IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 31 July 2024, accepted 26 August 2024, date of publication 30 August 2024, date of current version 10 September 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3452609

RESEARCH ARTICLE

Copy-Move Forgery Detection Technique Using Graph Convolutional Networks Feature Extraction

VARUN SHINDE[1], (Member, IEEE), VINEET DHANAWAT[2], (Member, IEEE), AHMAD ALMOGREN[3], (Senior Member, IEEE), ANJANAVA BISWAS[4], MUHAMMAD BILAL[5], RIZWAN ALI NAQVI[6], AND ATEEQ UR REHMAN[7], (Senior Member, IEEE)

[1]Cloudera Inc., Austin, TX 78701, USA
[2]Meta Platforms Inc., Menlo Park, CA 94025, USA
[3]Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11633, Saudi Arabia
[4]AWS AI & Machine Learning, San Diego, CA 92129, USA
[5]Department of Computer Engineering, HITEC University, Taxila 47040, Pakistan
[6]Department of AI and Robotics, Sejong University, Seoul 05006, Republic of Korea
[7]School of Computing, Gachon University, Seongnam 13120, Republic of Korea

Corresponding authors: Ateeq Ur Rehman (202411144@gachon.ac.kr) and Rizwan Ali Naqvi (rizwanali@sejong.ac.kr)

This work was supported by King Saud University, Riyadh, Saudi Arabia, through Researchers Supporting Project number (RSP2024R184).

ABSTRACT In the development of image forensics, detection of Copy-Move Forgery (CMF) has become a major challenge due to the proliferation of image forgery techniques. The CMF is widely utilized to alter the content of the original image to spread false information or to use such forged digital images for illegal purposes e.g. false evidence in the court of law, or to blackmailing any individual. This paper presents a new method for CMF Detection (CMFD) that uses the power of Graph Convolution Networks (GCNs) and its multiple layers with ReLU activation, for CMFD and analysis. The aim to use GCN is due to its ability to improve the feature extraction process by utilizing the spatial and structural affiliation between elements in the digital images. Also, the GCN aims to store information about images and use it to graphically describe images with pixels or image areas as features, spatial and correlation relationships as edges. By pulling data from this image, GCN is able to obtain content rich features that are very powerful at detecting CMF regions. In proposed methodology, we utilized Support Vector machine (SVM) for classification and the binary cross-entropy loss, and the Adam optimizer for improving accuracy. Our scheme successfully achieves high accuracy and is effective in CMFD. We use the MICC F220, and CoMoFoD datasets to test the GCN in our proposed CMFD method. Through much testing and evaluation, we have found that GCN has the tremendous ability for CMFD in digital images in term of accuracy.

INDEX TERMS CMFD, forensic science, feature extraction, GCN.

I. INTRODUCTION

In today's progressed age, the ease of CMF images utilizing advanced computer program instruments has given rise to an extraordinary concern. Among various types of image manipulations, CMF is a prevalent technique, but it often results in questionable or suspicious enhancements in the image's appearance [1]. In CMF method, an area of a picture is unlawfully reproduced and stuck someplace else in the same picture, making replicated or cloned locale as showed up in Figure 1. This bewildering act can have genuine consequences, which causes the spread of beguiling data and the compromise of picture realness. In this way, the change of compelling and strong CMFD methodologies is fundamental [2].

Traditional techniques for CMFD have typically relied on handmade features and block-based inspection, which may not fully capture the subtle relationships between image areas [3]. To effectively detect CMF regions in the digital images it is pertinent to extract meaningful features from the digital images [4]. The neural network can be utilized to detect the CMF regions more accurately [5], [6]. To solve

The associate editor coordinating the review of this manuscript and approving it for publication was Donato Impedovo.

(a) (b)

FIGURE 1. (a) Original image, (b) CMF tampered image.

this issue and increase CMFD accuracy, we suggest a unique technique that takes the advantage of GCNs' superior feature extraction capability.

GCNs have picked up conspicuousness in later a long time due to their capacity to demonstrate complex connections and conditions inside graph-structured data. In the context of computerized image forensics, an image can be conceptualized as a graph, with pixels or image regions as hubs and spatial or relevant connections as edges. GCNs, designed to proliferate data over graph hubs, offer a promising arrangement to capture the intricate designs and conditions that develop in images.

