



# Journal of Integrated SCIENCE & TECHNOLOGY

# Securing Visual Integrity: Machine learning approaches for forged image detection

Rohita Patil<sup>1</sup>, Vrushali Raut<sup>1</sup>, S. A. Shirsat<sup>1</sup>, Supriya Rajankar<sup>1</sup>, Anjali Yadav<sup>2</sup>, Somnath Wategaonkar<sup>3</sup>

<sup>1</sup>Electronics and Telecommunication Engineering, Sinhgad College of Engineering, Pune, India, <sup>2</sup>Sinhgad Institute of Technology and Science Narhe, Pune, India. <sup>3</sup>Bharati Vidyapeeth College of Engineering, Navi Mumbai, India.

Received on: 10-Dec-2023, Accepted and Published on: 26-Feb-2024

#### ABSTRACT

Image forgery detection is a critical area of digital forensics, attempting to discover manipulated regions within images to assure their authenticity and integrity. This study investigates the use of machine learning techniques,



particularly the Convolutional Neural Networks for image fraud detection. The suggested method involves training classifier to distinguish between original and counterfeit images using extracted features or patches. An image dataset is divided into training and testing sets in this study to facilitate CNN training on patches corresponding to original images. The accuracy of the trained model in identifying phony regions is then evaluated using an additional test set. To measure the effectiveness of the CNN-based forgery detection system, evaluation criteria such as accuracy, precision and recall are used. Proposed system achieves 99.15% accuracy with VGG16 network with tuned parameters.

Keywords: Image Forgery, Machine Learning, VGG16, Deep Learning

## **INTRODUCTION**

In the past ten years, the amount of image data collected has increased dramatically with introduction of common networking platforms like Facebook and Instagram. Internet firms such as Facebook are quite concerned about using image and video editing programs like Adobe Photoshop and GNU Gimp to make photo shopped photographs and films.<sup>1-4</sup> Image forgery has become more common in the digital age as individuals and organizations create fake photos for a range of purposes.<sup>5,6</sup> These fakes could be used for misinformation, deceit, or other malicious purposes. Therefore, it is becoming more and more important to have tools and techniques to recognize and prevent picture counterfeiting. Using machine learning is among the most innovative approaches.

Images like these are frequently exploited maliciously, like inciting mobs, and are major sources of fake news. We need to confirm the legitimacy of any suspicious photograph before taking any action.<sup>7</sup> To address this issue, IEEE Information Forensics and Security Technical Committee (IFS-TC) first introduced the First Image Forensics Challenge in 2013. It is a detection and

\*Corresponding Author: Rohita Patil, Sinhgad College of Engineering, Pune. India. Tel: +91-9923184950; Email: rohita.here@gmail.com

Cite as: J. Integr. Sci. Technol., 2024, 12(5), 815.

©Authors, ScienceIN https://pubs.thesciencein.org/jist

localization forensics challenge.<sup>21,22</sup> They made available an open dataset of digital photos that included both manipulated photos produced with algorithms like these and photo shot in various lighting conditions. The task was divided into two stages as i) to categorize images as authentic or unaltered and ii) to identify and pinpoint areas of image falsification.

Because it can extract high-level information from images, the deep convolutional neural network design known as the VGG16 network is especially helpful in the detection of image forgeries. It is useful for feature extraction, hierarchical representation, transfer learning, robustness to variations and its wide applicability.

Without explicit programming, computers can learn from data.<sup>9</sup> It can be applied to different image processing tasks, including the detection of phony images.<sup>3</sup> The objective is to train a ML model to identify patterns in real photos, which it can then use to identify fakes.

