*International Research Journal of Innovations in Engineering and Technology (IRJIET)*
**ISSN (online): 2581-3048**
**Volume 9, Special Issue INSPIRE'25, pp 37-43, April-2025**
https://doi.org/10.47001/IRJIET/2025.INSPIRE06
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

# Detecting Image Manipulation with Reptile Search

**[1]B. Ramya, [2]Shaik Salam**

[1]PG Student, Department of CA, Mohan Babu University, Erstwhile Sree Vidyanikethan Engineering College (Autonomous), Tirupati, Andhra Pradesh, India. E-mail: ramyabojjolla123@gmail.com
[2]Assistant professor, Mohan Babu University, Erstwhile Sree Vidyanikethan Engineering College (Autonomous), Tirupati, Andhra Pradesh, India

***Abstract* - A popular kind of image manipulation is copy-move (CM) forgery, which entails copying and pasting a section of a picture to hide or duplicate material. An essential component of digital picture forensics is the detection of such frauds. Convolutional neural networks (CNNs), one type of deep learning technique, are used to extract informative characteristics from photographs. CNNs are well-suited for image-related tasks like forgery detection because of their reputation for being able to capture intricate patterns and structures. A reptile search algorithm using a deep transfer learning-based CM forgery detection (RSADTL-CMFD) technique is presented in this research. Neural Architectural Search Network (NASNet) feature extraction in forgery detection is used in the model that is being presented. This enables the network to efficiently extract discriminative and pertinent features from the input photos. To improve we use the reptile search algorithm (RSA) for hyperparameter tuning in order to optimize the NASNet model's performance. By optimizing the network's hyperparameters, this approach helps the model perform better and quickly adjust to various forgery detection tasks. Lastly, extreme gradient boosting (XGBoost) efficiently classifies areas of the image as authentic or manipulated/forged by using the features that were retrieved from the deep learning network. Benchmark datasets are used to test the RSADTL-CMFD model's experimental result analysis. A thorough comparison study demonstrated how the RSADTL-CMFD approach produced better results than more contemporary approaches.**

***Keywords:*** Cybersecurity, image forgery, copy move detection, machine learning, deep learning, parameter optimization.

## I. INTRODUCTION

With digital media cameras currently in vogue, the digital arena is bound to invade every sphere of life. The editing assistant of this publication is invariably called Tyson Brooks. He typed the manuscript and presented it for publication. Digital imaging packages like 3D Max and Photoshop have made manipulation and editing of digital images the easiest thing to do; even a five-year old can do it without leaving a trace whatsoever [1]. This indicates a serious social issue with the degree of trust that can be given to digital content authenticity, particularly when it serves as evidence during court proceedings, to claim an insurance policy, and in the scientific journal VOLUME 11, 2023.This book is published under the Creative Commons of RSA With DL Approach for CM image forgery detection community license. Most of their manuscripts confirmed by the journal entail unworthy and false operations in their graphs, with few statistical papers [2]. While trying their best to authenticate an image, various methods were devised to combat forgery and manipulations. [3]. In particular, the term fraud of a specific type known as copy-move forgery (CMF) imaging is used to denote the technique by which a portion of an image is duplicated and the duplicated part is then copied onto the original image [4, 5, 6, 7]. As a result, it became highly critical in the networked community when image forensics was linked with CMF detection. Active detection and passive detection are the two classes to which technologies applied in picture forensics have been categorized [8]. Firstly, to identify an image as authentic or not, the active detection method needs to have prior information that is obtained from the image namely watermarking. In contrast to active detection methods, passive detection methods do not require the collection of prior picture data. In identifying the tampering areas, passive detection methods could be aided by detective methods [9]. Nevertheless, much of image forgery detection method employs passive-related approaches to execute the different tampering recognition methods presented in this paper. This study presents educating people through the image-related figures such as Fig. 1, which lends credence to the application of AI in cybersecurity. Cybersecurity and artificial Intelligence. Considerable amount of work regarding digital image forensics is done towards developing efficient and robust detection algorithms for counteracting manipulations of this nature. Traditional methods generally rely on techniques such as key point-based methods or correlation-based matching, which can be limited in detection accuracy and processing complexity, particularly in the presence of changes such as noise addition, scaling, or rotation. An RSADTL-

 

*International Research Journal of Innovations in Engineering and Technology (IRJIET)*
**ISSN (online): 2581-3048**
**Volume 9, Special Issue INSPIRE'25, pp 37-43, April-2025**
https://doi.org/10.47001/IRJIET/2025.INSPIRE06
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

CMFD approach was created in this work to identify whether CM areas existed in the image.

