Knowledge-Based Systems 340 (2026) 115670

Contents lists available at ScienceDirect

Knowledge-Based Systems

journal homepage: www.elsevier.com/locate/knosys

TayLoXNet: A taylor-inspired hybrid loss function for xception-based image forgery detection

Sujin J S [a,*], P. Bhuvaneswari [b], A.P. Subapriya [c], Granty Regina Elwin J [d]

[a] Assistant Professor, Department of ECE, PSG Institute of Technology and Applied Research, Coimbatore, Tamilnadu, 641 062, India
[b] Professor, Department of Biomedical Engineering, ACS College of Engineering, Bangalore, Karnataka, 560074, India
[c] Assistant Professor, Department of Computer and Communication Engineering, Kathir College of Engineering, Coimbatore, 641062, India
[d] Professor, Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, 641008, India

ARTICLE INFO

Keywords:
Image forensics
Copy-move forgery
Taylor loss xception network
Taylor softmax mean square loss
Learning rule decomposition

ABSTRACT

Manipulating digital images to present a false version of reality is known as image forgery. This modification is performed to deceive the viewers by removing, adding, or altering the elements in an image. Advanced Deep Learning (DL) approaches have been extensively used for detecting image forgery in recent years, as they enable automated analysis of subtle inconsistencies and complex patterns in images. These approaches, however, frequently experience overfitting issues and tend to miss detections due to a significant number of false negatives. Therefore, a new method called the Taylor Loss Xception Network (TayLoXNet) is introduced to detect image forgery. Firstly, the accumulated image is preprocessed by employing a median filter. After extracting the relevant features, the TayLoXNet method is employed to detect image forgery. In this approach, TayLoXNet is implemented by modifying XceptionNet's learning rule with the Taylor Softmax Mean Square (TaylorSMS) loss. Besides, the TaylorSMS loss function is developed by merging the Mean Squared Error (MSE) and SoftMax loss using the Taylor series. Furthermore, the newly devised TayLoXNet method is evaluated using maximal True Negative Rate (TNR), accuracy, and True Positive Rate (TPR) and obtained superior values of 97.227%, 97.366%, and 98.357%, respectively.

1. Introduction

Image forensics is the field of science which assists us in identifying and tracking down image forgeries by determining whether an image is created using the claimed device or whether its present state matches the original acquired image [1]. Images are processed employing a variety of approaches in image forensics to identify evidence, retrieve destroyed evidence, and generate suitable reports on incidents to offer to the court or other relevant parties [2]. The foundation of image forensics approaches is the idea that every phase of an image collecting and processing procedure, from original image to its post-processing, storage, and compression, comprises certain intrinsic statistics and produces a unique record. The absence, presence, or irregular forensic features embedded in the image itself can therefore be employed to determine the image's origin or identify if it is real or modified [1]. Since Deep Learning (DL) algorithms and user-friendly image editing software have advanced, image forging has become readily accessible [3]. Altering a prevailing image's appearance, composition, or content to accomplish a desired outcome is termed image editing. This procedure can involve everything from minor alterations to more substantial changes, all without significantly altering the original image. Modern learning-based algorithms have substituted human, labour-intensive methods in image editing [4]. Image editing processes include either local modifications limited to a selection or broad changes (filters, color/intensity corrections, deformations) [5]. These forgeries can be generated employing free editing software programs, including Adobe Photoshop, GNU's Not Unix (GNU), and GNU Image Manipulation Program (GIMP), that have some advanced image-altering options [6].

Forged images that are difficult to verify with the human eye can be generated by employing modern deep forging methods, content substitution, or feature alteration. Public safety, individual privacy, and even national safety are at risk from the extensive distribution of such images [7]. In the highly automated and interrelated world, digital image and video security has become highly important in applications, including medical imaging, pay-per-view television, private video conferences, industrial or military imaging schemes, passwords, online transactions,

* Corresponding author.
E-mail address: drsujinjs@gmail.com (S.J. S).

https://doi.org/10.1016/j.knosys.2026.115670
Received 6 November 2025; Received in revised form 5 February 2026; Accepted 1 March 2026
Available online 2 March 2026

legal digital signatures, and so on [8]. Software for photo editing can make things more enjoyable, but it also provides hackers the chance to alter images intentionally, which affects digital security. Therefore, detecting if an image has been modified is vital [9]. Image security is one of the primary concerns in any industry, which secures digital homes and businesses from criminal acts and other safety risks. Even yet, it is very difficult to detect forged images employing Photoshop and other robust image manipulation software [10]. Image forgery detection is a crucial aspect of information security [11,12]. The goal of detecting digital image forgery is to detect if an image is authentic or forged, exploiting a binary classification task. The features acquired by the image allocation procedures accomplished at several stages of digital image acquisition and storage are advantageous to the passive image forgery detection methods [6]. Further, there are two classes of forgery detection techniques: DL-based techniques and baseline approaches. Moreover, the precision and durability of these conventional models are limited because they mostly depend on human extraction characteristics. These kinds of approaches accomplish certain standard stages, such as preparing images, matching and extracting features, detecting forgeries, and post-processing [9].