Few examples of image forgery i) Copy-move forgery: Cutting, pasting,<sup>4</sup> and reassembling pieces of a picture to create a new one is what copy-move forgery entails. ii) Splicing: Splicing is the method of combining several images to create new one and iii) Retouching: The process of altering the appearance of image is identified as retouching.<sup>1</sup>

Image forgery detection techniques include i) Digital Forensic: The investigation of digital images using forensic techniques.<sup>2</sup> To determine the validity of an image, metadata such as timestamps and camera information are analyzed, ii) Statistical Analysis:

1

Analyzing an image's statistical characteristics, such as its color distribution or noise pattern, to spot any irregularities that might point to manipulation, iii) Hashing and Watermarking: Digital watermarks or cryptographic hash functions are used to check an image's integrity and identify changes.

Machine learning can be used to detect the various types of evidence left by each of these forgery types. In the identification of images, machine learning outperforms more traditional forgery detection techniques.<sup>23,24</sup> Machine learning outperforms traditional approaches for detecting image forgeries in terms of consistency, speed, flexibility, accuracy, scalability, and automation.<sup>8</sup> These advantages make it a desirable method for detecting fake images in wide type of applications. Among the numerous advantages are: i) Using machine learning algorithms on massive datasets of photographs, it is possible to detect picture forgeries on a large scale. This is important for applications. Without requiring human assistance, these algorithms can be trained to automatically identify image forgeries.<sup>10,13</sup> This lowers possibility of human error while saving time and resources.

Machine learning approach use two different approaches like

i) Feature based approach: Using machine learning algorithms to classify images as authentic or manipulated by extracting features from images such as shape, texture or color descriptors.

ii) Deep Learning approach: CNNs and other convolutional neural networks are used to detect image forgeries. Deep learning architectures are also being used more and more. From picture data, these models can automatically identify intricate patterns and features.<sup>15</sup>

The main challenges in this work are Development in Editing Tools, Adversarial Attacks and Computational Complexity.

i) Developments in Editing Tools: The sophistication of image editing tools makes it harder to identify forgeries.

ii) Adversarial Attacks: Assailants may employ strategies to produce forgeries that deliberately avoid identification tools.

iii) Computational Complexity: Some techniques for detecting forgeries can be computationally demanding, which limits their applicability in real-time scenarios.

The deployment of image forgery is mainly required in

i) Media Forensics: Authenticating images in journalism, legal proceedings, and other situations where trustworthiness is critical.

ii) Security: Ensuring image integrity in security and surveillance systems.

iii) Content Verification: Preventing misinformation from spreading by validating the authenticity of images shared on social media and online platforms.

The main objectives of the research work is enhancing detection accuracy, defake recognition, real time detection capability, forensic analysis integration, user friendly solution.

## LITERATURE SURVEY

A. Review traditional and contemporary techniques for image forgery detection, emphasizing their strengths and limitations. An overview of both traditional and contemporary techniques for image forgery detection, highlighting their respective strengths and limitations as described in Table 1 and Table 2.

Traditional Techniques				
Techniques	Strengths	Limitations		
Metadata Analysis	Examination of metadata, including timestamps and camera information, can reveal inconsistencies that suggest manipulation <sup>16</sup>	Easily altered or stripped metadata, limited effectiveness against more advanced forgery techniques		
Error Level Analysis ELA	ELA highlights areas of an image with diverse compression levels, aiding in the detection of regions that may have been manipulated.	Sensitivity to image compression variations, less effective in detecting subtle forgeries.		
Source Camera Identifications	Matching an image to the specific characteristics of a camera can provide evidence of authenticity. <sup>17</sup>	Requiresadatabase of camerasignatures, limitedapplicabilitytoimagesfromunknownordiverse sources.		
Image Forensics with Filters	Applying filters to images can reveal hidden patterns or alterations.	Limited effectiveness against sophisticated forgery techniques, potential for false positives.		