This paper presents a novel technique for CMFD utilizing GCNs as the foundation of our feature extraction process. By representing an image as a graph and utilizing GCNs to learn feature representations, we point to distinguish CMF's with upgraded accuracy and robustness. The proposed strategy envelops the following key steps:

A. GRAPH CONSTRUCTION

We amend the picture into a graph representation, where center points compare to individual picture components, and edges imply associations between them. This graph epitomizes both spatial and relevant information, allowing us to capture the essential structure of the image.

B. FEATURE EXTRACTION WITH GCN'S

The heart of our approach lies in utilization of GCNs to remove imperative include representations from the graph. By causing data over centers, GCNs capture complicated regions, spatial conditions, and significant nuances, in this way upgrading the include space.

C. FORGERY DETECTION

Our preliminary outcomes is that the proposed technique holds ensure in basically upgrading the exactness and strength of CMFD in digital pictures. By saddling the capabilities of GCNs, we point to provide an arrangement that can effectively combat the creating challenges posed by picture imitations in today's progressed landscape.

We jump into the points of interest of our technique, display test comes about, and look at the proposals and future bearings of this explore in the field of advanced image forensics.

II. OUR CONTRIBUTIONS

In the proposed technique for CMFD utilizing GCNs, a few commitments can be highlighted to illustrate the novel perspectives and advancements over existing strategies. Here is a point by point portrayal of these contributions:

- Introduction of GCN for Image Forensics: The proposed technique leverages GCNs to identify CMF in digital pictures. This approach is novel in the setting of image forensics, where GCNs are utilized to demonstrate and handle the connections between picture regions as a graph structure, capturing perplexing nearby and worldwide dependencies.
- Feature Extraction and Graph Development: The GCN converts the image into graph structure by using the pixels as nodes and similarity as edges. The convolutions layers applied to make the model learn new feature representations. The GCN model provides content rich features from input image.
- Handling Complex Forged Region: By modeling the issue as a graph, the proposed strategy can way better handle complex imitation designs, such as non-contiguous or sporadically molded copied locales. Conventional strategies may battle with these designs, but the GCN's capacity to learn from the graph structure permits it to successfully distinguish and separate between true and copied regions.
- End-to-End Learning System: The proposed GCN-based approach gives an end-to-end learning system for CMFD. This contrasts with conventional strategies that

regularly require isolated steps for highlight extraction, coordinating, and classification. The GCN show coordinating these steps into a cohesive handle, learning straightforwardly from the crude picture information to the last location of forgeries.

- Improved Detection Execution: Exploratory comes about illustrate that the GCN-based approach accomplishes higher precision and strength compared to conventional strategies. The capacity of GCNs to utilize the data between picture patches leads to moved forward execution in identifying inconspicuous and advanced imitations, which are regularly missed by conventional CMFD methods.
- Scalability and Versatility: The proposed strategy is adaptable and can be adjusted to distinctive sorts of pictures and fraud scenarios. The utilize of graph-based modeling and GCNs gives adaptability in dealing with different picture resolutions and complexities. Also, the system can be expanded to consolidate other sorts of features and extra relevant data, advance improving its pertinence and effectiveness.

The proposed CMFD strategy utilizing GCN presents a noteworthy progression in the field of picture forensics. By leveraging the control of GCNs to show and analyze the connections between picture patches, the strategy accomplishes prevalent execution in recognizing complex duplicities. This commitment not as it were illustrates the potential of GCNs in picture forensics but too sets the organize for future investigate and advancement in applying graph-based procedures to different picture analysis tasks.

The rest of the article is categorized as follow:

The literature review section provides detail achievements and limitations of recent CMFD methods.

The proposed methodology sections give details about our proposed CMFD method.

The Experimental setups section mention details about hard and software setup for conduction experiments, following by the evaluations metrics and results section. Finally, discussion and conclusion sections provide extensive discussion and conclusion about the proposed CMFD methodology and its results.

III. LITERATURE REVIEW

Many researchers has proposed CMFD techniques in the last 2 decades. Barad and Goswami [7] presented the survey that discuss about two types of CMFD, traditional which uses image processing, and other are Deep Learning (DL) based techniques. It suggest the DL based techniques are more efficient in extracting more complex features then traditional CMFD techniques. However the computational cost of the proposed method is very high. Mayer and Stamm [8] suggest a novel Forensic Similarity Graph (FSG) technique that utilize the concept of ''community'' to detect CMF regions. However, it does not take in account the post processing attacks on forged images. Selvarathi et al. [9] uses a Convolution Neural Network (CNN) to train the model and Scale-Invariant Feature Transform (SIFT) for feature extraction for CMFD. It able to detect the CMF regions in the image with greater accuracy but trade-off in the complexity of the methodology due to CNN.

