

Optimizing feature extraction for tampering image detection using deep learning approaches

Ramaraj Muniappan¹, Dhendapani Sabareeswaran², Chembath Jothish³, Joe Arun Raja³, Srividhya Selvaraj⁴, Thangarasu Nainan⁵, Bhaarathi Ilango¹, Dhinakaran Sumbramanian¹

¹Department of Computer Science, Rathinam College of Arts and Science, Coimbatore, India

²Department of Computer Science, Government College of Arts and Science for Women, Tiruppur, India

³Department of Computer Science, Presidency University, Bengaluru, India

⁴Department of Computer Science, KPR College of Arts Science and Research, Coimbatore, India

⁵Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, India

Article Info

Article history:

Received Mar 9, 2024

Revised Apr 29, 2024

Accepted May 6, 2024

Keywords:

Deep learning

Feature extraction

Image classification

Performance matrix

Tamper detection

ABSTRACT

Tamper image detection approach using deep learning involves, creating a model that can accurately identify and localize instances of image tampering, by employing advanced feature extraction methods, object detection algorithms, and optimization techniques that could be manipulated on need basis. Enhance the integrity of visual content by automating the detection of unauthorized alterations, to ensure the reliability of digital images across various applications and domains. The problem addressing the optimization feature extraction techniques involves the detection of subtle manipulations, handling diverse tampering techniques, and achieving robust performance across different types of images and scenarios. The proliferation of sophisticated image editing tools makes it challenging to detect tampered regions within images, necessitating proposed techniques for automated tamper image detection. The research work will focus on four different feature extraction algorithms such as non-negative factorization (NNF), singular value decomposition (SVD), explicit semantic analysis (ESA), principal component analysis (PCA), which are outsourced. Detecting tampered images through deep learning necessitates the meaningful selection and adjustment of several parameters to enhance the model's effectiveness. Integrating the feature extraction algorithm with the suggested methods effectively identifies critical features within the dataset, thereby improving the detection capabilities and achieving higher accuracy.

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



Corresponding Author:

Ramaraj Muniappan

Department of Computer Science, Rathinam College of Arts and Science

Coimbatore-21, Tamilnadu, India

Email: ramaraj.phdcs123@gmail.com

1. INTRODUCTION

Identifying alterations in digital images of post-capture, commonly addressed as the Image Integrity or tampered image detection issue, is a prominent area of study within image processing [1]. This issue holds paramount importance across various sectors like journalism, biometric identification, forensic investigations, legal proceedings, and copyright protection, where confirming the authenticity and unaltered state of digital images is often critical [2]. Fascinated on the enrichment of experimental investigations into algorithms for detecting image tampering, particularly those employing deep learning techniques, is crucial for boosting the reliability and performance of these detection systems [3]. The rapid advancement of image editing software and generative algorithms has made the detection of tampered images increasingly challenging [4]. A variation of

the wavelet transform that uses integers instead of floating-point arithmetic [5]. This choice can be advantageous for digital image processing, as it reduces computational complexity and can avoid rounding errors, making it more suitable for discrete data like digital images. This part suggests that the algorithm incorporates a form of digital signature or authentication mechanism that is encrypted for additional security [6].

It may involve employing the various methods such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), autoencoders, and generative adversarial networks (GANs), among additional techniques [7]. The objective here would be to compare and contrast these methods in terms of effectiveness, efficiency, and areas of application [8]. These might include issues like low detection accuracy in complex images, difficulty in generalizing across different datasets, or the computational inefficiency of existing models [9]. This could involve methods for enhancing edge detection, texture analysis, or color consistency, which are often telltale signs of splicing but can be challenging to detect with standard methods [10]. In contrast to conventional methods of detecting image tampering, which may examine images in segments or depend on extracting features and then classifying them, you only look once (YOLO) simplifies the approach by approaching the detection task as a singular regression challenge. It directly transitions from image pixels to the coordinates of bounding boxes and probabilities of classes [11], [12]. Fast-R-CNN utilizes a CNN to extract features from distinct regions, moving away from the traditional practice of processing each region in isolation. It adopts a collective convolutional feature map for the entire image to decrease redundancy and reduce computational demands [13].

The extracted features that are processed with the multiple fully connected layers, which assess whether each region is tampered or untampered images, while which is fine-tuning the bounding boxes around areas potentially tampered to increase precision [14]-[16]. Fast region-based CNN (fast R-CNN's) processing time and resource requirements are still significant, especially when dealing with high-resolution images or extensive datasets [17]. In this context, the proposed algorithm has utilized to iteratively refine the classification model's ability to distinguish between manipulated and authentic images by fine-tuning the model's parameters [18]. When applying PSO to the problem of identifying tampered images, the algorithm starts with a population (swarm) of candidate solutions (particles), where each particle represents a potential set of parameters for the classification model. These parameters could define features of the image to be analyzed, thresholds for decision-making, or weights within a neural network used for classification [19].

2. REVIEW OF LITERATURE

Recent research has focused on using deep learning classification algorithms for detecting tampered images. This includes CNN, single shot multibox detector (SSD), and YOLO. The efficiency of these methods in recognizing tampered images has been highlighted through their ability to extract features and identify patterns. These models are trained to discern anomalies indicative of image manipulation, with methodologies focusing on optimizing detection accuracy and efficiency by minimizing loss values and simplifying the detection process. Xu *et al.* [20], has leveraged sophisticated advancements in digital image processing and machine learning to enhance the ability to detect manipulated images. A novel approach that combines feature enhancement methods with supervised contrastive learning to identify splicing forgeries, where parts of one image are cut and pasted into another to create a deceptive composite. Raveendra and Nagireddy [21], has demonstrated with the efficacy of an innovative approach combining adaptive segmentation with deep learning networks for the detection and localization of tampering in video content. Solaiyappan and Wen [22], has systematically evaluating a range of models, they have identified specific techniques that offer superior performance in identifying manipulated images, thereby holding significant promise for enhancing the security and reliability of medical imaging data.