**Table 2:** Contemporary Techniques used for Image Forgery

 Detection

Contemporary Techniques			
Techniques	Strengths	Limitations	
Digital Image	Utilizes machine	Requires extensive	
Forensics using	learning algorithms	labeled datasets for	
Machine	to analyze patterns	training, may	
Learning	and features	struggle with unseen	
	indicative of forgery,	or novel forgery	
	offering high	methods.	
	accuracy. <sup>18</sup>		
Deep Learning	Deep neural networks	Computationally	
Approaches	can automatically	intensive, may	
	learn complex	require substantial	
	features, effective	resources for	
	against deep-fake and	training, potential	
	advanced	vulnerability to	
	manipulations.14	adversarial attacks.	
Block-chain for	Utilizes block-chain	May not prevent	
Image	technology to create a	initial forgery but	
Authentication	tamper-proof record	provides a reliable	
	of an image history. <sup>19</sup>	record post-capture.	
Multi-Modal	Integrates	Complexity and	
Fusion	information from	resource-intensive,	
	multiple sources,	may pose challenges	

	such as metadata, pixel-level analysis, and deep learning, more robust detection.	for real-time processing.
GAN (Generative Adversarial Network Detection	Develops models specifically designed to detect the output of GANs used in creating deep-fake images. <sup>20</sup>	Constant evolution of GANs may require frequent updates to detection models.
Spatio-Temporal Analysis	Examines both spatial and temporal aspects of images or videos to detect inconsistencies or anomalies. <sup>16</sup>	Resource-intensive, especially for video analysis, and may face challenges in real-time applications.

### B. Common Challenges and Considerations

1. Adversarial Attacks: A lot of modern techniques are susceptible to adversarial attacks, in which malevolent parties manipulate images on purpose in order to trick the detection system. Ensemble approaches can increase resilience against adversarial attacks by combining several models to generate predictions. Ensemble approaches, which increase the uncertainty of the model and lessen its susceptibility to certain attack methodologies, can significantly reduce the impact of adversarial attacks by utilizing numerous models with varied architectures or training strategies.

2. Computational Complexity: In particular, deep learning techniques can be computationally costly, requiring strong hardware and a substantial amount of processing time. The numerous parameters of VGG16 may add to its high computational complexity. By eliminating low-contributing filters or superfluous parameters, model pruning strategies seek to shrink the model's size without materially compromising its functionality. Pruned models are more efficient since they require fewer calculations during inference. Using optimized libraries and frameworks to implement VGG16 can increase computing efficiency. Libraries such as TensorFlow, PyTorch, and Tensor Flow Lite provide deep learning model optimizations, such as VGG16, to take advantage of hardware acceleration and accelerate inference.

3. Generalization: Over-fitting is avoided by using regularization techniques like dropout, weight decay, and batch normalization, which place restrictions on the model's parameters during training. Regularization improves the model's performance on unobserved data by encouraging it to learn representations that are more straightforward and broadly applicable. Cross-validation is a method that divides the dataset into several subsets for training and validation in order to evaluate the model's generalization performance.<sup>15</sup>

4. Ethical Issues: The application of forgery detection techniques brings up issues with consent, privacy, and possible abuse. In order to reduce prejudice and guarantee equity for all demographic groups, image forgery detection systems should be carefully planned and assessed. To prevent prejudices that can

result in unjust treatment or discrimination, great attention should be made to the diversity and representativeness of the training data.

C. An overview of ML in the identification of forgeries that machine learning techniques have been used recently to overcome the difficulties associated with detecting image forgeries. Some of them are explored in Table 3.

In feature-based classification, classifiers in conventional machine learning techniques are trained using manually created features that are taken from images. These characteristics—texture descriptors, color histograms, statistical measurements—are used to discriminate between real and artificially altered regions in photographs. Using labeled datasets—which are collections of samples with known input-output pairs—algorithms are trained via supervised learning.