Zhou et al. [10] The show accomplishes lofty exactness in occasion location by leveraging chart convolutional systems to capture complex spatial and transient conditions. It appears solid execution over shifted datasets, showing great generalizability. The approach moreover benefits from improved highlight representation, driving to more exact occasion distinguishing proof. In any case, it is computationally seriously, requiring noteworthy preparing control and memory. Furthermore, the complexity of building and overseeing expansive charts can influence adaptability and commonsense execution in real-time frameworks. Hosny et al. [11] presented a novel CMFD technique which utilizes quaternion polar complex exponential transform moments (QPCETMs) that has ability to detect CMF regions even after post processing attacks like scaling, rotational and translation transformation in the digital images. However, it does not take in account the CMF regions which are attacked by compression, contrast change, and color reduction. Qazi et al. in [12] presented a learning-based advanced CMFD framework. It utilize the ResNet50v2 using lingering layers to train the CMFD model. The proposed CMFD technique show promising results, however it lacks in detecting complex shape CMF regions in digital images.

Gharibi et al. in [13] utilizes the a non-deep-learning based a texture-based method for CMFD. It uses Principle Component Analysis (PCA) for reducing feature size. However it is block-based CMFD technique which increase the computational cost of the proposed method. Amirini et al. [14] presented a key point-based CMFD technique. In the proposed CMFD method, it make the clusters of the extracted features to make the detection process fast. However, it does not take in account the post processing attack on CMF regions in digital images. Al-Qershi et al. in [15] write a survey article which primarily focus on passive CMFD methods. It presented the advantages of passive technique over active CMFD techniques. Xue et al. in [16] proposed a strategy viably recognizes copy-move imitations by utilizing Sphere (Situated Quick and Turned BRIEF) highlights, accomplishing elevated precision and strength against common changes like scaling and turn. It benefits from the productivity of Sphere, coming about in speedier handling times appropriate for commonsense applications. The method is moreover less computationally requesting compared to a few progressed strategies. Be that as it may, it may battle with exceedingly complex imitations including unobtrusive varieties, and its execution can be influenced by picture commotion and moo surface regions. Moreover, it might require fine-tuning to keep up precision over diverse sorts of pictures and fraud scenarios. Another technique [17] presented by Hosny et al. proposed a methodology for CMFD which detect object from the input image and extract features for only detected object hence reducing the computational cost of the proposed CMFD method. The proposed CMFD method detect

CMF regions after post processing attack like JPEG compression, rotational, and scaling transformation, but unable to detetec CMF regions that are attacked with translational transformation. Narasimhamurthy et al. in [18] proposed a strategy accomplishes soaring precision in identifying copy-move frauds by utilizing altered SURF (Speeded-Up Robust Features) and the AKAZE (Accelerated-KAZE) finder, successfully distinguishing produced locales indeed beneath different changes. It benefits from the strong highlight extraction capabilities of SURF and the effectiveness of the AKAZE locator, coming about in dependable and quick discovery. Zimba et al. in [19] proposed a CMFD technique and utilize Discrete Wavelet Transform (DWT) with PCA through Eigenvalue Decomposition (EVD). It lacks the detection of CMF regions under post-processing attacks.

Warif et al. in [20] presented a study to recognizes key challenges, such as taking care of complex replications and keeping up precision over various picture CMF attacks. The study offers profitable bits of knowledge into the confinements of existing strategies, counting towering computational costs and affectability to clamor. It too traces future investigate bearings, emphasizing the require for more strong and productive calculations. Be that as it may, it does not propose unused strategies, centering instep on summarizing and analyzing existing investigate. Chen et al. [21] This strategy viably recognizes locale duplication imitations by utilizing Harris corner focuses for vigorous highlight extraction and step division insights for exact coordinating. It accomplishes high exactness and unwavering quality in distinguishing copied locales, indeed in the nearness of geometric changes. The approach is proficient, permitting for moderately quick preparing times. In any case, it may battle with complex frauds including unpretentious varieties in surface or low-contrast regions. Moreover, the execution can be delicate to clamor and requires cautious tuning of parameters for ideal comes about. Shahroudnejad and Rahmati in [22] presented a strategy leverages affine-SIFT for viable copy-move imitation discovery, giving strength to relative changes and accomplishing elevated precision in recognizing CMF regions in digital images. It also has ability to detect CMF regions even after resized, however it compromises its precision.