Sharma *et al.* [23] in 2023, has introduced an innovative and effective fragile watermarking approach tailored for pinpointing tampering in satellite imagery. Proposed method stands out by offering a high degree of sensitivity to alterations, ensuring that even the subtlest tampering attempts can be accurately detected and localized. Kadha and Das [24] in 2023, unveils a groundbreaking method for identifying the resampling in heavily compressed JPEG images, and utilizing a deep learning model that is specially optimized for reducing block artifacts (BAR). This method marks a significant advancement in digital forensics, addressing the intricate challenge of identifying tampering in images subjected to high levels of compression. Chaitra and Reddy [25] in 2023 has developed a reliable method to detect the numerous copy-move forgeries within images that are making use of a refined pre-trained deep learning model. This optimization has demonstrated substantial improvements in detecting forgeries with high precision and recall rates, thereby contributing to the reliability and trustworthiness of digital media. El_Tokhy [26] in 2023, has proficiently demonstrated the design and deployment of highly precise algorithms for identifying forgeries in digital radiography images, harnessing the strong capabilities of CNNs. Selvan *et al.* 2022 [27], the algorithm was developed through this research exhibit not only high accuracy in forgery detection but also an

impressive ability to localize the alterations within the images, contributing to their practical applicability in clinical and forensic settings.

Jalab *et al.* [28], introduces an innovative algorithm for image enhancement based on the fractional mean of pixels which is specifically designed to markedly enhance the detection of image splicing. The focusing on the nuanced manipulation of pixel values to enhance image features, the algorithm facilitates a more accurate and efficient identification of spliced regions within an image. Shi *et al.* [29] in 2023, has illustrate the fractional mean approach allows for a refined adjustment of pixel intensities, thereby improving the visibility of subtle discrepancies that are indicative of splicing. Nguyen *et al.* [30] in 2022, has comprehensively explored the burgeoning field of deep learning technologies as applied to both the creation and detection of deepfakes. Concurrently, the same technological advances provide a beacon of hope through the development of sophisticated deepfake detection methods that leverage deep learning algorithms to identify and flag manipulated content with increasing accuracy.

3. METHOD

CNNs are central to deep learning for image processing, employing layers that progressively abstract features to recognize complex patterns. Architectural innovations over the years have led to the development of models like YOLO, SSD, and faster R-CNN, each offering different advantages in terms of speed, accuracy, and the ability to detect objects at various scales.

3.1. NMF: non-negative matrix factorization

Utilize non-negative matrix factorization (NMF) as a technique for feature extraction to identify and represent intrinsic patterns, structures, and components within a given dataset. The NMF methods decompose the original non-negative matrix into a set of basis vectors and coefficients, where the basis vectors serve as interpretable features capturing essential characteristics of the data. The (1) is:

$$NMF = X \approx WH \quad (1)$$

NMF aims to factorize a non-negative matrix X into two non-negative matrices W and H matrix W contains the basis vectors (features) that represent the fundamental patterns or shapes present in the image. Matrix H contains the coefficients that indicate how much of each basis vector is present in the original image. Each row of H corresponds to a different region of the image, and the elements are non-negative.

3.2. SVD: singular value decomposition

Singular value decomposition (SVD) techniques as a feature extraction method to enhance tampered prediction in digital images. This technique is to decompose image matrices using SVD, extracting singular vectors and values to identify key patterns and features indicative of both authentic and potentially tampered regions. The (2) and (3) is:

$$X = U\Sigma V^T \quad (2)$$

where U and V is denoting the orthogonal matrices, with Σ is being a diagonal matrix comprised of the singular values.

$$X_k = (U_k, \varepsilon_k, V_k^T) \quad (3)$$

The reconstructed matrix X_k approximates the original data using the retained features. Retain only the top k singular values and their corresponding columns in U and V . This reduces the rank of the matrix and achieves dimensionality reduction. SVD is used to decompose the input matrix X , and only the top k singular values and vectors are retained for reconstruction. The resulting matrix $X_{reconstructedk}$ approximates the original data using the most significant features.

3.3. ESA: explicit semantic analysis

Explicit semantic analysis (ESA) techniques for feature extraction with the aim of capturing and representing the semantic content inherent in textual data. Even through ESA is to transform textual descriptions into a high-dimensional semantic space, capturing the underlying semantics of the associated images. Let I be the image matrix, T be the textual metadata vector, and F be the combined feature vector. W_t and W_v are weight matrices for the textual and visual features, respectively. The following (4) and (5) is:

$$T = ESA(D), \text{ and } F = [W_t \cdot T, W_v \cdot V] \quad (4)$$

$$V = ImageFeatureExtraction(I), \text{ and } Prediction = Classifier(F) \quad (5)$$

where D is the set of textual descriptions associated with the images. Using a suitable image processing or deep learning approach. Concatenate the weighted textual and visual features into a single vector. Use a classifier (e.g., a machine learning model) to predict whether the image is tampered based on the combined feature vector. Here, F represents vector multiplication or concatenation, depending on the context. The weights W_t and W_v can be adjusted during training to give appropriate importance to textual and visual features.