Within the framework of image forgery detection, these datasets comprise both real and altered images, labeled appropriately to reflect their actual characteristics. To acquire discriminative characteristics for identifying picture forgeries, a variety of machine learning methods are used, including Support Vector Machines (SVM), Random Forests, and Neural Networks. These algorithms use the attributes that are extracted from the photos to identify real and changed images by evaluating the labeled data.<sup>19</sup>

Deep Learning, particularly Convolutional Neural Networks (CNNs), is one of the most effective strategies for detecting forgeries. CNNs do well in this domain because of their innate capacity to learn hierarchical features from input data. CNNs are efficient at detecting elaborate manipulations, such as deep-fake content and minor image modifications.<sup>17</sup>

Tab	le 3:	Machine	Learning	Tec	hniques
-----	-------	---------	----------	-----	---------

Method and	Use	Advantages	Limitatio
Description			ns
Feature-Based	Texture, color	Easy to	Manual
Classification:	histograms, and	understand	feature
To train	statistical	straightforwar	engineerin
classifiers,	measurements	d and.	g is
handcrafted	are among the		necessary
features	characteristics		due to the
extracted from	that are		limited
images are	employed to		capacity to
frequently used	differentiate		capture
in traditional	real and		intricate
machine	artificial areas.		and subtle
learning			manipulati
methods. <sup>24</sup>			ons
Supervised learn	To learn discri	When given e	Reliance o
ing:	minative featur	nough trainin	n labeled
Algorithms for s	es for forgery d	g data, it can a	datasets an
upervised learni	etection, Suppo	ttain high acc	d potential
ng are trained on	rt Vector Mach	uracy.	difficulty
labeled datasets	ines (SVM), Ra		with new
that comprise re	ndom Forests,		or hidden
al and altered im	and Neural Net		manipulati
ages.	works are used.		ons are li
			mitations.
Deep Learning:	Because CNNs	Advantages in	Requires a
Convolutional N	are capable of a	clude high acc	large amo
eural Networks (	utomatically le	uracy, versatil	unt of labe

R. Pat	il et.	al.
--------	--------	-----

CNNs) are one o f the most popul ar deep learning techniques in the field of forgery detection. Generative Adv ersarial Network s (GANs): Gene rating realistic f orgeries is done with GANs, and specific models are created to id entify the output of GANs <sup>20</sup>	arning hierarch ical features, th ey are useful fo r identifying de epfake content and subtle mani pulations Deepfake conte nt detection is a ided by discrim inator networks , which are trai ned to recogniz e images produ ced by GANs.	ity in handlin g complicated and sizable d atasets, and re sistance to dif ferent kinds o f forgeries Specializing i n a particular kind of forger y, strong agai nst sophisticat ed manipulati on methods.	led data fo r training; computati onally de manding. As GANs develop, t hey requir e constant updates an d are vuln erable to h ostile attac ks
Transfer of Learning: Forgery detection tasks are optimized using models that pre-trained on huge datasets (like ImageNet).	Enables better performance on smaller, domain- specific forgery datasets by utilizing knowledge gathered from diverse datasets.	Prevents data scarcity problems and expedites training.	Potential bias from pre- training data; may not be ideal for all forgery detection tasks.
Group/Ensemble Technique: Merging predicti ons from several models often distinct kin d to improve perfo rmance as a who le. <sup>23</sup>	To increase rob ustness and gen eralization, bag ging or boostin g techniques ar e used. Strengths	Less over fitting and inc reased accura cy	Enhanced computati onal intric acy.
Interpretability a nd explain ability: Improved explai nability of mach ine learning mod els is being wor ked on so that us ers can compreh end the reasonin g behind a mode l's choice.	Model predicti ons are explain ed by methods such as LIME ( Local Interpret able Model- agnostic Expla nations).	Promotes und erstanding an d trust in mod el decisions.	Balance b etween int erpretabili ty and co mplexity.
Processing in re al time: Machine learning models and algorithms are optimized fo r real- time image forg ery detection use s. <sup>21</sup>	Facilitates the p rompt detection and handling o f manipulated c ontent in dyna mic online envi ronments.	Fast detection , appropriate f or real- time processin g application.	Accuracy and speed can be diff icult to bal ance.