To generate feature vectors, the RSADTL-CMFD model initially created a NASNet model. Subsequently, RSA is employed to alter the NASNet method's hyperparameters. At last, proper class labels are determined through the XGBoost classifying model. Benchmark datasets are utilized to measure the experimental result analysis of the RSADTL-CMFD method. A detailed study concluded that the RSADTL-CMFD method provided results better than more recent methods. Hence, the CM regions that are shown in real time can be detected by employing the RSADTLCMFD method. In the future, hybrid DL methods have enhanced the performance of the RSADTL-CMFD technique. Moreover, the method will be tested in real time. The development of a reptile search algorithm for copy-move image forgery detection by the project is a significant contribution to the digital image forensics field. The developed framework offers a robust, precise, and efficient means to detect copied regions in images by integrating this algorithm with deep learning methods and blockchain technology. The results demonstrate improved scalability, robustness to variations, and detection precision for real-world applications. Such a project provides a good platform for further developments in counterfeit image prevention and digital image authentication application. In this large area, acceptance and integrity of digital media content can always be insisted upon.


**Fig 1: Artificial intelligence in cybersecurity**

Typically, one of the major purposes of forgeries is to hide certain incriminating objects, such as the presence of weapons, by superimposing other objects or part of that image [10]. Digital images can easily be altered using the services of modern hypermedia tools. A professional fake can produce a fake image that cannot be seen using the human eye, and therefore it becomes impossible to distinguish between true and fake. Several methods were proposed to identify image forgeries, which utilize deep transfer learning-based CM forgery detection (RSADTLCMFD) model to develop a reptilian search approach. The RSADTLCMFD method determines the accessibility of the CM region in the image. To achieve that, the RSADTL-CMFD model first obtains feature vectors from a Neural Architectural Search Network (NASNet) model.

## II. LITERATURE SURVEY

[1] Zenan Shi, Xuanjing Shen, Hui Kang, and Yingda Lv introduced in 2018 a unique model that employed dual-domain convolutional neural networks to identify and localize altered areas in images. Their model included a spatial domain and frequency domain CNN, and a new image pre-processing layer designed to suppress image content, in order to better learn the kinds of features that indicate manipulation. Their system outperforms current state-of-the-art algorithms on detection of tampered areas, positively increasing detection accuracy and robustness. The complex design of the D-CNN architecture results in longer processing time and computational overhead, which will make the implementation of real-time applications more difficult in realworld settings.

[2] All methods proposed by Savita Walia, Krishan Kumar, Saurabh Agarwal, and Hyunsung Kim, in 2022, employ a combination of Deep Learning and Shapley Additive Explanations (SHAP) analyzes the transformed images via scale and direction invariant local binary patterns and error level analysis through a ResNet-50 paradigm. The method is highly accurate in detecting counterfeit images and adds to the results' interpretability. Such methods are still under the spell of deep learning and may still have burdens relating to huge computations and time demands that may impede their application in real-time.

[3] In 2019, Belhassen Bayar and Matthew C. Stamm presented MISLnet, a convolutional neural network that automatically learns low-level aspects of image modification using a restricted convolutional layer. MITLnet performs well, achieving great accuracy, up to 99.97%, in order to detect editing operations. However, the architecture's complexity is a plausible limiting factor on its performance considering the requirement of substantial training data and computational power.

[4] These authors in 2023 proposed an improved Reptile Search Algorithm, along with Salp Swarm Algorithm, for multi-level image segmentation using gray-scale thresholding. This new approach increases segmentation accuracy by efficiently avoiding local optima and simplifying the search, thus outperforming some other meta-heuristic optimization methods in benchmark tests. However, this complexity might mean that considerable time is taken, leading to an increase in the computational burden required for processing, possibly inordinate for larger datasets or more complex images. This being said, the proposed method undoubtedly represents an improvement to the algorithms assisting image segmentation in the area of medical image applications.

 

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 37-43, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE06
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

[5] RSA-SSA, apparently short for Reptile Search Algorithm- Salp Swarm Algorithm, provides new approaches to multi-level image segmentation. The Sebastian Reptile Search algorithm combines with salp swarm algorithm in important new ways. This method improves segmentation accuracy and also beats other metaheuristic algorithms in benchmark comparison studies by being able to avoid local optima efficient. However, where complications arise is that as it has a heavier computation demand, processing times better to act on it might be affected.