The efficiency of conventional techniques is often influenced by variables, such as algorithm selection and parameter settings, which lead to high computing costs and difficulties in addressing real-time needs [9]. When correlated to prevailing approaches, DL-based models perform well in experiments and can automatically learn specific characteristics during training [12]. DL is an essential part of Machine Learning (ML) that classifies images as either real or forged for detecting forged digital images [13]. In image processing, DL is a robust tool that has attained remarkable outcomes in object denoising, style transfer, segmentation, identification, classification, and compression. Applying DL approaches to image security to address more classical problems has also drawn a lot of attention and has recently made significant advances [14]. The development of image forensics technology has been assisted by the broad utilization of DL technology in this field. In image forensics, DL algorithms, including Convolutional Neural Networks (CNNs), have recently revealed superior results [9,15]. Copy-Move Forgery Detection (CMFD) is one based upon image content image forgery detection methods [12]. Consequently, the CMFD approach has been a significant and ongoing research topic in digital image forensics, which is dedicated to recognizing and assessing them. On the other hand, the target regions' contrast and brightness are identical to those of other regions of the image, which makes it challenging to identify them within the whole image [16].

1.1. Problem statement

The widespread availability of advanced image editing tools enables digital images to be modified or altered without leaving visible traces. These manipulated images, commonly known as forged images, can be used to spread misinformation, harm reputations, produce false evidence, and commit fraud in areas such as social media, law enforcement, journalism, and scientific research. Although image manipulation techniques continue to advance, reliable detection of forged images remains a challenging task. Conventional image forgery detection methods mainly depend on handcrafted features and predefined rules, which limits their effectiveness in identifying manipulation types, such as splicing, copy-move retouching and deepfake generation. Even though DL- based approaches improve detection performance by learning complex image representations many existing models suffer from overfitting when trained on limited datasets and produce high false negative rates, resulting in missed detections. These issues reduce the generalization capability and practical reliability of current systems. Therefore, there is a strong need for an automated and robust detection framework that can accurately identify forged images. Thus, an effective DL method, TayLoXNet is proposed, which enhances the Xception architecture through the TaylorSMS loss function to reduce overfitting, decrease false negatives and improve overall image forgery detection performance.

1.2. Contribution

The primary objective of the proposed TayLoXNet model is to address the overfitting problem and high false negative rate in image forgery detection by introducing a Taylor series–based loss function that stabilizes training and improves generalization performance. The primary contributions of this research are detailed below,

- This work introduces TayLoXNet, a new approach for image forgery detection that modifies XceptionNet's learning rule.
- In this approach, TayLoXNet is implemented by adapting XceptionNet's learning rule with TaylorSMS. The TaylorSMS loss, developed by integrating MSE and SoftMax losses through a Taylor series expansion, addresses overfitting and lowers false negative rates.

1.3. Structural organization

The remaining sections are organized as follows: Section 2 presents the literature survey and highlights the limitations of traditional methods. Section 3 discusses the TayLoXNet approach for image forgery detection. Section 4 illustrates the results produced by TayLoXNet, and Section 5 concludes the paper.