Nguyen and Katzenbeisser in [23] proposed a CMFD strategy which uses Radon Transformation (RT) and Phase Correlation (PC). Due to the RT, and PC it enable the proposed method to detect CMF regions even after rotational transformation. The proposed CMFD method trade off with accuracy and precision. Chen et al. in [24] suggest a CMFD technique which take advantages of Fractional Quaternion Cosine Transforms (FrQCT). FrQCT has ability to extract color features which help the proposed methodology extract more rich features from forged image. However, it lacks detecting CMF regions under post-processing attacks. Farhan et al. [25] presented a survey on CMFD techniques which discussed various types of CMF techniques and discuss several CMFD methods presented in last decade. The study pointed out limitations in many CMFD methods i.e. lack of evidence why specific approach is used and how it helps in capturing the CMF regions. Yang et al. in [26] proposed a CMFD technique which uses SIFT to extract features from CMF image. The proposed technique has ability to detect CMF regions under rotational transformation post-processing attack.

Mahoud and Husien in [27] uses a Pseudo-Zernike Moment (PZM). It can detect CMF regions even after post-processing attack like color and contrast adjustment thanks to PZM. However, it lack in detecting scale invariant CMF regions. Divya et al. in [28] a CMFD technique which benefits from the vigor and speed of SURF, permitting for productive highlight extraction. The utilize of SVM improves the classification exactness, making the strategy solid over different fraud scenarios. Be that as it may, it is computationally requesting, requiring critical handling control for both feature extraction and CMFD. Also, the approach may battle with complex imitations and high commotion levels, requiring cautious parameter tuning for ideal execution.

Wang et al. in [29] presented a novel key point based CMFD technique, which utilizes clustering and segmentation followed by hybrid feature extraction using Fast Quaternion Generic Polar Complex Exponential Transform (FQGPCET) and ray-level co-occurrence matrix (GLCM) from the selected segments of the input image. However, it does not take in account the post-processing attack like JPEG compression, scaling and rotational transformation.

IV. PROPOSED METHODOLOGY

The technique for CMFD utilizing GCNs is an orderly approach planned to address the challenges of recognizing picture imitations, especially the modern CMF's that are predominant in the advanced CMF post-processing attacks. It leverages the control of GCNs to change digital pictures into organized graphs, empowering nuanced feature extraction and strong imitation discovery. The technique includes information collection, graph representation, demonstrate design, preparing, assessment, and vigor investigation. By using this strategy, analysts can development the state-of-the-art CMFD system in digital picture forensics, contributing to the conservation of picture genuineness in a manipulated digital world as appeared in Figure 2.

A. DATA COLLECTION AND PREPARATION

Data collection and preparation are crucial steps in the development of any machine learning model. Following us discussing about dataset selection and pre-processing in out proposed CMFD technique.

1) DATASET SELECTION

We select a MICC F220 [30] and CoMoFoD [31] datasets D_1 & D_2, comprising N_1 & N_2 images, where each image is represented as I_{1i} & K_{2i} is the ground truth forgery map for

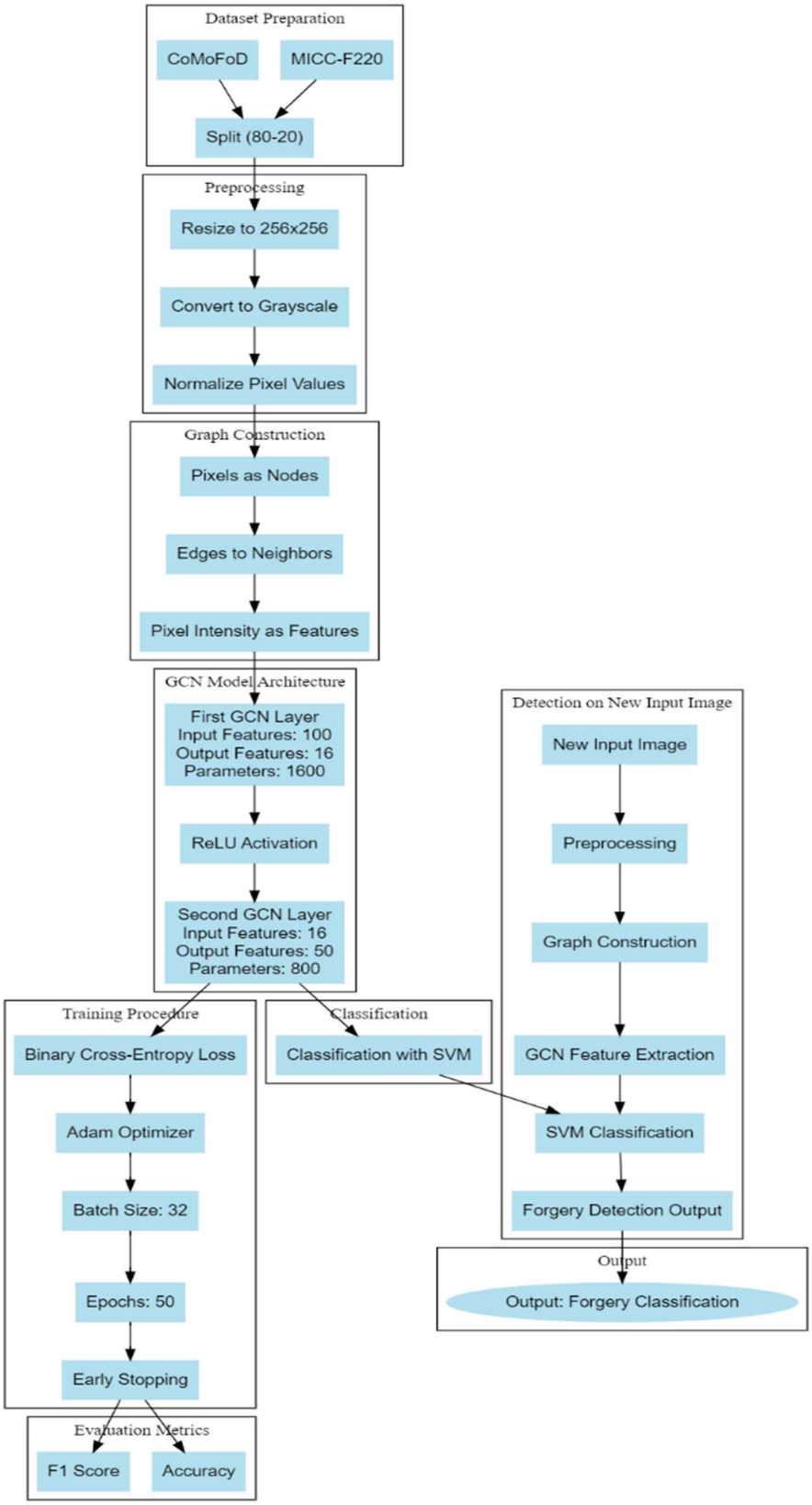

FIGURE 2. Proposed CMFD block diagram.

image I_i using. (1).

$$D_1 = \{(I_{11}, K_{11}), (I_{12}, K_{12}), \ldots, (I_{1N}, K_{1N_1})\}$$
$$D_2 = \{(I_{21}, K_{21}), (I_{22}, K_{22}), \ldots, (I_{2N}, K_{2N_2})\} \quad (1)$$

Here N_1 & N_2 is 220 as MICC F220 consist of 220 images, out of which 110 are original images and 110 consist of forged images with the resolution of 800 by 532 pixels, and CoMoFoD consist of 200 forged images which include truth, and forged images with post processing attack i.e. JPEG compression, color reduction, scaling, and rotational transformations with the resolution of 512 by 512 pixels. An original and forged image from MICC F220 and CoMoFoD dataset are presented in Figure 3.

The both dataset has original images as well as tempered images with ground truth. As shown in Figure 2, the images from both dataset are split into 80-20 ratio for target and test data. The ground truth help to correctly calculate the accuracy of out proposed CMFD method.

2) PREPROCESSING

We normalize and preprocess the images, converting them to grayscale I_{gray} using (2) and (3) [32].

$$I_{gray} = sum(I)/3 \quad (2)$$
$$I_{normalized} = (I - min(I))/(max(I) - min(I)) \quad (3)$$

B. GRAPH REPRESENTATION OF IMAGES

Graph representation of images includes changing a picture into an organized graph, where the components of the graph compare to the components of the picture, such as pixels or picture regions [33]. Each hub in the graph represents a substance, and edges characterize connections between these substances. We represent a picture as a graph as appear in Figure 4.