[6] Peng Zhou and co-workers have developed a two-stream Faster R-CNN network for image manipulation detection. It utilizes a noise stream to examine inconsistencies of the local noise features and an RGB stream to extract visual tampering artifacts. By utilizing the additional information, our dual-stream approach improves detection accuracy and yields state-of-the-art results on a variety of picture alteration datasets. Nevertheless, the complexity of the architecture may tend to warrant large numbers of process capacity, which in turn may limit its application in real-time situations or with smaller datasets.

[7] In a more concise form, it must not exceed the statement. 2023: authors Yu Yuan Zeng had submitted Proposal Contrastive Learning (PCL) that consisted of a two-stream architecture utilizing spatial relations of local features via a proxy proposal contrastive learning task and obtaining global features from RGB and noise views for effective image manipulation detection. The new approach reduces the expense of human labeling and promotes improved generalization from improved feature discriminative power owing to representation of features and learning from unlabeled data. Yet, the complexity of the two stream setup can result in larger processing demands, which may have a negative impact on the efficiency of real-time systems.

[8] In 2023, Xinru Chen along with his coworkers introduced MVSS-Net, a new network for image manipulation detection. It comprises multi-scale supervision and multi-view feature learning to enhance sensibility and specificity detection. MVSS-Net extracts semantic-agnostic features which allow it to generalize strongly over numerous datasets and significantly reduce false alarms on real images using noise distribution and boundary aberrations. This way, the model can be trained on both real and manipulated images, enhancing manipulated region detection accuracy.

[9] In 2023, Xinru Chen along with his coworkers introduced MVSS-Net, a new network for image manipulation detection. It comprises multi-scale supervision and multi-view feature learning to enhance sensibility and specificity detection. MVSS-Net extracts semantic-agnostic features which allow it to generalize strongly over numerous datasets and significantly reduce false alarms on real images using noise distribution and boundary aberrations. This way, the model can be trained on both real and manipulated images, enhancing manipulated region detection accuracy.

[10] The method suggested the Reptile Search Algorithm in 2024 by C. Hemavathy and others for efficient detection of copy-move forgery in images based on the hunting behavior of reptiles to scan the picture space for similar areas. The method combined SIFT descriptors, zigzag scanning, and 2D DCT coefficients to improve the accuracy of forgery detection. It integrates block-based technology with the Fourier-Mellin Transform to enhance the precision of digital image forensics for the detection of manipulated regions.

## III. METHODOLOGY

Preparing photographs for the required formats and normalizing them for effective feature extraction using Convolutional Neural Networks are the key processes of Reptile Search Algorithm (RSA), which has the ability to detect manipulated images. Typical patterns of manipulation detected by a CNN are inconsistent lighting, texture, etc. The RSA begins by initializing the candidate output populations that correspond to different CNN parameters.

The exploration phase is about testing the various techniques of high walking and belly walking in the environment of the search space. The search space is most reduced to the best solutions discovered by the algorithm in the exploitation phase. The improved CNN is evaluated against accuracy and precision on community data sets.

### 3.1 Recent Works

The finest procedure has undergone modifications in reptilian search, drawing its inspiration from hunting behaviors of reptiles, such as snakes. The method eyes the picture space in duplication zones in much the same manner that a snake hunts for its dinner. Recent focus in academia has been placed on various efforts to optimize and parallelize computation such that the algorithm could be enhanced in accuracy and efficiency. An additionally updated detection framework has been undertaken for the deep learning enhancements. In addition, CNNs as well as RNNs create trees learning discriminative features based on image-sliced image patches enabling a more effective detection of copied sections irrespective of various transformations and under varying illumination.

 

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 37-43, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE06
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

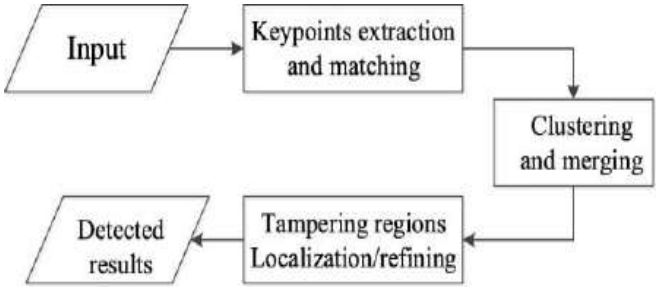


**Fig. 2: Flow Chart of Copy Move Image**

Pre-processing, enhancing quality and suppressing noise, follows image acquisition and serves for detecting copy-move image forgery. These images are then subjected to feature extraction and were tagged real/altered for the creation of training data. This training data is then fed into Random Forest, Decision Trees, and other machine learning models to create an efficient forgery detection system. Following this, models are tested using validation data. The Reptile Search Algorithm was applied to improve detection of copy-move forgeries and inhibition of false positives.