# METHODOLOGY

Image forgery detection is an important task in digital image analysis and forensics. It entails recognizing any edits, manipulations, or tampering with an image in order to deceive viewers or manipulate the content.

Figure 1 shows that the complete process of image forgery detection process. The method begins with getting the digital image suspected of being forged or modified.



Figure 1. Block Diagram of Image Forgery Detection System

To improve image quality and standardize the format for analysis, preprocessing techniques such as noise reduction, resizing, color space conversion, and filtering is applied to the image prior to analysis. Feature extraction process is used for obtaining important information from an image that can signal probable fraud. Statistical traits, metadata, discrepancies, artifacts, and traces left by manipulation tools are all examples of features. Convolutional Neural Networks (CNNs) is used in which Deep neural networks that are trained to automatically learn discriminative features and patterns suggestive of forgeries. Following feature extraction and analysis, a classification stage is carried out in which machine learning or pattern recognition techniques are utilized to determine whether the image is legitimate or altered.

Deep CNNs have showed favorable results in a variety of tasks involving image processing, including the detection of forgeries. CNNs can automatically learn and extract complex information from photos, allowing them to discriminate between legitimate and altered content when it comes to detecting image forgeries.

#### A. Steps how deep CNNs can be used to detect forgery

1. Compile a dataset that includes both authentic and altered photos. It could include photos with copy-move forgeries, splicing, or other forms of alterations.

2. Ensured consistency and enough variance for training, prepared the dataset by scaling, standardizing, and augmenting the photos.

3. Created a CNN architecture suited for forgery detection often entails.

a. Convolutional Layers: These layers remove features in a hierarchical manner, identifying patterns at various levels of abstraction.

b. Layer Pooling: Layer pooling decreases the spatial dimensions of convolutional layers while keeping critical information.c. Fully Connected Layers: These layers integrate retrieved features to identify authentic or manipulated images.

4. Feature Learning: On the prepared dataset, the CNN is trained to learn discriminative features that distinguish between authentic and altered images.

5. Loss Function: For classification tasks, common loss functions like as cross-entropy are used.

6. Optimization methods (such as Adam and SGD) are used to minimize loss and update network parameters.

7. The model's performance is assessed using ROC curves, F1score, accuracy, precision, and recall as metrics.

8. The trained model is tested with previously unseen data to determine its ability to generalize. Use the model to detect forgeries and provide a tool for identifying modified photographs.

## **B. JPEG Compression**

JPEG compression is a popular technique for compressing digital photographs. While JPEG compression can dramatically reduce file size by leveraging human visual perception, it can also leave traces or artifacts that can be valuable in counterfeit detection or forensic investigation. When an image is modified and saved several times using JPEG compression, the re-encoding process introduces new artifacts. These artifacts may be distinct from those produced during the initial compression. Boundaries between the added and original sections of an image may exhibit various JPEG compression artifacts in some scenarios of image alteration, such as splicing or cloning. JPEG quantization tables, Discrete Cosine Transform (DCT) coefficients, and unique artifact patterns created by compression are frequently examined in forensic analysis. Artifacts that are inconsistent or abnormal may indicate manipulation.

Copy-paste forgeries, in which portions of a picture are copied and pasted, frequently produce distinct boundaries. Because of the disparities in quality between the pasted and original sections, these boundaries may have varying levels of JPEG compression artifacts. Multiple JPEG compression re-savings of an image might accentuate existing artifacts or generate new ones, highlighting anomalies in modified areas. JPEG quantization table analysis can identify differences or abnormalities between changed and unaltered areas of an image, indicating possible fabrication.