In this diagram:

- Each circle (node) represents a region of the image.
- Edges (arrows) represent the similarity or relationship between the regions.

To make a more point by point and particular graph representation of an actual image, we perform the following

- Divide the image into littler regions (i.e., superpixels).
- Represent each region as a node.
- Define edges based on similitude measures such as color, surface, or spatial proximity.

For illustration, adjacent regions with relative color histograms might have edges between their comparing nodes, weighted by the degree of similitude. This structure empowers the application of graph-based calculations for CMF detection.

1) NODE AND EDGE CONSTRUCTION

We create a graph G for each image, comprising nodes (image regions or pixels) [34] and edges to capture spatial relationships using (4).

$$G_i = (V_i, E_i) \quad (4)$$

FIGURE 3. (a) Original image, and (b) forged image from MICC F220 dataset, (b) original image, and (d) forged image from CoMoFoD dataset.

2) NODE FEATURE EXTRACTION

We extract node features, including pixel values I, texture features T_i and color histograms H_i using (5).

$$X_i = \{[I_1, T_1, H_1], [I_2, T_2, H_2], \ldots\} \quad (5)$$

C. GCN ARCHITECTURE

1) GCN LAYER

The GCN layer is a significant component in graph-based profound learning models, particularly when connected to assignments like hub classification, interface expectation, or, in our case, CMFD.

The GCN layer engenders data through the graph structure to capture connections and conditions among hubs as displayed in Figure 5.

This diagram represents a GCN layer, showing how node features are propagated and transformed:

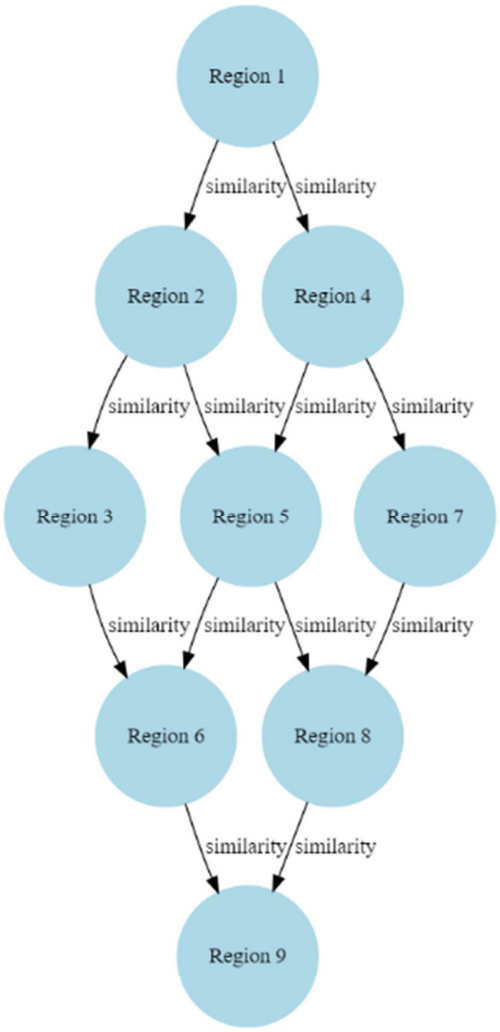

FIGURE 4. Image regions and their relationship in graph representation.

Nodes: Each node (e.g., $R1, R2, \ldots, R9$) represents a region of the image.

Edges: The edges (e.g., $w_1, w_2, \ldots, w_8$)) represent the relationships (weights) between these regions.

Feature Propagation: Dotted lines illustrate the propagation of node features through the weight matrix W^l to the next layer $l + 1$.

In this diagram, the cluster on the left represents the node features at layer 1, and the cluster on the right represents the node features at layer $l + 1$, after applying the GCN layer transformation. Each node in the l layer is connected to its corresponding node in the $l + 1$ layer by a dotted line, representing the application of the weight matrix W^l. The solid lines within each cluster represent [35] the adjacency relationships among the nodes.

Given an input feature matrix X representing node features, an adjacency matrix A representing the graph structure, and weight matrix W for the layer, the output X_{new} after applying the GCN layer can be calculated as in (6).

$$X_i = \sigma(A_i X_i W_i) \tag{6}$$

Here,

X is the input feature matrix of shape (number of nodes, number of features per node).

A is the adjacency matrix of the graph, encoding the relationships between nodes.

W is the weight matrix for the layer.

σ represents the activation function (commonly ReLU or another non-linear activation function).

2) FEATURE PROPAGATION

We describe how information is propagated across the graph using GCN layers to capture relationships and dependencies within the image using Equ. 7.

$$X_{i_{new}} = \sigma(A_i X_i W_i) \tag{7}$$

D. TRAINING THE GCN

1) LOSS FUNCTION

For CMFD, the approach we utilize is to outline the errand as a twofold classification issue where proposed CMFD predicts whether each pixel or locale is portion of a fraud or not. A reasonable loss function for this double classification errand is the twofold cross-entropy loss as displayed in Figure 6.

This diagram delineates the prepare of CMFD utilizing a GCN and the parallel cross-entropy loss function. Here's a brief clarification of each component:

Input Image: The input image that is to be checked for forgery.

GCN Layers: Multiple layers of the GCN that process the image and extract features.

Output (Predictions): The output from the GCN, representing the predictions for each pixel or region, indicating whether it is part of a forgery.

Ground Truth Labels: The actual labels indicating whether each pixel or region is part of a forgery.

Binary Cross-Entropy Loss: The loss function used to measure the discrepancy between the predicted and actual labels [36].

The mathematical equation for the binary cross-entropy loss is shown in (8).

$$L = -\frac{N}{1}\sum_{i=1}^{N}(K_i log(P_i) + (1 - K_i) log(1 - P_i)) \tag{8}$$

Here:

L is the binary cross-entropy loss.

N is the total number of pixels or regions.

K_i is the ground truth label (1 for forgery, 0 for non-forgery) for pixel or region i.

P_i is the predicted probability that pixel or region i belongs to a forgery.

This loss function penalizes the model based on the logarithmic difference between the predicted probability P_i and the ground truth label K_i. It energizes the show to relegate giant probabilities for genuine forgery regions and low probabilities for non-forgery regions. In the context of GCNs, this loss function is frequently connected to the yield of the last

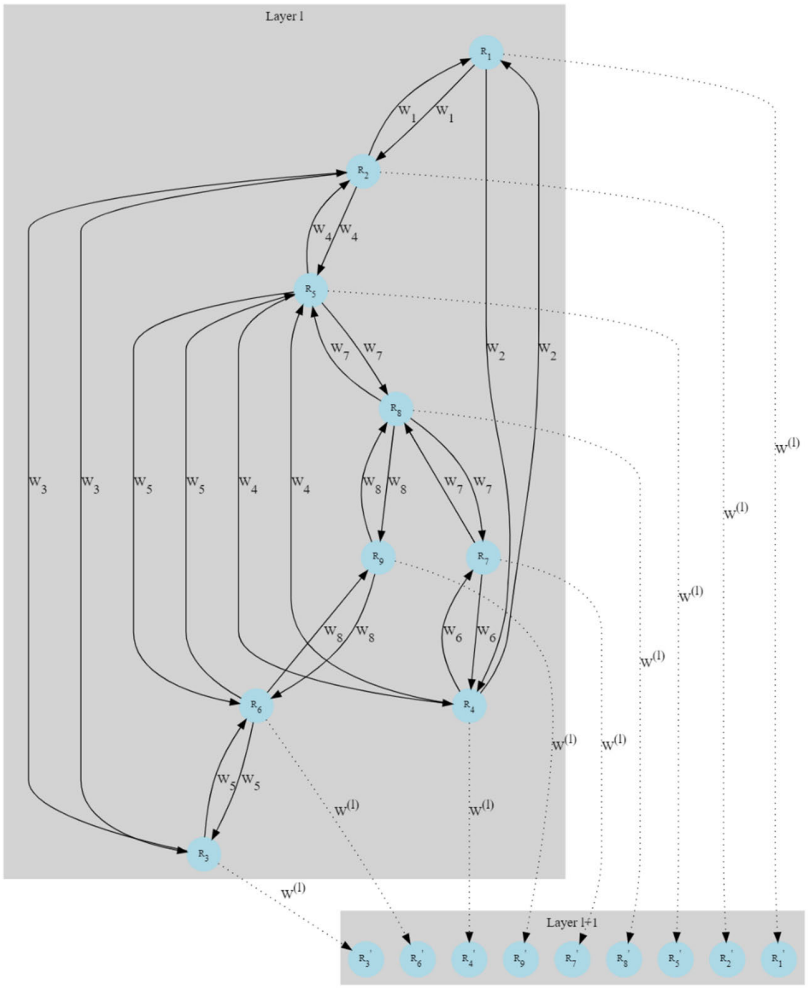

FIGURE 5. Feature transformation and propagation.

layer or a classification layer in the model. The objective amid preparing is to alter the organize parameters (weights) to minimize this loss, progressing the model's capacity to accurately classify regions as forgery or non-forgery.