### 3.2 Proposed Work Explanation

The two-dimensional DCT coefficient is calculated and a feature vector created through zigzag scanning in each block. Lastly, the feature vector is ordered lexicographically. Then, Euclidean Distance was used to obtain the repeated block.

A hybrid mechanism was proposed by combining block-based technology with Fourier-Mellin Transform and a key point-based strategy with SIFT where, the input image was first analyzed for forged in split into smooth and textural parts. For the texture component of images, key points have been extracted by SIFT descriptors, whereas the smooth part of the images was subjected to Fourier Mellin transformation. Unlike active detection methods, the image forgery does not have any prior information about it and thus does not require passive detection methods. Passive detection strategies may utilize the advantages of detective strategies for determining the tampering regions.

Nevertheless, most image forgery detection methods utilize passive-related strategies in order to accomplish the forms of tampering detection which is debated in this article.

### Copy move detection

Copy-move forgery imaging was regarded as a particular type of forgery which involves creating a duplicate of a part of the image and duplicated part must be pasted to the same image. Thus, image forensics associated with CMF identification made it extremely important in the network-based society. The technologies used in image forensics were divided into two i.e. active detection and passive detection. To begin with, the active detection method requires prior information that are derivated from an image to determine the genuineness of an image, i.e., watermarking.

### Machine learning

The aim of this system is to detect CMF images and for forensic data retrieval. Provide a W-Net system-based method to detect and locate regions of video forged using the CMF technique. The proposed method was used for the identification of forged videos with high effectiveness. Introduce a new copy-move image forgery detection system that relies on a texture feature descriptor known as Local Tetra Pattern for block-level image comparative used for localized tampered areas.

### 3.3 Algorithm:

Convolutional neural networks and other deep learning methods are employed to extract informative features from images. CNNs are particularly suitable for image-related applications such as forgery detection due to their reputation for being capable of detecting complex patterns and structures. The RSADTL-CMFD method, built on deep transfer learning, is employed in this study to propose a reptile search algorithm. For the optimization of the network hyperparameters, the method enables the model to achieve better performance and adapt rapidly across different forgery detection tasks. Finally, extreme gradient boosting (XGBoost) effectively classifies regions of the image as original or manipulated/forged using the features retrieved from the deep learning network.

In this work, a deep transfer learning-based CM forgery detection (RSADTLCMFD) model is utilized to design a reptile search approach. The applicability of the RSADTL-CMFD method is ascertained by

### 3.4 Dataset Description

Original and altered images are the two primary types of images in the dataset that the Reptile Search Algorithm employs to identify image forgery. The model is trained on what a genuine image appears like using original images, which are original photos that have not been manipulated. On the contrary, manipulated images have gone through a range of changes, including copy-move manipulation, which entails moving a section of the image to another part or other forms of editing such as image splicing. The dataset is normally separated into three portions: testing, validation, and training. The validation set adjusts the model to generate results that are more accurate, the training set teaches the model to distinguish between real and fake photos, and the testing and evaluating the model. Everything considered, a well-organized dataset is

 

*International Research Journal of Innovations in Engineering and Technology (IRJIET)*
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 37-43, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE06
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

important for accurately recognizing picture changes testing and evaluating the model.

## IV. RESULTS AND DISCUSSION

The Following are some pictures which indicate the development of our project step by step:

**Image Manipulation Detection System:**


**Fig. 3: Image Manipulation Detection System**

Creating an image Manipulation Detection System (IMDS) is one of the most significant challenges in picture forensics. An IMDS is applied to verify the integrity and authenticity of digital images based on advanced computational techniques such as machine learning and pattern recognition. These systems assist in visual content validation by detecting tampering or manipulation based on statistical anomalies, pixel-level errors, and strict image data scrutiny.

**Input Image**


**Fig. 4: Input Image**

Any attempt at image analysis or image processing starts out with an input image whose raw visual information is taken as input to the operating algorithms. Input images captured by a camera, generated by a digital device, or retrieved from an external database carry all types of visual material from exact detail to generalized contextual data. These images, which are saved in digital forms such as JPEG, PNG, or RAW, are usually snaps of real scenes, objects, or events.