3.4. Fast R-CNN method

Fast R-CNN signifies considerable advancements in the realm of object detection and has been customized for a variety of applications, including the detection of image tampering using deep learning techniques. Fast R-CNN builds upon the ideas introduced by R-CNN and improves upon it in both speed and accuracy. For tampered image detection, fast R-CNN is adapted to identify areas within an image that may have been altered, leveraging its object detection capabilities to focus on irregularities that suggest manipulation. The (6), (7), and (8) is:

$$F = f(I * K + b) \quad (6)$$

where I stand for the input image or the feature map received from the preceding layer, K is the kernel or filter used on the image, $*$ symbolizes the convolution process, b refers to the bias term that is incorporated with the output of the convolution, f represents a non-linear activation function (e.g., rectified linear unit (ReLU)), and F denotes the resulting feature map. The outcome of the region of interest (RoI) pooling layer for a specific region R_i can be depicted as:

$$P_i = pool(F/R_i) \quad (7)$$

$$V_i = f(w \cdot P_i + b) \quad (8)$$

Where F/R_i denotes the portion of the feature map F corresponding to the region R_i and pool node of (\cdot) is represents the pooling operation (usually max pooling) applied to resize the features within R_i to a fixed size (e.g., 7×7). The RoI pooling layer takes the feature map F and a set of N proposed regions R_1, R_2, \dots, R_n (generated by a region proposal algorithm) as inputs. Each region R_i is defined by a four-tuple (x_i, y_i, w_i, h_i) representing the top-left corner coordinates (x_i, y_i) and the width w_i and height h_i of the region. After RoI pooling, each fixed-size feature vector P_i is passed through one or more fully connected (FC) layers to generate a feature vector V_i for each region is denoted by (7). When (8), W and b are the weights and biases of the FC layer, f is a non-linear activation function, V_i is the output feature vector for region R_i .

3.5. Enhanced YOLO algorithm

The enhanced YOLO algorithm represents an advanced iteration of the original YOLO, a groundbreaking deep learning model for real-time object detection. YOLO fundamentally treats object detection as a unified regression challenge, which is directly deriving bounding boxes and class probabilities from entire images in a single assessment. At the heart of YOLO's feature extraction are CNNs. The mathematical operation performed by a convolutional layer on the input image can be represented as follows on the (9) is:

$$F_{ij}^{(l)} = \mu \left(\varepsilon_m \varepsilon_n K_{mn}^{(l)} \cdot I_{(i+m)(j+n)}^{(l-1)} + b^{(l)} \right) \quad (9)$$

where: $F_{ij}^{(l)}$ is the feature map produced by the convolutional layer (l) at position (i, j) . σ represents a non-linear activation function, such as ReLU. $K_{mn}^{(l)}$ is the kernel or filter applied at position (m, n) in layer (l) . $I_{(i+m)(j+n)}^{(l-1)}$ is the input to layer (l) , which can be the original image or the output of the previous layer. $b^{(l)}$ is the bias term for the convolutional layer (l) .

3.6. Batch normalization and activation functions

Following convolution, batch normalization and activation functions are applied to stabilize and accelerate training, as well as to introduce non-linearities into the model. Batch normalization can be represented as:

$$x^{(k)} = \frac{x^{(k)} - \mu_\beta}{\sqrt{\sigma_\beta^2 + \epsilon}} \tag{10}$$

$$y^{(k)} = \gamma x^{(k)} + \beta \tag{11}$$

where $x^{(k)}$ is the input to the batch normalization layer for feature (k) . μ_β and σ_β^2 are the mean and variance of the batch, respectively. ϵ is a small constant added for numerical stability. $\gamma x^{(k)}$ and β are parameters to be learned, representing scale and shift. $y^{(k)}$ is the normalized and scaled output.

3.7. Improved feature extraction in enhanced YOLO

Enhanced YOLO versions may incorporate deeper or more sophisticated architectures, such as Darknet-53 used in YOLOv3, or borrow concepts from architectures like ResNet (with residual connections to facilitate training of deeper networks). For example, a residual block's operation can be summarized as:

$$F(x) = \sigma(k_2 * \sigma(x + b_1) + b_2) + x \tag{12}$$

where $F(x)$ is the output of the residual block. k_2 and k_1 are kernels for the two convolutional layers in the block. b_1 and b_2 are biases for the two convolutional layers. x is the input to the residual block. σ is the activation function. When adapted for detecting tampered images, the enhanced YOLO algorithm leverages this efficiency and introduces improvements in accuracy, sensitivity to small and challenging objects (which can include subtle tampered areas), and general robustness. The class probabilities indicate the presence of objects within those boxes.

4. RESULT AND DISCUSSION

4.1. Accuracy

It is considered as the basic metric and the most important metric to evaluate the algorithms. Accuracy is referred as the close value of the measurement to a standard value. Accuracy is assessed by evaluating the quantity of correct predictions relative to the total number of predictions or by calculating the ratio of accurate predictions to the dataset's magnitude.

$$Accuracy = \frac{\text{Number of Correct Predictions}}{\text{All of the Predictions}} \tag{13}$$

4.2. Precision

Precision is vital for securing accurate results, particularly when sample data which is integrated into real-world datasets and it is small errors have the potential to escalate into larger issues under certain circumstances. In such scenarios, precision proves to be key in addressing these challenges. At its core, precision is defined as the proportion of relevant instances out of all instances that have been retrieved.

$$Precision = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}} \text{ or } Precision = \frac{\text{True Positive}}{\text{Total Predicted values}} \tag{14}$$

4.3. Recall

Recall is a measure of number of positive cases the classifier correctly predicted, over all the positive cases. It is also known as sensitivity. It is calculated by finding the number of correctly predicted positive instances over the number of total positive instances in the data set. Recall is considered as the best metric for the best model when there is a high cost associated with false negatives.

$$Recall = \frac{\text{True Positive}}{\text{True Positive} + \text{False Negative}} \text{ or } Recall = \frac{\text{True Positive}}{\text{Total Actual values}} \tag{15}$$

4.4. Percentage of tampering

The original image x and the forged image y are compared using structural dissimilarity and the percentage obtained is taken for finding out the tampering percentage.

$$TP = \frac{(2\mu_x\mu_y+C1)(2\sigma_{xy}+C2)}{(\mu_x^2+\mu_y^2+C1)(\sigma_x^2+\sigma_y^2+C2)} \tag{16}$$

Where μ_x is the average of x is, μ_y is the average of y, σ_x^2 is the variance of x, σ_y^2 is the variance of y, σ_{xy} is the co-variance of x and y. $C1=(K_1L)^2$ and $C2=(K_2L)^2$ are the two variables to stabilize the division with weak denominator where L is the dynamic range of the pixel values and $K1=0.01$, $K2=0.03$ by default.

Figure 1 shows various images that have been manipulated. These images feature realistic forgeries created through a mix of techniques such as resampling, smoothing, splicing, and other forms of alteration. The primary objective of the proposed study is to determine the specific manipulations applied, thereby classifying images as either tampered or original. Several methods exist for detecting tampered or altered images, including analyzing the edges, inspecting shadows, identifying missing reflections, and searching for evidence of cloning, among others. Context-based methods for detecting image tampering have been applied to the images shown in Figure 1.

Table 1 illustrates the feature extraction points obtained by applying various algorithms-NNF, SVD, ESA, and a proposed algorithm-to all the input images shown in Figure 1. Among these, ESA recognized for its robustness and ability to detect and describe features in a low-dimensional space. The data reveals that the proposed algorithm outperforms the others, including an enhanced YOLO algorithm, by achieving the highest number of feature extraction points, recorded at 167. Conversely, NNF is identified as the algorithm with the lowest performance in this metric, with its feature extraction points calculated at 130.

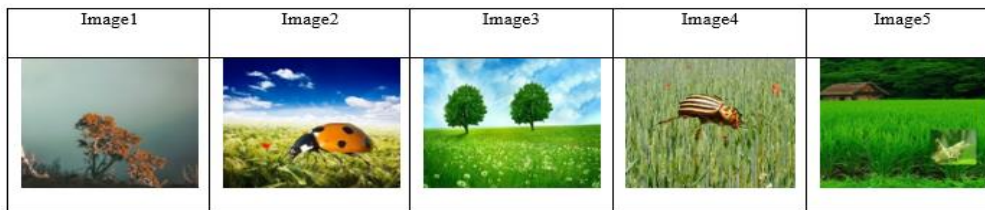


Figure 1. Input image

Table 1. Feature extraction points

Algorithm	Feature extraction points
NNF	130
SVD	156
ESA	173
Proposed	167

The illustration in the preceding Figure 2 represents the process of detecting and extracting features from an image. Within computational methods, YOLO employed as a stochastic optimization algorithm for selecting the features and classifying them. It involves the iterative identification of the most relevant and beneficial feature set to either enhance or sustain performance in classification tasks. Furthermore, the Table 1 indicates that the proposed algorithm, when optimized with particle swarm optimization (PSO), delivers superior outcomes in comparison to all other evaluated algorithms.

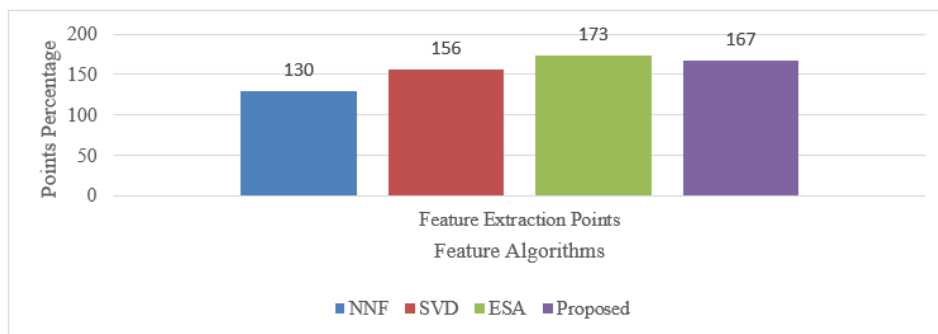


Figure 2. Feature extraction points detection

Table 2 presents the feature extraction points yielded by several algorithms ENNF, ESVD, EESA, and EYOLO when applied to the input images depicted in Figure 1. EESA is highlighted as an effective and efficient feature detector and descriptor, characterized by its minimal dimensionality. The data further demonstrates that the proposed algorithm surpasses the performance of existing algorithms like NNF, SVD, ESA, and YOLO by achieving the highest number of feature extraction points, marked at 183. In contrast, NNF shows to generate the lowest feature extraction points, with its count determined to be 125.

Table 2. Extracted the feature points with PSO

Algorithm	Feature extraction points
Enhanced NNF	125
Enhanced SVD	140
Enhanced ESA	165
Enhanced PSO	159
EYOLO	183

Figure 3 demonstrates the identified forgery areas within an image, a result produced by a forgery region extraction algorithm. This illustration reveals that the NNF algorithm's performance is inferior compared to both SVD and ESA. Moreover, it indicated that the proposed YOLO algorithm outshines its counterparts in efficacy. The enhanced YOLO detector has been utilized to identify significant keypoints across both smooth and textured areas of the image. The process involves the detection of potential duplicate regions in test images through the comparison of descriptor vectors. Key points marked in Figure 2 that are indicative of areas suspected to be inauthentic or altered from the original image content. These tampered areas are highlighted in green, facilitating a clearer understanding and identification of the alterations. Experimental results, encompassing various images with tampering of random sizes and locations, demonstrate that the method for image verification and tampering localization offers superior performance over contemporary techniques, even when subjected to diverse forms of attacks.

The Ensemble classifier works to reduce both bias and variance, which enhances the models' accuracy. The data presented in the preceding table confirms that the developed EYOLO (enhanced you only look once) model achieves higher tampering detection rates, recording percentages of 4.9, 7.69, 7.98, 3.8, and 7.12 for input images 1, 2, 3, 4, and 5, respectively. Additionally, the precision, accuracy, recall, and computation time have been measured, with the findings documented in Table 3.

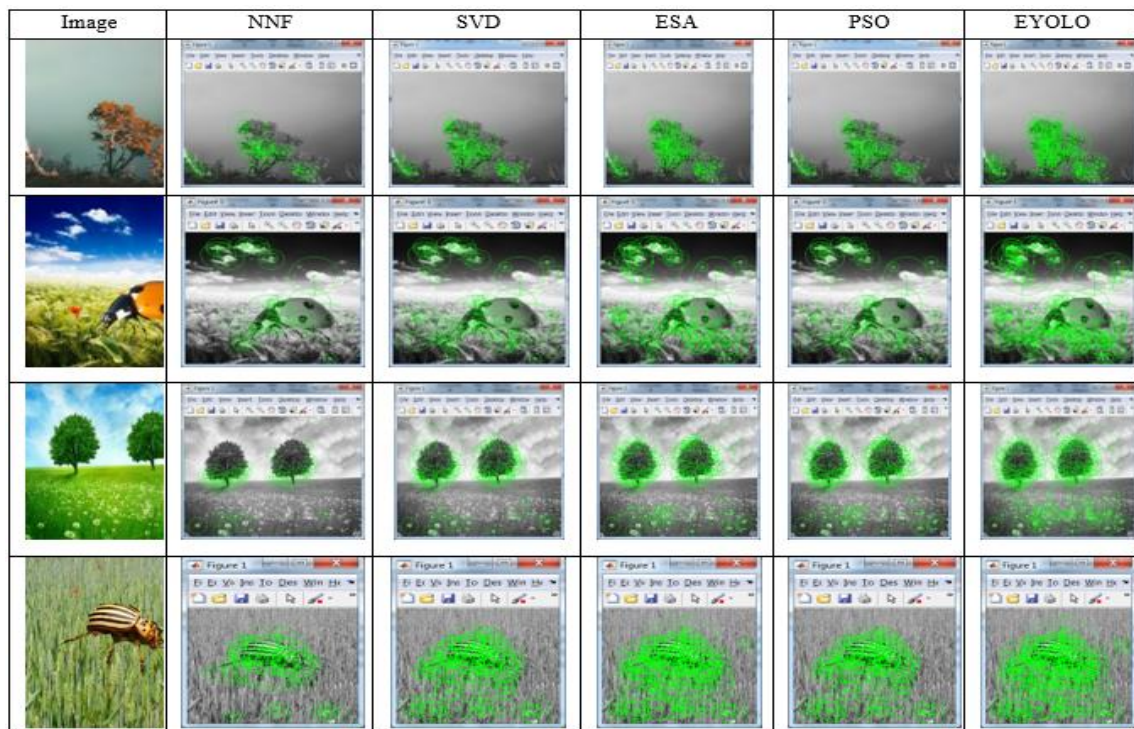


Figure 3. Tampered output images

Table 3. Performance of ensemble classifier

Algorithm	Accuracy	Precision	Recall	Time	Percentage of tampering
ENNF	85	84	85	6.14	4.9
ESVD	86	85	86	5.9	7.69
EESA	87	86	87	5.8	7.98
EPSO	87	86	87	5.6	3.8
EYOLO	88	87	88	5.3	7.12

The Figure 4 is describing a scenario where an ensemble classifier algorithm is applied to detect tampering in an image, possibly for the purpose of digital image forensics. Typically, an ensemble classifier enhances the detection process's accuracy and robustness by amalgamating the outputs from various classification models. The use of the same parameter across different instances or features of the image could refer to the consistent application of the ensemble classifier's criteria or settings in evaluating the image for tampering evidence.

The Table 4 illustrates the classification using fast RCNN classifier. The accuracy, precision, recall and time are calculated. The fast RCNN has an ability to generate complex decision boundaries in the feature space. Table 4 demonstrates that EYOLO exhibits superior tampering detection percentages in comparison to other algorithms. The tampering percentages for images 1, 2, 3, 4, and 5 are recorded at 3.2, 4.69, 4.51, 5.4, and 5.14, respectively.

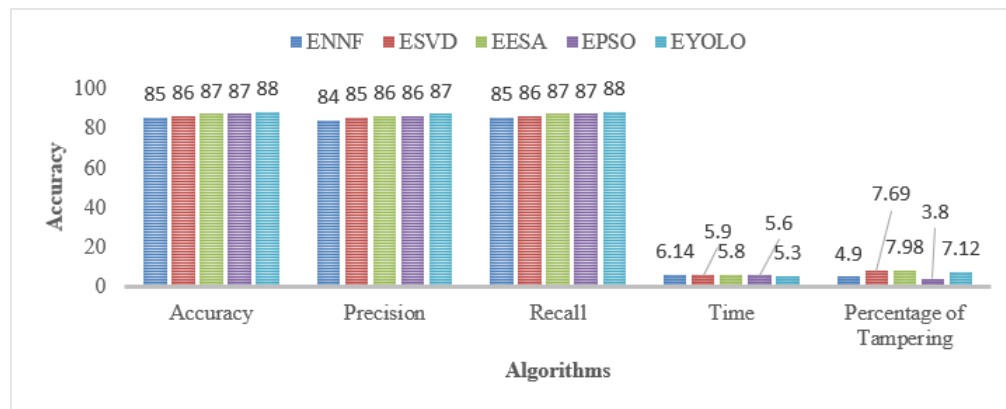


Figure 4. Ensemble classifier algorithm applied on tampered image

Table 4. Performance of fast RCNN classifier

Algorithm	Accuracy	Precision	Recall	Time	Percentage of tampering
ENNF	91	90	91	3.9	3.2
ESVD	92	91	92	3.5	4.69
EESA	93	92	93	3	4.51
EPSO	97	96	97	2.1	5.4
EYOLO	94	93	94	2.14	5.14

Figure 5 likely illustrates the application of the Fast R-CNN classification algorithm on a tampered image, emphasizing its performance across various metrics such as accuracy, time, precision, recall, and additional measures. This visualization serves to showcase the efficacy of fast R-CNN in the domain of digital image forensics, specifically in detecting and classifying tampered regions within images.

The Table 5 illustrates the classification performance using the YOLO classifier. The enhanced classifier's capability to identify tampered areas in the input images is superior, as evidenced by the highest tampering percentages among all proposed methods. Thus, the proposed EYOLO method which is identified as the most effective, especially when compared to methods evaluated with the YOLO classifier. The subsequent figure visualizes the performance comparison of the proposed algorithms using Ensemble, Fast RCNN, and YOLO classifiers, indicating that the YOLO classifier exhibits the most effective tampering detection rate among the classifiers compared.

Figure 6 illustrates the application of an enhanced YOLO classification algorithm on a tampered image, evaluated based on several key performance metrics: accuracy, time, precision, recall, and an additional commentary. The enhanced YOLO algorithm, renowned for its real-time object detection

capabilities, has been further optimized in this scenario to identify and classify tampered areas within images. The improvements aim to bolster the algorithm's sensitivity to irregularities that signify tampering, thereby enhancing its forensic utility.

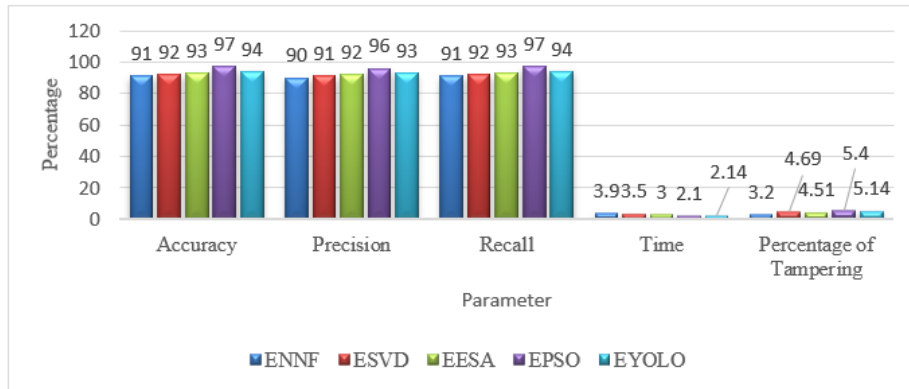


Figure 5. Fast R-CNN classification algorithm applied on tampered image

Table 5. Illustrate on the EYOLO classifier

Algorithm	Accuracy	Precision	Recall	Time	Percentage of tampering
ENNF	94	93	94	3.43	4.2
ESVD	96	95	96	3.1	4.9
EESA	97	96	97	2.46	5.48
EPSO	99	98	99	2.13	2.98
EYOLO	99	98	99	1.9	5.7

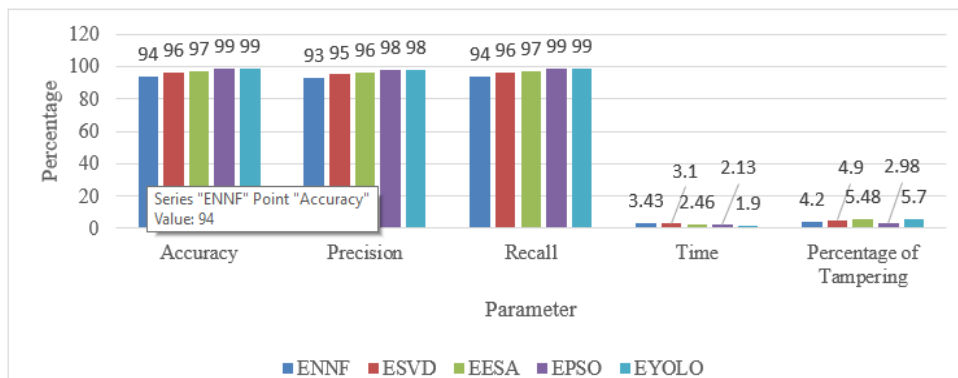


Figure 6. Enhanced YOLO classifier algorithm applied on tampered image




5. CONCLUSION

This paper proposes an automated optimizing feature extraction for tampering image detection using deep learning approaches that has proven to be a significant stride in ensuring the integrity and authenticity of digital images. Employing state-of-the-art deep learning strategies, such as enhanced CNNs, has enabled many researchers to attain the unparalleled accuracy in detecting content alterations. The integration of sophisticated feature extraction techniques has enhanced the models' sensitivity to subtle discrepancies that distinguish tampered images from authentic ones. This progress not only bolsters the reliability of digital media in various applications from the legal proceedings to journalism and beyond-but also sets a foundation for future advancements in the field. As proposed deep erudition knowledge which continues to progress, and further refinements in feature extraction methods are anticipated, promising even greater efficiency and accuracy in detecting image tampering. The ongoing collaboration between technological innovation and domain-specific expertise is key to navigating the challenges posed by increasingly sophisticated manipulation techniques, thereby safeguarding the trustworthiness of digital imagery in an era where visual content plays a crucial role in communication and information dissemination.




REFERENCES

- [1] R. Gupta, V. Anand, S. Gupta, and D. Koundal, "Deep learning model for defect analysis in industry using casting images," *Expert Systems with Applications*, vol. 232, p. 120758, Dec. 2023, doi: 10.1016/j.eswa.2023.120758.
- [2] V. Kadha, V. V. N. J. S. L. Nandikattu, S. Bakshi, and S. K. Das, "Forensic analysis of manipulation chains: a deep residual network for detecting JPEG-manipulation-JPEG," *Forensic Science International: Digital Investigation*, vol. 47, p. 301623, Dec. 2023, doi: 10.1016/j.fsidi.2023.301623.
- [3] A. Heidari, D. Javaheri, S. Toumaj, N. J. Navimipour, M. Rezaei, and M. Unal, "A new lung cancer detection method based on the chest CT images using Federated Learning and blockchain systems," *Artificial Intelligence in Medicine*, vol. 141, p. 102572, Jul. 2023, doi: 10.1016/j.artmed.2023.102572.
- [4] P. Heiselberg, K. Sørensen, and H. Heiselberg, "Ship velocity estimation in SAR images using multitask deep learning," *Remote Sensing of Environment*, vol. 288, p. 113492, Apr. 2023, doi: 10.1016/j.rse.2023.113492.
- [5] I. Hussain, S. Tan, B. Li, X. Qin, D. Hussain, and J. Huang, "A novel deep learning framework for double JPEG compression detection of small size blocks," *Journal of Visual Communication and Image Representation*, vol. 80, p. 103269, Oct. 2021, doi: 10.1016/j.jvcir.2021.103269.
- [6] Y. Zhao, J. Zhang, and Y. Cao, "Manipulating vulnerability: Poisoning attacks and countermeasures in federated cloud-edge-client learning for image classification," *Knowledge-Based Systems*, vol. 259, p. 110072, Jan. 2023, doi: 10.1016/j.knsys.2022.110072.
- [7] M. R. Abbasniya, S. A. Sheikholeslamzadeh, H. Nasiri, and S. Emami, "Classification of breast tumors based on histopathology images using deep features and ensemble of gradient boosting methods," *Computers and Electrical Engineering*, vol. 103, p. 108382, Oct. 2022, doi: 10.1016/j.compeleceng.2022.108382.
- [8] Y. Zhang, F. Ding, S. Kwong, and G. Zhu, "Feature pyramid network for diffusion-based image inpainting detection," *Information Sciences*, vol. 572, pp. 29–42, Sep. 2021, doi: 10.1016/j.ins.2021.04.042.
- [9] A. I. Muhammad, R. Singh, and Y. Ibrahim, "Face recognition with particle swarm optimization (PSO) and support vector machine (SVM)," 2020.
- [10] M. Ramaraj, D. Sabareeswaran, V. Vijayalaksmi, C. Jothish, N. Thangarasu, and G. Manivasagam, "Sophisticated CPBIS methods applied for FBISODATA clustering algorithm using with real time image database," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 30, no. 1, pp. 614–624, Apr. 2023, doi: 10.11591/ijeecs.v30.i1.pp614-624.
- [11] A. J. Oliveira, B. M. Ferreira, and N. A. Cruz, "A performance analysis of feature extraction algorithms for acoustic image-based underwater navigation," *Journal of Marine Science and Engineering*, vol. 9, no. 4, 2021, doi: 10.3390/jmse9040361.
- [12] C. Tchito Tchagpa *et al.*, "Biomedical image classification in a big data architecture using machine learning algorithms," *Journal of Healthcare Engineering*, vol. 2021, 2021, doi: 10.1155/2021/9998819.
- [13] G. Hermosilla *et al.*, "Particle swarm optimization for the fusion of thermal and visible descriptors in face recognition systems," *IEEE Access*, vol. 6, pp. 42800–42811, 2018, doi: 10.1109/ACCESS.2018.2850281.
- [14] N. S. B. M. Said, H. Madzin, S. K. Ali, and N. S. Beng, "Comparison of color-based feature extraction methods in banana leaf diseases classification using SVM and K-NN," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 24, no. 3, pp. 1523–1533, 2021, doi: 10.11591/ijeecs.v24.i3.pp1523-1533.
- [15] P. N. Huu and T. P. Ngoc, "Hand gesture recognition algorithm using SVM and HOG model for control of robotic system," *Journal of Robotics*, vol. 2021, 2021, doi: 10.1155/2021/3986497.
- [16] R. Agarwal and M. Pant, "Image tampering detection using genetic algorithm," *MATEC Web of Conferences*, vol. 277, p. 02026, 2019, doi: 10.1051/mateconf/201927702026.
- [17] S. Ahmed, M. Frikha, T. D. H. Hussein, and J. Rahebi, "Optimum feature selection with particle swarm optimization to face recognition system using gabor wavelet transform and deep learning," *BioMed Research International*, vol. 2021, 2021, doi: 10.1155/2021/6621540.
- [18] 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.
- [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*, vol. 2021, 2021, doi: 10.1155/2021/9989237.
- [20] Y. Xu, J. Zheng, A. Fang, and M. Irfan, "Feature enhancement and supervised contrastive learning for image splicing forgery detection," *Digital Signal Processing*, vol. 136, p. 104005, May 2023, doi: 10.1016/j.dsp.2023.104005.
- [21] M. Raveendra and K. Nagireddy, "Tamper video detection and localization using an adaptive segmentation and deep network technique," *Journal of Visual Communication and Image Representation*, vol. 82, p. 103401, Jan. 2022, doi: 10.1016/j.jvcir.2021.103401.
- [22] S. Solaiyappan and Y. Wen, "Machine learning based medical image deepfake detection: a comparative study," *Machine Learning with Applications*, vol. 8, p. 100298, Jun. 2022, doi: 10.1016/j.mlwa.2022.100298.
- [23] S. Sharma, S. Shivani, and N. Saxena, "An efficient fragile watermarking scheme for tamper localization in satellite images," *Computers and Electrical Engineering*, vol. 109, p. 108783, Aug. 2023, doi: 10.1016/j.compeleceng.2023.108783.
- [24] V. Kadha and S. K. Das, "A novel method for resampling detection in highly compressed JPEG images through BAR using a deep learning technique," *Optik*, vol. 291, p. 171356, Nov. 2023, doi: 10.1016/j.ijleo.2023.171356.
- [25] B. Chaitra and P. V. Bhaskar Reddy, "An approach for copy-move image multiple forgery detection based on an optimized pre-trained deep learning model," *Knowledge-Based Systems*, vol. 269, p. 110508, Jun. 2023, doi: 10.1016/j.knsys.2023.110508.
- [26] M. S. El Tokhy, "Development of precise forgery detection algorithms in digital radiography images using convolution neural network," *Applied Soft Computing*, vol. 138, p. 110174, May 2023, doi: 10.1016/j.asoc.2023.110174.
- [27] G. Emil Selvan, M. Azees, C. Rayala Vinodkumar, and G. Parthasarathy, "Hybrid optimization enabled deep learning technique for multi-level intrusion detection," *Advances in Engineering Software*, vol. 173, p. 103197, Nov. 2022, doi: 10.1016/j.advengsoft.2022.103197.
- [28] H. A. Jalab, M. A. Alqarni, R. W. Ibrahim, and A. Ali Almazroi, "A novel pixel's fractional mean-based image enhancement algorithm for better image splicing detection," *Journal of King Saud University - Science*, vol. 34, no. 2, p. 101805, Feb. 2022, doi: 10.1016/j.jksus.2021.101805.
- [29] Z. Shi, X. Shen, H. Chen, and Y. Lyu, "PL-GNet: pixel level global network for detection and localization of image forgeries," *Signal Processing: Image Communication*, vol. 119, p. 117029, Nov. 2023, doi: 10.1016/j.image.2023.117029.
- [30] T. T. Nguyen *et al.*, "Deep learning for deepfakes creation and detection: a survey," *Computer Vision and Image Understanding*, vol. 223, p. 103525, Oct. 2022, doi: 10.1016/j.cviu.2022.103525.




BIOGRAPHIES OF AUTHORS

Dr. Ramaraj Muniappan    is working as an Assistant Professor in the Department of Computer Science at Rathinam College of Arts and Science, Coimbatore. He holds a Ph.D., degree in Computer Science at Bharathiar University in the year of 2020 with specialization in data mining with image process and also fuzzy logic in the image analysis. His research areas are data mining, image processing, fuzzy logic, pattern recognition, and deep learning concept. He has published more research article in the reputed various national and international journals and also filed the patents in the same field. He has a reviewer of many international journals including with IEEE, ASTESJ, and JERS. He can be contacted at email: ramaraj.phdcs@gmail.com or ramaraj.phdcs123@gmail.com.






Dr. Dhendapani Sabareeswaran    is working as an Assistant Professor in the Department of Computer Science at Government Arts and Science for Women, Tiruppur. He holds a Ph.D., degree in Computer Science at Karpagam Academy of Higher Education in the year of 2020 with specialization in data mining. His research areas are data mining, image processing, fuzzy logic, and pattern recognition. He has published more research article in the reputed various national and international journals and also filed the patents in the same field. He can be contacted at email: sabaredhandapani@gmail.com.






Dr. Chembath Jothish    completed his Ph.D. from Karpagam deemed to be University, Coimbatore, Tamilnadu in the year 2020, under the title “Next web page prediction using enhanced preprocessing and ensemble clustering based hybrid markov model using web log data”. More than 15 research journals have been published in reputed journals which are either Scopus indexed, Web of Science and international journals of repute, which would help the Internet mechanism to predict the user’s intention and interest, when internet is browsed using mathematical model algorithms after cleaning the internet data, thereby giving accurate predictions using mathematical models. Author also has attended 3 international conferences held in the Sultanate of Oman, Malaysia and Cochin. Currently author is working in Presidency University, Bengaluru. The teaching and research experience is around two decades starting from 2003 to toll date. He can be contacted at email: jothishchembath12@gmail.com.






Dr. Joe Arun Raja    received the M. Tech., degree and Ph.D. degree in Computer and Information Technology from Manonmaniam Sundaranar University. He has 17 years of teaching experience in Computer Science Department. He is currently working an Associate Professor in School of Information Science, Presidency University. He has published four international conference and eight journal papers. His research interests include machine learning, medical informatics, and GIS. He can be contacted at email: joearunraja@gmail.com.






Dr. Srividhya Selvaraj    is working as an Associate Professor in the Department of Computer Science at KPR College of Arts Science an Research, Coimbatore. She has more than a decade of teaching experience in different verticals. She is a reviewer in various international journals and life-time member in IAENG. Her research area includes data mining, machine learning, and deep learning. She has about 10+ research papers published in national and international journals. She also presented more than 15 papers in national and international conferences and also published many books. She can be contacted at email: vidhyasai14@gmail.com.






Dr. Thangarasu Nainan    is currently working as an assistant professor in the Department of Computer Science, at Karpagam Academy of Higher Education, Coimbatore. He is greatly fascinated with the advanced computing technology and research programs is cluster computing, cryptography and network security, cloud computing, artificial intelligent system, information security in large database, and data mining as well as the strong teaching experience. His doctoral dissertation also focuses on advanced security systems with cloud computing, and he have published more than 13 publications in reputed journals, which he find would be a great addition to the success of your teaching and research department. He can be contacted at email: drthangarasu.n@kahedu.edu.in.



Mr. Bhaarithi Ilango    is working as an Assistant Professor in the Department of Computer Science at Rathinam College of Arts and Science, Coimbatore. He holds a NET. Qualification in computer science at NTA in the year of 2023 with specialization in data mining with image process and also fuzzy logic in the image analysis. His research areas are data mining, in the various fields. He has published more research article in the reputed various national and international journals and also filed the patents in the same field. He can be contacted at email id: bhaarithi.cs@rathinam.in.



Dr. Dhinakaran Subramanian    MCA., M.Phil., Ph.D., Controller of Examinations and Associate Professor in Computer Science, Rathinam College of Arts and Science (Autonomous), Coimbatore – 641021, Tamil Nadu, India. He has sixteen years of dedicated teaching experience to excel in his field of research work. He has written several research articles in international, peer reviewed, and Scopus Indexed journals. He published in reputed national and international journals in different pasture of research. He has presented papers at various national level and international level conferences. He is also acting as subject expert of the Board of Studies for various leading Autonomous Colleges. He has written in six books. He is also acting as an Subject expert of the Board of Studies for Bharathiar University. He is a former Senate Member of Bharathiar University. He can be contacted at email: dhinakaran.cs@gmail.com.