#### **EXPERIMENTAL RESULTS**

Image forgery detection entails detecting changes or manipulations done to digital images. To analyze the efficacy of picture forgery detection algorithms, several assessment measures are routinely utilized. These measures aid in determining the algorithms' accuracy, precision, recall, and overall efficacy. Among the important evaluation metrics are:

## **A. Evaluation Metrics**

**1. Accuracy:** Calculates the ratio of successfully detected forged and authentic regions to the total number of regions to determine the overall correctness of the detection method.

**2. Precision:** The precision of positive forecasts is measured. It is the proportion of accurately discovered forged regions to the total number of forged regions anticipated.

**3. Recall:** The algorithm's ability to correctly identify all faked regions is measured by recall. It is the proportion of accurately detected forged regions to total forged regions.

**B. Two-class Classification:** The algorithm is intended to categorize images into two groups: original and forgery. This binary classification scheme distinguishes between genuine and tampered with or fabricated images.

**C. Splitting the Dataset:** Two sets of images were taken from the collection: a test set and a training set. The 80:20 ratio indicates that 80% of the images were used to train the classifier, with the remaining 20% used to evaluate the classifier's performance.

**D.** Patch Creation: Patches are smaller picture parts derived from the original photographs. These patches are likely to contain specific characteristics or traits that are critical for determining whether a picture has been edited. Creating patches from original images allows the system to learn and detect these distinguishing properties throughout the training process. Table 4 presents a comparative analysis between the suggested and current techniques.

Sr. No.	Techniques	Accuracy	Recall	Precision
1	Markovian rake transform [11]	79.74%	-	-
2	DCT coefficients analysis [14]	90.91	-	-
3	Markov chain [12]	95.6		
4	Proposed + VGG16	94.6	92.4	97.0
5	Proposed + ResNet50	95.09	92.6	97.4
6	Proposed + ResNet50 with fine tuning	98.65	93.7	98.6
6	Proposed + VGG16 with fine tuning	99.15	95.3	98.7

**Table 4:** Technique-specific comparative analysis

**E. Key Findings:** Because of the deep design of VGG16, hierarchical features may be effectively extracted from images, capturing both high-level and low-level information. This feature enables the model to identify minute patterns and traits suggestive of image manipulations. VGG16 is a good choice for identifying counterfeit photos that may be rotated, resized, or subjected to other modifications because it has demonstrated resilience to a variety of image transformations and distortions.

## **CONCLUSION**

This paper describes the image forgery detection system using machine learning algorithm. The system takes input image from

database. This image is reshaped and difference is evaluated with original image. The deep convolutional neural network is utilized to process forgery detection. Proposed technique is compared with existing state of art methods. In proposed work ResNet50 and VGG16 networks are utilized with fine tuning parameters. The accuracy achieved is 99.15% with recall 95.3% and precision 98.7%.

## **FUTURE SCOPE**

Investigate multi-modal approaches that mix information from other sources, such as text, audio, or metadata, with visual material to improve forgery detection. Integrating VGG16-based models with different modalities may improve detection performance and provide additional information for detecting sophisticated forgeries.

## **CONFLICT OF INTEREST**

The authors declared no conflict of interest the for publication of thiswork.

### REFERENCES

- 1. Christian Riess and Tiago Jose de Carvalho, "Exposing Digital Image Forgeries by Illumination Color Classification." *IEEE Trans. OnInformation Forensics Secur.* 8.
- P.D. Reshma, C. Arunvinodh. Image forgery detection using SVM classifier. In ICIIECS 2015 - 2015 IEEE International Conference on Innovations in Information, Embedded and Communication Systems; 2015.
- 3. B. Xu, G. Liu, Y. Dai. Detecting image splicing using merged features in chroma space. *The Scientific World Journal*. 2014.
- Y. Cao, T. Gao, L. Fan, Q. Yang. A robust detection algorithm for copymove forgery in digital images. *Forensic Sci. Int.* **2012**, 214 (1–3), 33–43.
- A. Kuznetsov, V. Myasnikov. A copy-move detection algorithm using binary gradient contours. In *Lecture Notes in Computer Science (including* subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); 2016; Vol. 9730, pp 349–357.
- B. Bayar, M.C. Stamm. On the robustness of constrained convolutional neural networks to JPEG post-compression for image resampling detection. In ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings; 2017; pp 2152–2156.
- Y. Rao, J. Ni. A deep learning approach to detection of splicing and copymove forgeries in images. In 8th IEEE International Workshop on Information Forensics and Security, WIFS 2016; 2017; pp 1–6.
- I. Amerini, T. Uricchio, L. Ballan, R. Caldelli. Localization of JPEG Double Compression Through Multi-domain Convolutional Neural Networks. *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*. 2017, pp 1865–1871.
- K. Simonyan, A. Zisserman. Very deep convolutional networks for largescale image recognition. 3rd International Conference on Learning Representations, ICLR 2015 - Conference Track Proceedings. 2015.

- J. Dong, W. Wang, T. Tan. CASIA Image Tampering Detection Evaluation Database. In 2013 IEEE China Summit and International Conference on Signal and Information Processing; IEEE, 2013; pp 422–426.
- P. Sutthiwan, Y.Q. Shi, H. Zhao, T.T. Ng, W. Su. Markovian rake transform for digital image tampering detection. *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)* 2011, 6730 LNCS, 1–17.
- W. Wang, J. Dong, T. Tan. Effective image splicing detection based on image chroma. *Proceedings - International Conference on Image Processing, ICIP.* 2009, pp 1257–1260.
- W. Wang, J. Dong, T. Tan. Image tampering detection based on stationary distribution of Markov chain. *Proc. - Int. Conf. Image Process. ICIP* 2010, 2101–2104.
- Z. Lin, J. He, X. Tang, C.K. Tang. Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis. *Pattern Recognition*. 2009, pp 2492–2501.
- H. A. Alberry, A. A. Hegazy, G. I. Salama. A fast SIFT based method for copy move forgery detection. *Futur. Comput. Informatics J.* 2018, 3 (2), 159–165.
- K.R. Revi, M. Wilscy. Scale invariant feature transform based copy-move forgery detection techniques on electronic images - A survey. In *IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, ICPCSI 2017*; 2018; pp 2315–2318.
- N. Kanagavalli, L. Latha. A survey of copy-move image forgery detection techniques. In *Proceedings of the International Conference on Inventive Systems and Control, ICISC 2017*; 2017; pp 1–6.
- B. Xiao, Y. Wei, X. Bi, W. Li, J. Ma. Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering. *Inf. Sci. (Ny).* **2020**, 511, 172–191.
- M.J. Kwon, I.J. Yu, S.H. Nam, H.K. Lee. CAT-Net: Compression artifact tracing network for detection and localization of image splicing. In *Proceedings - 2021 IEEE Winter Conference on Applications of Computer Vision, WACV 2021*; Waikoloa, HI, USA, 2021; pp 375–384.
- 20. Y. Wu, W. Abdalmageed, P. Natarajan. Mantra-net: Manipulation tracing network for detection and localization of image forgeries with anomalous features. In *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*; Long Beach, CA, USA, 2019; Vol. 2019-June, pp 9535–9544.
- S.S. Ali, V.S. Baghel, I.I. Ganapathi, S. Prakash. Robust biometric authentication system with a secure user template. *Image Vis. Comput.* 2020, 104, 104004.
- I. Castillo Camacho, K. Wang. A comprehensive review of deep-learningbased methods for image forensics. J. Imaging 2021, 7 (4), 69.
- R.H. Jagdale, S.K. Shah. Modified Rider Optimization-Based v Channel Magnification for Enhanced Video Super Resolution. *Int. J. Image Graph.* 2021, 21 (1), 2150003.
- R.H. Jagdale, S.K. Shah. V Channel magnification enabled by hybrid optimization algorithm: Enhancement of video super resolution. *Gene Expr. Patterns* 2022, 45.