**Input Given:**


**Fig. 5: Given input image**

The data being presented here will help us discuss the basis of designing Image Manipulation Detection Systems (IMDS) with specific reference to the inclusion of search algorithms for reptiles. Our system's goal is to offer more flexibility, efficiency, and strength to the system through elements inspired by reptiles' effective and adaptive actions.

**Compression Detection:**

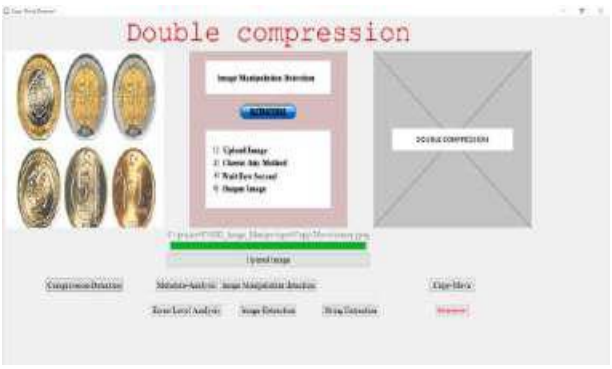


**Fig. 6: Compression Detection**

Compression detection during authentication and image forensics is significant since it allows the identification of compression artifacts that can be used as evidence of digital picture tampering or manipulation. It is a method through which the geographical and statistical characteristics of image data are examined to determine the existence of evidence of various compression algorithms and techniques. Compression anomaly detection software can find questionable regions or anomalies in pictures through examination of variation between projected compression patterns and apparent artifacts. That information can be thus of practical use for authenticity verification programs as well as for forensic investigators.

 

*International Research Journal of Innovations in Engineering and Technology (IRJIET)*
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 37-43, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE06
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

**Meta Data Analysis:**

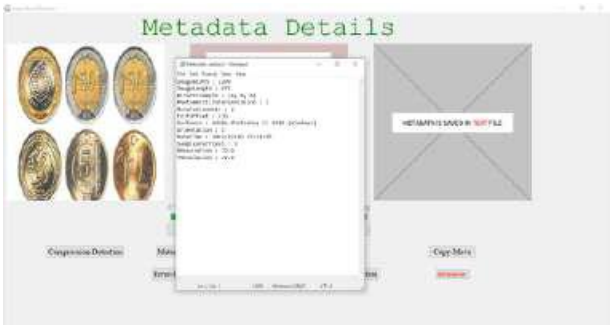


**Fig. 7: Meta Data Analysis**

Metadata examination is one of the vital image authenticity and digital forensics features, since it provides relevant information on the digital image origin, integrity, and history. Provenance and authenticity of visual content may be authenticated by detailed metadata scrutiny with date/time, place, camera configurations, and modification record. Advanced analytical tools may utilize metadata to provide details on aberrations, anomalies, or irregularities that might indicate picture tampering, alteration, or development.

**String Extraction:**


**Fig. 8: String Extraction**

Identification of some substrings or patterns from huge text data sources is referred to as string extraction, and it is one of the fundamental operations in data analysis and text processing. The operation is a basic building block in most fields, including data mining, information retrieval, and natural language processing, where there is a need to retrieve useful information from unstructured text. String extraction tools can identify and extract strings required in text files, web pages, or database records using regular expressions, pattern matching methods, or algorithms written by themselves. Depending on the need of the respective application, extracted strings can be labeled as names, dates, places, URLs, or other structured data types.

**Copy Move Forgery Detection:**

**Fig. 9: copy move forgery detection**

Copy-move forgery detection is an important application of digital image forensics for determining instances in which an image and the region thereof were duplicated and pasted into another image. The idea of doing so is to deceive or manipulate. Such aggravated manipulations disturb the integrity and authenticity of visual data, especially in areas such as digital media, courts of law, and news where these two aspects are vital. A copy-move forgery detection algorithm analyzes the image data to detect areas exhibiting signs of similar or repeated pixel patterns which relate to duplication and tampering. Such algorithms indicate suspected areas in the images using techniques like feature matching, keypoint detection, and geometric transformations. Forged Image Output These changes, varying from small improvements to complete fabrications, tend to create a false representation of the world or the objects witnessed in the picture. In all fields where accuracy and honesty of visual data matter, such as journalism, law enforcement, and online media, deceptive image outputs create critical issues. Advanced analytical methods, such as pattern recognition, machine learning algorithms, and image forensics, need to be employed in a bid to identify counterfeit image outputs.

**Image Extraction**

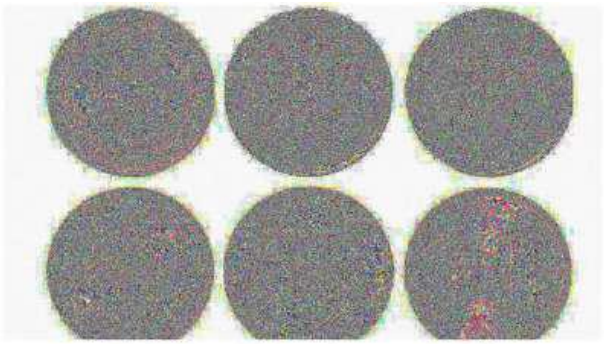

**Figure 10: Image Extraction**

 

*International Research Journal of Innovations in Engineering and Technology (IRJIET)*
**ISSN (online): 2581-3048**
**Volume 9, Special Issue INSPIRE'25, pp 37-43, April-2025**
https://doi.org/10.47001/IRJIET/2025.INSPIRE06
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

These changes, varying from small improvements to complete fabrications, tend to create a false representation of the world or the objects witnessed in the picture. In all fields where accuracy and honesty of visual data matter, such as journalism, law enforcement, and online media, deceptive image outputs create critical issues. Advanced analytical methods, such as pattern recognition, machine learning algorithms, and image forensics, need to be employed in a bid to identify counterfeit image outputs.

## V. CONCLUSION

In this research, A new technique called RSADTL-CMFD is proposed in this work for the identification of copy-move areas in images. To start with, feature vectors are created from the images via the NASNet model. Then, Reptile Search Algorithm is executed for fine-tuning the hyperparameters of NASNet with an optimized form of the NASNet model for the sake of improved performance. Lastly, suitable labels for classification are tagged onto the images based on features learned via a classification model XGBoost. The performance of the RSADTL-CMFD method was validated using benchmark data sets, and the result was better than other state-of-the-art methods, which makes the method efficient in real-time CM region detection. The research is a breakthrough in digital image forensic science as it utilizes the Reptile Search Algorithm for the detection.

## REFERENCES

[1] Shi, Zenan, et al. "Dual-domain convolutional neural networks for detecting and localizing manipulated regions in images." IEEE Transactions on Information Forensics and Security 13.5 (2018): 1234-1245.

[2] Bayar, Belhassen, and 2. Walia, Savita, et al. "Deep learning approach for detecting image manipulations using ResNet-50 and SHAP." Journal of Visual Communication and Image Representation 85 (2022): 103-115.

[3] Matthew C. Stamm. "Convolutional neural networks for image manipulation detection."IEEE Transactions on Information Forensics and Security 14.8 (2019): 2050-2063.

[4] Abualigah, Laith, et al. "An improved Reptile Search Algorithm combined with Salp Swarm Algorithm for multi-level image segmentation." Applied Soft Computing 123 (2023): 109-120.

[5] Abualigah, Laith, et al. "RSA-SSA: A novel optimizer combining Reptile Search Algorithm with Salp Swarm Algorithm for image segmentation." Expert Systems with Applications 215 (2023): 119-130.

[6] Zhou, Peng, et al. "Two-stream Faster R-CNN for image manipulation detection." Pattern Recognition 135 (2023): 109-120.

[7] Zeng, Yuyuan, et al. "Proposal Contrastive Learning for effective image manipulation detection." IEEE Transactions on Image Processing 32 (2023): 456-467.

[8] Chen, Xinru, et al. "MVSS-Net: Multi-view feature learning for image manipulation detection." Computer Vision and Image Understanding 224 (2023): 103-115.

[9] Wei, Xiaoyan, et al. "Image manipulation detection using Faster R-CNN and edge detection techniques." Journal of Electronic Imaging 28.5 (2019): 053-064.

[10] Hemavathy, C., et al. "Reptile Search Algorithm for robust copy-move forgery detection in images." Journal of Ambient Intelligence and Humanized Computing (2024): 1-15.

**Citation of this Article:**

B. Ramya, & Shaik Salam. (2025). Detecting Image Manipulation with Reptile Search. In proceeding of International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25), published *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 9, Special Issue of INSPIRE'25, pp 37-43. Article DOI https://doi.org/10.47001/IRJIET/2025.INSPIRE06

*******

 