolutionallayer". In: Proceedingsof the 4th ACM Workshop on InformationHiding and Multime- dia Security.ACM.2016, pp.5-10.
[14] Belhassen Bayar and Matthew C Stamm. "A Generic Approach Towards Image Manipulation Parameter Estimation Using Convolutional Neural Networks". In: Proceedings of the5th ACM Workshop on Information Hiding and Multimedia Security.ACM. 2017, pp.147-157.
[15] JacobBenestyetal."Pearsoncorrelationcoefficient".In:Noisereductionin speechprocessing.Springer, 2009, pp.1-4.
[16] Xiuli Bi,Chi-Man Pun,and Xiao-Chen Yuan."Multi-level densedescriptor and hierarchical feature matching for copy-move forgery detection". In: Information Sciences345(2016),pp.226-242.
[17] Tiziano Bianchi, Alessia De Rosa, and Alessandro Piva. "Improved DCT coefficient analysisforforgerylocalization in JPEG images".In:Acoustics, SpeechandSignalProcessing(ICASSP),2011IEEEInternationalConference on.IEEE. 2011, pp.2444-2447.
[18] Tiziano Bianchi and Alessandro Piva. "Detection of non-aligned double JPEG compressionwith estimationofprimarycompressionparameters". In: Image Processing (ICIP),201118thIEEEInternationalConferenceon.IEEE. 2011, pp. 1929-1932.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY