

Exploration of digital image tampering detection using CNN with modified particle swarm optimization in deep learning

Umamaheswari, Kannan, Juliet Rozario, Manimekala
Department of Computer Science, Christ University, Bangalore, India

Article Info

Article history:

Received Oct 4, 2024

Revised Dec 20, 2024

Accepted Mar 9, 2025

Keywords:

Convolutional neural networks

Deep learning

Ensemble learning

Image tampering

Particle swarm optimization

ABSTRACT

The field of image processing is crucial for many different applications, including forensic evidence, insurance claims, medical imaging, bio-informatics, artifact collection and more. In many sectors nowadays, digital photographs are regarded as a trustworthy source of information. The manipulation of such photographs leads to a variety of issues. The study presents a method using convolutional neural networks (CNN) combined with modified particle swarm optimization (MPSO) to improve the accuracy of tampering detection. This advancement contributes to improved reliability in fields requiring image authenticity verification, such as forensics and media. The design includes the collection of a dataset comprising both original and tampered images for training and testing the model. A dataset, such as the Media Integration and Communication Center (MICC) dataset, is utilized, which includes various images that have been altered through different tampering techniques. This dataset serves as the foundation for training the CNN and evaluating its performance. The findings indicate that the proposed MPSO_CNN method outperforms traditional techniques in terms of precision, accuracy, recall, and F-measure, demonstrating its effectiveness in identifying tampered images. The results highlight the significance of using advanced deep learning techniques for reliable image authenticity verification.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Umamaheswari

Department of Computer Science, Christ University

Bangalore, Karnataka, India

Email: umamaheswari.d@christuniversity.in

1. INTRODUCTION

It is one of the interesting fields which already proved its efficiency in solving the classification problems related to images. Due to its fullest performance in case of detecting objects and classifying the scenes, learning is the most popular one which helps the researchers to extract complex dependencies from the high dimensional inputs [1]. The total number of features present in the tampered image would change, if any pre-processing operation is performed on that image [2]. A robust feature set is created by classifying and combining all the extracted features for improving the image [3]. The perfect designing and usage of the feature sets helps us to differentiate the tampered image from the original one. The main difficulty lies in this task is the extraction of the correct features [4]. Usually, the tampered images are smoothened during the post-processing to reduce or clear out the edge erection changes. The researches have to find out these things with the help of the copy-move or splicing detection techniques [5]. The first step in the research is pre-processing which includes the various steps like normalization of an image, rescaling and analysing the error level in the input images [6].

The tampering recognition and localization problem for pictures occurs when it is obtained through splicing of content initially shot from dissimilar camera types [7]. The copy-move forgery, splicing and retouching are some of the conventional forgery detection methods. In these methods copy-move proves its worthiness through detecting the colour, texture and device properties [8].

Deep learning is one of the sub fields of machine learning where the concepts are influenced by artificial neural network. It learns the structures deeply using neural network architectures and thus it is called as deep neural network [9]. The methods in the deep learning helps us to discover the salient features of the image and proves its worthiness [10]. The face swapping technique is also one of the remarkable growths in the graph of deep learning. With the help of convolutional neural networks (CNN), mostly the face detection, pose estimation are also possible [11]. In many of the emerging detection of tampering methods, CNN is the most important and crucial one in extraction of the important features to detect the image forgery. In their existing form, CNN will absorb structures that capture an image's content as conflicting to manipulation recognition features [12]. In the recent days, the CNN proves its ability to achieve the best results in case of images in the fields like medicine, and insurance [13]. Maximum number of researches includes particle swarm optimization (PSO) algorithm to optimize the architecture of CNN in order to achieve the expected results in various applications [14]. The PSO when combined with CNN optimizes the process thus increasing the performance in various tasks [15]. Some of the disadvantages in PSO with CNN are rectified in modified PSO with CNN to improve the efficiency and reduce the consumption of time.

Many applications, like the gathering of artifacts, the submission of receipts, and the remembering of events, heavily rely on digital photos. However, a lot of the issues we face today are brought on by digital images. The image source is also used for a variety of unlawful operations [16]. With the aid of image editing software, digital information can be changed, with the ability to add or remove items as well as perform any action on the original image. Because of the picture alterations, the original image's legitimacy is in doubt. Sometimes, inadvertent picture manipulation cannot be taken seriously [17]. In the field of military courts and politics, the images have a powerful impact on the national security and stability which helps in attaining the peace of people's life [18]. That's why the risk is taken to find out the percentage of tampering in the images. Sometimes the best versions of DCNN architectures helps us to obtain the salient features of the taken image. But the image should be normalized in order to classify them [19].

Due to the problems in the double compression and recompression of images, most of the researchers concentrate on JPEG images to localize easily. But in the field of research, the tools should not be concentrating on any particular image format and it should be easy the localize the modified region [20]. Conventional approaches in the image processing finds out the patterns related to the tampered content while classifying the data. But regarding the use of deep learning the researchers are happy with the performance and results when compared with the other approaches. Deep learning concentrates more on highly dependent generalization problems and proper selection of required parameters [21]. When these altered photographs are taken into account as forensic evidence, the matter becomes more serious. In these circumstances, it is important to demonstrate the authenticity of the visible visuals [22]. In the majority of hospitals, a patient's treatment is determined by the findings of medical scans [23]. There is no more thought given to this. Image manipulation causes the doctor to provide the incorrect treatment in certain circumstances. Medical data and scans are used mostly in the insurance industry to support claims for medical insurance [24].

Even today, crop insurance claims can be made using photos of crop damage caused by flooding [25]. In these circumstances, direct investigation is not possible. Therefore, the insurance companies validate the photographs sent by the clients. In this case, tampering benefits the con artists. In the case of crop and medical insurance, the reimbursement will be provided as anticipated after verification of the altered or faked pictures [26]. The tampering detection method we suggest determines the degree of tampering and hence confirms the defined image's expected authenticity [18]. The companies can therefore release the funds following the verification. As a result, the authentic submission and transactions satisfy both parties [27]–[29]. Finally, the effectiveness of the current and suggested strategies is assessed. Image forgeries can be detected and localized by using deep convolution neural network to classify the images and also to train and test the data to obtain the best results when compared with the other approaches.

2. METHOD

2.1. Enhanced image tampering detection using deep learning and swarm intelligence

This model's primary objective is to detect manipulated images. Images that have been tampered with can convey false information because they have been manipulated in some way. Figure 1 shows the steps in the proposed workflow model:

- Image input: the first step is to take the digital image that we want to check. This could be any photo, like a picture from a news article or a personal photo.
- Preprocessing: before analyzing the image, it needs to be prepared. This might involve resizing the image or adjusting its quality so that the analysis can be done more effectively.
- Feature extraction: in this step, the model looks for specific features in the image. Features are important parts of the image that can help identify if it has been changed. The significant features are extracted with CNN from the image and taken for comparing with the training data to find out the authenticity of that input image.
- Using CNN: this is a type of artificial intelligence that helps in analyzing the image. CNNs are good at recognizing patterns, much like how our brains recognize faces. They look at the features extracted earlier to determine if the image is real [26].
- PSO: this is a technique used to make the CNN work faster and more efficiently. Imagine a group of birds flying together to find food; they communicate and adjust their paths to reach their goal quickly. Similarly, this method helps the CNN find the best way to analyze the image [29].
- Tampering detection: after processing the image, the model checks for signs of tampering. If it finds any, it can tell us how much of the image has been changed. This is important because knowing the extent of tampering can help us understand how reliable the image is.
- Output results: finally, the model provides results that indicate whether the image is authentic or has been manipulated. This output can be used by various sectors, such as law enforcement or media, to ensure the information they are sharing is accurate.

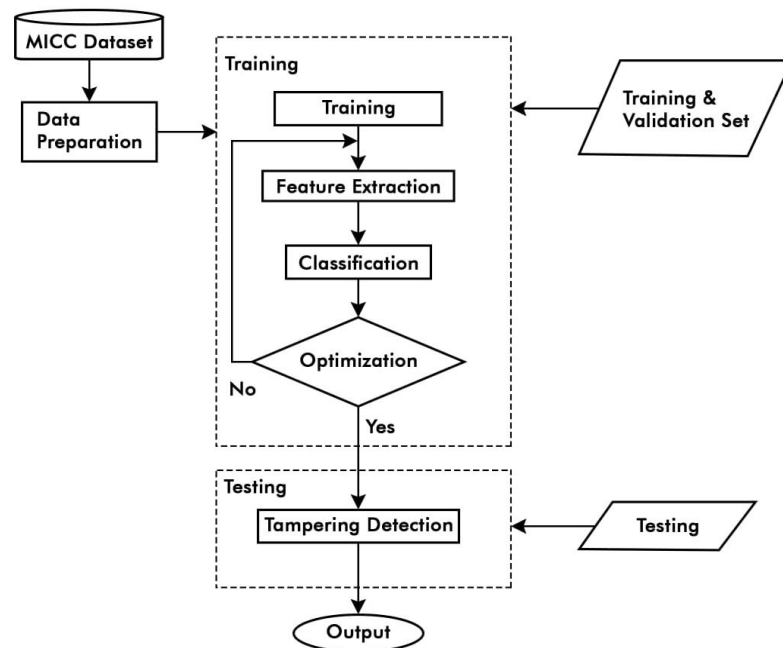


Figure 1. Proposed workflow model

2.2. Modified particle swarm optimization using convolutional neural networks

The modified PSO algorithm proposed in this work provides an excellent solution for image tampering and classification. The proposed algorithm begins by initializing particles with random positions and velocities. Each particle's fitness is then assessed, and its personal best position (Pb) is updated if its current fitness surpasses its previous best. The global best position (Gb) is similarly updated if any particle's Pb improves upon it. Particle velocities are adjusted using an equation that incorporates inertia weight, acceleration coefficients, and random numbers, guiding them toward their Pb and the Gb. Subsequently, particle positions are updated by adding their velocities, with a conditional rule that either applies the full calculated velocity or limits it to a maximum percentage increase. This iterative process of fitness evaluation, best position updates, and velocity/position adjustments continues until a predefined stopping criterion is met, signifying convergence towards a solution. The following are the steps that the proposed MPSO_CNN should follow in Algorithm 1.

Algorithm 1. MPSO_CNN

1. Initialize the parameters using random positions and velocities.
2. Assess each particle's fitness.
3. Determine the particle best (P_b): if particle I 's fitness value is higher than its best fitness value (P_b), particle I 's current fitness value will be its new P_b .
4. Determine the global best (G_b): G_b is set to the current value if any updated P_b is superior to the G_b .
5. Use the following equation to update the particle Velocities

$$V_y = IV_y + A_1R_1(P_b.i - P_i) + A_2R_2(G_b.i - P_i) \quad (1)$$

where V_y is the velocity, I is the inertia weight, A_1 and A_2 are the acceleration coefficients and R_1 and R_2 are the random numbers.

6. Add the velocity to the position value to move the particles to that location.

If $R_3 > PR_3$ then

$$P_i = P_i + V_{yi}(1 + 2P_v(R_4 - 0.5)) \quad (2)$$

Else

$$P_i = P_i + V_{yi} \quad (3)$$

where PR_3 is the percentage of particles covered by the change of the velocity and P_v is the maximum increase in the percentage speed of the particles.

7. The procedure is carried out till the desired result is reached.

3. RESULTS AND DISCUSSION

Both the original and tampered images in the database are accepted for training and the CNN catches the features for the whole dataset. The results of both the existing and new algorithms are shown in this section. These techniques are applied to Media Integration and Communication Center (MICC) dataset on MATLAB 2019a, and the classification performance indicators are listed below.

3.1. Evaluation parameters

Table 1 shows the evaluation parameters of the proposed model. evaluation parameters are essential for assessing the performance of classification models, particularly in tasks such as image tampering detection, where distinguishing between altered and unaltered images is critical.

Table 1. Evaluation parameters	
Metrics	Formula
Accuracy [27]	$\frac{\text{Number of Correct Predictions}}{\text{Allof the Predictions}}$
Precision [27]	$\frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}}$
Recall [27]	$\frac{\text{True Positive}}{\text{True Positive} + \text{False Negative}}$
F-measure [27]	$\frac{(2 * \text{Precision} * \text{Recall})}{(\text{Precision} + \text{Recall})}$
Percentage of Tampering [27]	$1 - \frac{(2\mu_x\mu_y + C1)(2\sigma_{xy} + C2)}{(\mu_x^2 + \mu_y^2 + C1)(\sigma_x^2 + \sigma_y^2 + C2)}$
	2

The major goal of the proposed research is to identify the kind of image manipulation that distinguishes an image as altered or unaltered. There are several techniques to spot modified or tampered with photos, including looking for signs of cloning, studying the edges, analyzing the shadows, and missing reflections. The images given in the Figure 2 shows the detection of tampering in the tampered images using

the techniques CNN [24], PSO_CNN [29] and MPSO_CNN and the classifications results are tabulated in Table 2.

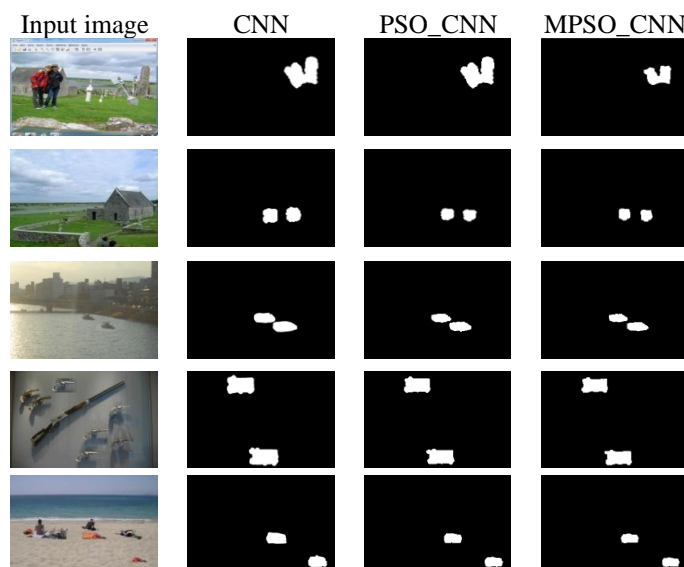


Figure 2. Tampered output image

Table 2. Classification using ensemble classifier

Algorithm	Image	Accuracy	Precision	Recall	F-measure	Percentage of tampering
CNN	Image1	93	91	93	92	3.6
	Image2	92	90	92	91	3.1
	Image3	92	91	91	91	2.7
	Image4	93	90	92	91	3.9
	Image5	93	90	92	91	3.9
PSO_CNN	Image1	95	93	95	94	3.5
	Image2	94	92	96	94	2.9
	Image3	94	92	96	94	2.6
	Image4	94	94	95	94	3.7
	Image5	95	93	95	94	3.9
MPSO_CNN	Image1	98	96	98	97	3.0
	Image2	98	95	97	96	2.5
	Image3	98	96	96	96	1.9
	Image4	97	95	97	96	2.9
	Image5	97	96	98	97	3.5

The ensemble classifier reduces bias and variance, which improves model accuracy. The Table 2 shows results for each image under the three different algorithms. For CNN, the accuracy ranges from 92% to 93%, with a percentage of tampering between 2.7% and 3.9%. For PSO, the accuracy improves slightly, ranging from 94% to 95%, with a percentage of tampering from 2.6% to 3.9%. The MPSO_CNN method shows the best results, with accuracy reaching up to 98% and a lower percentage of tampering, as low as 1.9%. The results indicate that the MPSO_CNN method is the most effective for detecting tampering in images, as it has the highest accuracy and the lowest percentage of tampering. This suggests that combining CNN with PSO leads to better performance in identifying altered images.

Back propagation neural network classifier (BPNN) is utilized to analyze the contours and corners of images, which helps in achieving accurate findings during the classification process. In the context of image tampering detection, a lower percentage indicates a better outcome in terms of authenticity. The results of the calculations for precision, accuracy, recall, and F-measure are reported in Table 3. CNN's accuracy varies from 90% to 93%, with a tampering rate of 2.7% to 3.9%. For PSO, accuracy improves marginally, ranging from 93% to 95%, with a tampering rate of 2.4% to 3.7%. MPSO_CNN outperforms both CNN and PSO_CNN across all metrics, with accuracy values reaching up to 98%, precision up to 96%, recall up to 98%, and F-measure up to 97%. It is concluded that the proposed MPSO_CNN is the preminent method when compared to the other two techniques and evaluated using BPNN classifier.

Table 3. Classification using BPNN classifier

Algorithm	Image	Accuracy	Precision	Recall	F-measure	Percentage of tampering
CNN	Image1	91	89	90	89	3.6
	Image2	90	89	90	89	2.8
	Image3	90	89	90	89	2.7
	Image4	90	88	89	88	3.7
	Image5	91	88	89	88	3.9
PSO_ CNN	Image1	94	92	93	92	3.2
	Image2	93	91	92	91	2.7
	Image3	94	91	91	91	2.4
	Image4	93	92	92	92	3.0
	Image5	94	92	93	92	3.2
MPSO_ CNN	Image1	97	95	97	96	2.8
	Image2	96	94	96	95	2.3
	Image3	96	95	96	95	1.9
	Image4	96	95	96	95	2.8
	Image5	97	95	97	96	3.2

Table 4 presents the performance metrics of the support vector machine (SVM) classifier applied to various images for the task of detecting tampering. The CNN algorithm shows good performance with accuracies mostly around 89-90%. The percentage of tampering ranges from 2.5 to 3.8. PSO_CNN method improved the results, with accuracies reaching up to 93% and the tampering percentage is slightly lower at 3.1 compared to CNN. The modified PSO method shows the best performance overall, with accuracies as high as 96 and the tampering percentage is 2.8, indicating it is very effective at detecting tampering.

Table 4. Classification using SVM classifier

Algorithm	Image	Accuracy	Precision	Recall	F-measure	Percentage of tampering
CNN	Image1	90	89	90	89	3.3
	Image2	89	89	90	89	2.9
	Image3	89	88	91	89	2.5
	Image4	90	88	90	89	3.5
	Image5	89	87	90	88	3.8
PSO_ CNN	Image1	93	92	93	92	3.1
	Image2	92	91	93	92	2.6
	Image3	91	92	92	92	2.1
	Image4	92	91	92	91	3.1
	Image5	93	91	93	92	3.4
MPSO_ CNN	Image1	96	95	97	96	2.8
	Image2	96	95	96	95	2.3
	Image3	95	94	97	95	1.7
	Image4	94	94	97	95	2.7
	Image5	95	94	96	95	3.2

The Tables 2-4 collectively assess the proposed MPSO_CNN by providing comparative performance metrics against other algorithms. The consistent superior performance of MPSO_CNN across various metrics and classifiers demonstrates its effectiveness and reliability in detecting digital image tampering, making it a significant advancement in the field. The quantitative evidence presented in these tables supports the conclusion that MPSO_CNN is a robust solution for image tampering detection. The consistent improvement in performance metrics across multiple tables highlights the effectiveness of combining modified PSO with CNN for this task.

4. CONCLUSION

The proposed MPSO_CNN was trained using both original and tampered images from the MICC dataset, allowing it to learn features across the entire dataset effectively. The developed model was able to detect the region of tampering accurately in the tampered images. The classification performance indicators were evaluated, showing that the proposed model outperformed existing algorithms in terms of accuracy and efficiency. This indicates that the integration of PSO with CNN enhances the model's ability to detect tampered images. The research emphasized the importance of robust feature extraction, which was achieved through preprocessing steps like normalization and error level analysis. Future works could explore the incorporation of more advanced deep learning architectures, such as generative adversarial networks (GANs) or transformer-based models, to enhance feature extraction and improve tampering detection accuracy.

ACKNOWLEDGMENTS

The authors would like to thank the reviewers for their valuable comments and suggestions. This work is not funded by any organization.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Umamaheswari	✓		✓						✓					
Kannan		✓		✓					✓			✓	✓	
Juliet Rozario				✓	✓			✓		✓				
Manimekala						✓	✓			✓				

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.




REFERENCES

- [1] L. M. Dang, K. Min, S. Lee, D. Han, and H. Moon, "Tampered and computer-generated face images identification based on deep learning," *Applied Sciences (Switzerland)*, vol. 10, no. 2, p. 505, Jan. 2020, doi: 10.3390/app10020505.
- [2] J. Bunk *et al.*, "Detection and Localization of Image Forgeries Using Resampling Features and Deep Learning," in *IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2017, pp. 1881–1889, doi: 10.1109/CVPRW.2017.235.
- [3] J. H. Bappy, A. K. Roy-Chowdhury, J. Bunk, L. Nataraj, and B. S. Manjunath, "Exploiting Spatial Structure for Localizing Manipulated Image Regions," in *Proceedings of the IEEE International Conference on Computer Vision*, IEEE, Oct. 2017, pp. 4980–4989, doi: 10.1109/ICCV.2017.532.
- [4] I. B. K. Sudiatmika, F. Rahman, T. Trisno, and S. Suyoto, "Image forgery detection using error level analysis and deep learning," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, no. 2, pp. 653–659, Apr. 2019, doi: 10.12928/telkomnika.v17i2.8976.
- [5] N. K. Hebbar and A. S. Kunte, "Transfer Learning Approach for Splicing and Copy-Move Image Tampering Detection," *ICTACT Journal on Image and Video Processing*, vol. 11, no. 04, p. 4, 2021.
- [6] W. P. Sari and H. Fahmi, "Effect of Error Level Analysis on The Image Forgery Detection Using Deep Learning," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, vol. 6, no. 3, pp. 187–194, Aug. 2021, doi: 10.22219/kinetik.v6i3.1272.
- [7] S. Manjunatha and M. M. Patil, "Deep learning-based technique for image tamper detection," in *Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV 2021*, IEEE, Feb. 2021, pp. 1278–1285, doi: 10.1109/ICICV50876.2021.9388471.
- [8] N. Goel, S. Kaur, and R. Bala, "Dual branch convolutional neural network for copy move forgery detection," *IET Image Processing*, vol. 15, no. 3, pp. 656–665, Feb. 2021, doi: 10.1049/ipr2.12051.
- [9] P. P. Dhavalkumar, "Smart Healthcare Forgery Detection Using Deep Learning," *International Journal of Advance Research and Innovative Ideas in Education*, vol. 5, no. 3, pp. 1670–1674, 2019.
- [10] P. Johnston, E. Elyan, and C. Jayne, "Video tampering localisation using features learned from authentic content," *Neural Computing and Applications*, vol. 32, no. 16, pp. 12243–12257, 2020, doi: 10.1007/s00521-019-04272-z.
- [11] X. Ding, Z. Raziei, E. C. Larson, E. V. Olinick, P. Krueger, and M. Hahsler, "Swapped face detection using deep learning and subjective assessment," *Eurasip Journal on Information Security*, no. 1, 2020, doi: 10.1186/s13635-020-00109-8.
- [12] B. Bayar and M. C. Stamm, "A deep learning approach to universal image manipulation detection using a new convolutional layer," in *Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security*, New York, NY, USA: ACM,




- Jun. 2016, pp. 5–10, doi: 10.1145/2909827.2930786.
- [13] S. K. Prabhakar, H. Rajaguru, K. So, and D. O. Won, "A Framework for Text Classification Using Evolutionary Contiguous Convolutional Neural Network and Swarm Based Deep Neural Network," *Frontiers in Computational Neuroscience*, vol. 16, Jun. 2022, doi: 10.3389/fncom.2022.900885.
 - [14] L. Bondi, S. Lameri, D. Guera, P. Bestagini, E. J. Delp, and S. Tubaro, "Tampering Detection and Localization Through Clustering of Camera-Based CNN Features," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, IEEE, Jul. 2017, pp. 1855–1864, doi: 10.1109/CVPRW.2017.232.
 - [15] T. Lawrence, L. Zhang, K. Rogage, and C. P. Lim, "Evolving deep architecture generation with residual connections for image classification using particle swarm optimization," *Sensors*, vol. 21, no. 23, pp. 1–23, Nov. 2021, doi: 10.3390/s21237936.
 - [16] A. H. Saber, M. A. Khan, and B. G. Mejbél, "A survey on image forgery detection using different forensic approaches," *Advances in Science, Technology and Engineering Systems*, vol. 5, no. 3, pp. 361–370, 2020, doi: 10.25046/aj050347.
 - [17] X. Chu and H. Li, "A Survey of Blind Forensics Techniques for JPEG Image Tampering," *Journal of Computer and Communications*, vol. 07, no. 10, pp. 1–13, 2019, doi: 10.4236/jcc.2019.710001.
 - [18] H. D. Deng and Y. Qiu, "Image-level forgery identification and pixel level forgery localization via a convolutional neural network," *NIPS*, pp. 1–6, 2018.
 - [19] Y. Muhammad, M. D. Alshehri, W. M. Alenazy, T. V. Hoang, and R. Alturki, "Identification of Pneumonia Disease Applying an Intelligent Computational Framework Based on Deep Learning and Machine Learning Techniques," *Mobile Information Systems*, pp. 1–20, May 2021, doi: 10.1155/2021/9989237.
 - [20] Y. Zhang, J. Goh, L. L. Win, and V. Thing, "Image region forgery detection: A deep learning approach," in *Proceedings of the Singapore Cyber-Security Conference (SG-CRC)*, 2016, pp. 1–11, doi: 10.3233/978-1-61499-617-0-1.
 - [21] Y. Rodriguez-Ortega, D. M. Ballesteros, and D. Renza, "Copy-move forgery detection (Cmfd) using deep learning for image and video forensics," *Journal of Imaging*, vol. 7, no. 3, pp. 1–16, Mar. 2021, doi: 10.3390/jimaging7030059.
 - [22] H. Fahmi and W. P. Sari, "Effectiveness of Deep Learning Architecture for Pixel-Based Image Forgery Detection," in *Proceedings of the International Conference on Engineering, Technology and Social Science (ICONETOS 2020)*, 2021, doi: 10.2991/assehr.k.210421.044.
 - [23] Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," in *2016 IEEE International Workshop on Information Forensics and Security (WIFS)*, IEEE, Dec. 2017, pp. 1–6, doi: 10.1109/WIFS.2016.7823911.
 - [24] A. A. Aminu and N. N. Agwu, "General Purpose Image Tampering Detection using Convolutional Neural Network and Local Optimal Oriented Pattern (LOOP)," *Signal & Image Processing: An International Journal*, vol. 12, no. 2, pp. 13–32, Apr. 2021, doi: 10.5121/sipij.2021.12202.
 - [25] B. Diallo, T. Urruty, P. Bourdon, and C. Fernandez-Maloigne, "Robust forgery detection for compressed images using CNN supervision," *Forensic Science International: Reports*, vol. 2, pp. 1–11, Dec. 2020, doi: 10.1016/j.fsir.2020.100112.
 - [26] D. H. Kim and H. Y. Lee, "Image manipulation detection using convolutional neural network," *International Journal of Applied Engineering Research*, vol. 12, no. 21, pp. 11640–11646, 2017.
 - [27] D. Umamaheswari and E. Karthikeyan, "Exploration of Digital Image Tampering Using Enhanced Feature Extraction Algorithms in Machine Learning," *International Journal on Technical and Physical Problems of Engineering*, vol. 14, no. 2, pp. 322–329, 2022.
 - [28] X. Wang, H. Wang, S. Niu, and J. Zhang, "Detection and localization of image forgeries using improved mask regional convolutional neural network," *Mathematical Biosciences and Engineering*, vol. 16, no. 5, pp. 4581–4593, 2019, doi: 10.3934/mbe.2019229.
 - [29] X. Kan *et al.*, "A novel PSO-based optimized lightweight convolution neural network for movements recognizing from multichannel surface electromyogram," *Complexity*, pp. 1–5, 2020, doi: 10.1155/2020/6642463.

BIOGRAPHIES OF AUTHORS






Dr. Umamaheswari    is currently working as Assistant Professor, Department of Computer Science, Christ (Deemed to be University), Yeshwanthpur Campus, Karnataka, India. She received her Ph.D. from Bharathiar University, Tamil Nadu, India. She has 16 years of teaching experience. Her areas of research interest include data mining, image processing and machine learning. She has published nearly 12 papers in national, international journals and Scopus indexed journals. She has presented papers in national and international conferences. She received a prestigious seed money grant, underscoring her commitment to pioneering innovative research projects. She can be contacted at email: umamaheswari.d@christuniversity.in.






Dr. Kannan    is currently working as Assistant Professor, Department of Computer Science, Christ (Deemed to be University), Yeshwanthpur Campus, Karnataka, India. He received his Ph.D. and M.Phil. degree in Computer Science from Vels University, Tamilnadu, India. He was a Rank Holder in M.Sc. (Computer Science), Madras University. His research interest includes machine learning, deep learning, data mining, and artificial intelligence in Health care sector. He has published more than ten research papers in IEEE, SCOPUS indexed journals. He also published two patents in Intellectual Property Rights and four Book Chapters in SPRINGER, ELSEVIER, CRC Press Publications. He has presented paper in Lincoln University, Malaysia. He serves as Meta-Reviewer in IEEE International Conference, IIIT Kottayam, India. He was a Technical Committee Member in International Conference, Thailand and India. He can be contacted at email: kannan.m@christuniversity.in.



Dr. Juliet Rozario    is an expert with over 14 years of academic experience. She has consistently contributed to advancing research, education, and practical applications in her field. Her areas of expertise include nature-inspired algorithms, artificial intelligence, and optimization techniques, which have proven instrumental in solving complex problems in diverse sectors. She received a prestigious seed money grant, underscoring her commitment to pioneering innovative research projects. She can be contacted at email: juliet.rozario@christuniversity.in.



Dr. Manimekala    is working as an Assistant Professor in the Department of Computer Science, Christ (Deemed to be University), Yeshwanthpur Campus, Bengaluru. She has 17 years of teaching experience. She has published research articles in National and International journals. She has also presented 18 papers in National and International conferences. She has authored in 1 book, 3 book chapters and she owned 2 patents. Her areas of interest are IoT, networking, machine learning and AI. She can be contacted at email: manimekala.b@christuniversity.in.