2. Literature review

CAMU-Net was devised by Zhao, K., *et al.* [12] for CMFD. The CAMU-Net technique attained robust performance, enhanced accuracy, and effective extraction of multi-scale key feature maps. Nonetheless, this method did not combine modern image processing methods to comprehensively address image tampering. In [16], a Recursive Wavelet Transform Network (RWTN—Net) was established by Niu, Y., et al. for CMFD. This technique demonstrated high robustness to geometric transformations, which also decreased the information loss, and contributed to optimized computational efficacy and robust generalization performance. Nevertheless, this technique failed in improving the method's capacity to differentiate tampered areas from background regions, due to insufficient utilization of edge information, ultimately limiting its potential to enhance detection accuracy. Liang, E., *et al.* [9] devised Transformer-based Copy-Move Forgery Detection (TransCMFD). The TransCMFD scheme efficiently collected the local and global features of forged images, optimizing the accuracy of tampered area localization. Moreover, this method made effective use of features from tampered areas and optimized both localization accuracy and the model's generalization ability. However, this approach was not trained on a set of databases, which limited its ability to detect forgeries across altered image types and resolutions. Lin, Y., *et al.* [7] introduced the Multi-View Feature Fusion Network (MFF-Net) to detect image forgery. The MFF-Net technique efficiently captured multi-view features, resulting in minimized redundancy, optimized texture representation, and enhanced integrity. Further, this method revealed strong generalization and robustness, delivering superior performance. Still, this approach did not focus on establishing lightweight techniques, which limited its efficacy.

Nirmalapriya, G., *et al.* [10] developed an Aquila Sine Cosine Algorithm-SqueezeNet (ASCA-SqueezeNet) for detecting image forgery. The ASCA-SqueezeNet model exhibited high robustness against noise, optimized feature extraction, enhanced computational efficacy, and detection accuracy. Nevertheless, this method did not combine more modern optimization approaches to replace the original ASCA technique, limiting the potential performance gains of the devised model. Khalil, A.H., et al. [6] presented MobileNetV2 for digital image forgery detection. The MobileNetV2 model enabled faster training while attaining lower computational costs, minimizing system complexity and

Fig. 13 shows the analysis by varying blur conditions, considering both datasets. Fig. 13a) shows the robustness analysis of the proposed TayLoXNet using dataset 1. When the blur strength is considered as 0.4, the CAMU-Net, RWTN—Net, TransCMFD, MFF-Net, and proposed TayLoXNet achieved accuracy of 80.990 %, 81.899 %, 83.888 %, 86.888 %, and 88.999 %, respectively. The assessment of TayLoXNet on dataset-2 is shown in Fig. 13(b). Accuracy values for comparison models are 77.988 % for CAMU-Net, 79.899 % for RWTN—Net, 82.888 % for TransCMFD, 84.888 % for MFF-Net, while the proposed TayLoXNet achieves 86.878 %. On Dataset 2, the model achieved 77.988 %, 79.899 %, 82.888 %, 84.888 %, and 86.878 %. The CAMU-Net, RWTN—Net, TransCMFD, and MFF-Net showed larger reductions in performance under blur, highlighting TayLoXNet's resilience to loss of image sharpness and its ability to detect subtle forgery artifacts despite blurred content.

(iii) Low-Light Condition

Analysis of the proposed TayLoXNet under extreme lighting scenarios is shown in Fig. 14. Fig. 14(a) illustrates its performance on dataset-1 across different light conditions. For the light intensity 0.9, the accuracy values achieved by CAMU-Net is 84.989 %, RWTN—Net is 86.999 %, TransCMFD is 89.879 %, MFF-Net is 91.888 %, and the proposed TayLoXNet model is 93.789 %, respectively. The performance of the proposed TayLoXNet on dataset-2 is shown in Fig. 14(b). With light intensity 0.9, the accuracy obtained by the CAMU-Net, RWTN—Net, TransCMFD, MFF-Net, and proposed TayLoXNet are 87.888 %, 89.877 %, 90.889 %, 92.789 %, and 94.999 %, respectively. These results confirm TayLoXNet's ability to reliably detect forgery even under poor illumination, outperforming CAMU-Net, RWTN—Net, TransCMFD, and MFF-Net, which show reduced accuracy when image brightness is low.

4.12. Cross-dataset validation

Cross-dataset validation measures how well a forgery detection method generalizes by using one dataset for training and a distinct dataset for testing. In this study, the models were trained using the CoMoFoD image forgery database and tested on the Copy-Move Forgery dataset, allowing us to assess how well the methods perform on unseen data with different characteristics. The cross-dataset validation analysis of the proposed TayLoXNet is illustrated in Fig. 15. The assessment of the TayLoXNet model using accuracy is provided in Fig. 15a). For k-value 8, the CAMU-Net achieved an accuracy of 89.988 %, RWTN—Net achieved 91.998 %, TransCMFD achieved 92.999 %, MFF-Net achieved 93.999 %, while TayLoXNet achieved 95.589 %, demonstrating superior performance compared to other models. Fig. 15b) shows the TPR analysis of the proposed TayLoXNet model. With 9 as k-value, the TPR recorded by the CAMU-Net, RWTN—Net, TransCMFD, MFF-Net, and proposed TayLoXNet are 90.888 %, 92.568 %, 93.878 %, 94.777 %, and 96.490 %, indicating that the proposed method detects forgeries more reliably across datasets. The TNR performance of the proposed TayLoXNet model is illustrated in Fig. 15(c). Here, the CAMU-Net achieved a TNR of 86.988 %, RWTN—Net achieved 88.989 %, TransCMFD achieved 90.988 %, MFF-Net achieved 92.999 %, and TayLoXNet achieved 95.010 % when considering the k-value 8, showing that TayLoXNet reduces false positives and maintains higher accuracy on clean regions. This highlights the robustness and practical applicability of the proposed method for real-world scenarios, where training and testing conditions may vary.

5. Conclusion

Image forgery is the process of altering or manipulating digital images to mislead or deceive viewers. It involves several actions, namely adding or removing objects, altering the context, and changing colors to create a false impression. Several image forgery detection techniques have been implemented, but they struggled to achieve high accuracy, resulting in a large number of false positives. Hence, a new model called TayLoXNet is introduced to detect image forgery. Firstly, the collected image from the dataset is preprocessed by exploiting the median filter. Following this, the relevant features are mined, and then the image forgery is detected using the TayLoXNet. Here, TayLoXNet is modelled by adjusting the learning rule of XceptionNet with TaylorSMS. In addition, the TaylorSMS loss function is developed by merging the Taylor series, MSE and SoftMax loss. Furthermore, the newly devised TayLoXNet method computed the maximal TNR, accuracy, and TPR of 97.227 %, 97.366 %, and 98.357 %. Future work aims to enhance the detection efficiency by incorporating a Generative Adversarial Network (GAN) based framework for enhancing the robustness of the proposed scheme to evolving attack patterns. Also, the TaylorSMS loss function can be further refined or combined with other adaptive loss strategies to improve learning on highly imbalanced datasets.

CRediT authorship contribution statement

Sujin J S: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources, Data curation, Writing – original draft, Writing – review & editing, Project administration. **P. Bhuvaneswari:** Conceptualization, Methodology, Software. **A.P. Subapriya:** Validation, Formal analysis, Investigation. **Granty Regina Elwin J:** Resources, Data curation, Writing – original draft, Writing – review & editing, Project administration.

Declaration of competing interest

The authors declare that they have no known competing financialinterestsor personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The data that support the findings of this study are openly available in the CoMoFoD - Image Database at https://www.vcl.fer.hr/comofod/ and the copy-move forgery dataset at https://figshare.com/articles/dataset/Going_deeper_into_copy_move_forgery_detection_exploring_image_telltales_via_multi_scale_analysis_and_voting_processes/978736?file=3157982.

References

[1] I.C. Camacho, K. Wang, A comprehensive review of deep-learning-based methods for image forensics, J. Imaging 7 (4) (2021) 69.
[2] R.S. Khalaf, A. Varol, Digital forensics: focusing on image forensics, in: 2019 7th International Symposium on Digital Forensics and Security (ISDFS), IEEE, 2019.
[3] M.A. Anwar, S.F. Tahir, L.G. Fahad, K. Kifayat, Image forgery detection by transforming local descriptors into deep-derived features, Appl. Soft. Comput. 147 (2023) 110730.
[4] Y. Huang, J. Huang, Y. Liu, M. Yan, J. Lv, J. Liu, W. Xiong, H. Zhang, L. Cao, S. Chen, Diffusion model-based image editing: a survey, IEEE Trans. Pattern Anal. Mach. Intell. (2025).
[5] P. Perez, M. Gangnet, A. Blake, Poisson image editing, in: Seminal Graphics Papers: Pushing the Boundaries, 2, 2023, pp. 577–582.
[6] A.H. KHALIL, A.Z. GHALWASH, H.A.-G. ELSAYED, G.I. SALAMA, H. A. GHALWASH, Inhancing digital image forgery detection using transfer learning, IEEE Access 11 (2023) 91583–91594.
[7] Y. Lin, T. Mao, Z. Chen, H. Lu, Z. Chen, Y. Kang, MFF-Net: a multi-view feature fusion network for generalized forgery image detection, Neurocomputing (2025) 130351.
[8] M. B, G. Holi, S.M. K, An overview of image security techniques, Int. J. Comput. Appl. 154 (6) (2016) 37–46.
[9] E. Liang, K. Zhang, Z. Hua, Y. Li, X. Jia, TransCMFD: an adaptive transformer for copy-move forgery detection, Neurocomputing 638 (2025) 130110.
[10] G. Nirmalapriya, B. Maram, R. Lakshmanan, M. Navaneethakrishnan, ASCA-squeeze net: aquila sine cosine algorithm enabled hybrid deep learning networks for digital image forgery detection, Comput. Secur. 128 (2023) 103155.
[11] C. Shi, L. Chen, C. Wang, X. Zhou, Z. Qin, Review of image forensic techniques based on deep learning, Mathematics 11 (14) (2023) 3134.

[12] K. Zhao, X. Yuan, T. Liu, Y. Xiang, Z. Xie, G. Huang, L. Feng, CAMU-Net: copy-move forgery detection utilizing coordinate attention and multi-scale feature fusion-based up-sampling, Expert. Syst. Appl. 238 (2024) 121918.
[13] A. Oke, K.O. Babaagba, Image forgery detection using cryptography and Deep learning, in: Proceedings of International Conference on Big Data Technologies and Applications, Springer Nature Switzerland, Cham, 2023.
[14] A.P. Rodrigues, P.S. Shetty, P. Shet, P.M. Cornelio, S.N. Baliga, R. Fernandes, Deep Learning in forensic sketch analysis, in: International Conference on Artificial Intelligence and Data Engineering (AIDE), Nitte, India, 2025. May.
[15] K.H. RHEE, Composition of visual feature vector pattern for deep learning in image forensics, IEEE Access 8 (2020) 188970–188980.
[16] Y. Niu, X. Wu, C. Liu, Recursive wavelet transform network for robust copy-move forgery detection, Neurocomputing (2025) 130373.
[17] K. Zhao, X. Yuan, Z. Xie, Y. Xiang, G. Huang, L. Feng, SPA-net: a deep learning approach enhanced using a span-partial structure and attention mechanism for image copy-move forgery detection, Sensors 23 (14) (2023) 6430.
[18] S. Gupta, S. Roy, Medav filter—Filter for removal of image noise with the combination of median and average filters, in: Recent Trends in Signal and Image Processing: ISSIP 2017, Springer, Singapore, 2019, pp. 11–19.
[19] J.S. Sujin, S. Sophia, High-performance image forgery detection via adaptive SIFT feature extraction for low-contrast or small or smooth copy–move region images, Soft comput 28 (1) (2024) 437–445.
[20] W. Wang, Q. Kou, S. Zhou, K. Luo, L. Zhang, Geometry-based completed local binary pattern for texture image classification, in: proceedings of 2020 IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP), IEEE, 2020.
[21] X. Lu, Y.A.F.A. Zadeh, Deep learning-based classification for melanoma detection using XceptionNet, J. Heal. Eng. 1 (2022) 2196096.
[22] S.A. Mangai, B.R. Sankar, K. Alagarsamy, Taylor series prediction of time series data with error propagated by artificial neural network, Int. J. Comput. Appl. 89 (1) (2014) 41–47.
[23] J.S. Kushwah, A. Kumar, S. Patel, R. Soni, A. Gawande, S. Gupta, Comparative study of regressor and classifier with decision tree using modern tools, in: Materials Today: Proceedings, 2022.
[24] Q. Wang, Y. Ma, K. Zhao, Y. Tian, A comprehensive survey of loss functions in machine learning, Ann. Data Sci. 9 (2) (2022) 187–212.
[25] S. Gonzalez, X. Qiu, R. Miikkulainen, Effective regularization through evolutionary loss-function metalearning, in: Proceedings of 2025 IEEE Congress on Evolutionary Computation (CEC), IEEE, 2025.
[26] "CoMoFoD - image database," [Online]. Available: https://www.vcl.fer.hr/comofod/. [Accessed May 2025].
[27] "copy-move forgery dataset," [Online]. Available: https://figshare.com/articles/dataset/Going_deeper_into_copy_move_forgery_detection_exploring_image_telltales_via_multi_scale_analysis_and_voting_processes/978736?file=3157982. [Accessed May 2025].
[28] P. Aryan, R.M.R. Yanamala, A. Pallakonda, R.D.A. Raj, K. Krishna Prakasha, Lightweight end-to-end patch-based self-attention network for robust image forgery detection, IEEE Access 13 (2025) 157674–157686. September.
[29] Q. Man, S. Gee, Y. Cho, Multi-domain perception transformer for generalized forgery image detection, Appl. Sci. 16 (1) (2026). January.