E. OPTIMIZATION

We optimize the GCN parameters (W_i) using an optimizer i.e. Adam optimizer [37] to minimize the loss using (9).

$$W_{i_{new}} = W_i - \alpha \frac{\partial L_i}{\partial W_i} \tag{9}$$

Here,

W_{new} is the updated set of model parameters.

W is the current set of model parameters.

α is the learning rate, a hyper-parameter that determines the step size in the parameter space.

$\frac{\partial W}{\partial L}$ is the gradient of the loss function L with respect to the model parameters W.

The gradient $\frac{\partial W}{\partial L}$ points in the direction of the steepest increase in the loss function. By subtracting this gradient from the current parameters, scaled by the learning rate α, we move the parameters in the direction that reduces the loss.

F. VALIDATION

To validate and update hyper-parameters in our proposed CMFD method we utilize the following (10).

$$\frac{\partial L_i}{\partial W_i} = 0 \tag{10}$$

G. CLASSIFIER SELECTION AND TRAINING

1) SVM CLASSIFIER

We uses SVM classifier which enable our proposed CMFD method to extract more rich and content full features from CMF picture. The Process of using SVM classifier in our proposed CMFD method is presented in Figure 7.

We employ a SVM classifier [38] for evaluating GCN-extracted features using (11).

$$Y_i = SVM(X_{i_{new}}) \tag{11}$$

Here,

Y_i is the output of the SVM classifier.

X_i is the feature matrix obtained from the GCN-extracted features.

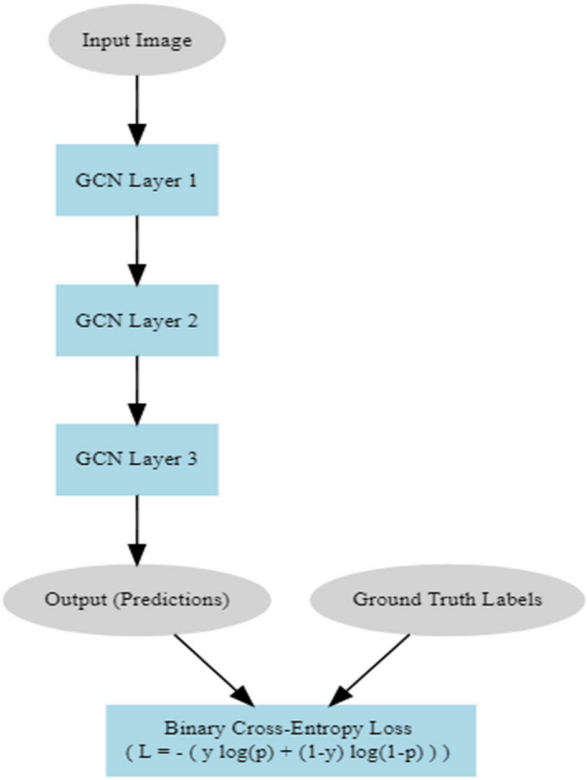

FIGURE 6. Binary cross-entropy loss for GCN layers.

The SVM classifier is trained to learn a decision boundary that separates different classes in the feature space. The decision boundary is determined by a set of weights (w) and biases (b). The decision function can be written as in (12).

$$Yi = sign(w \cdot Xi + b) \tag{12}$$

In this equation,
"w" is the weight vector.
"." denotes the dot product.
"b" is the bias term.

The sign function assigns a class label based on whether the dot product $w \cdot Xi + b$ is positive or negative. The SVM aims to maximize the margin between different classes, leading to a robust decision boundary.

The actual SVM training involves finding the optimal w and b that maximize the margin while satisfying certain constraints related to the correct classification of training samples. The trained SVM is used to predict the class labels of new samples based on their features.

V. EXPERIMENTAL SETUP

We have use the following hard and software specification for out experimental setup as presented in Table 1.

VI. PERFORMANCE EVALUATION METRICS

The adequacy of the proposed GCN-based CMFD strategy was surveyed utilizing two key assessment measurements: accuracy and F1 score [39]. These measurements give a comprehensive understanding of the model's execution, especially in the setting of double classification errands such as forgery detection.

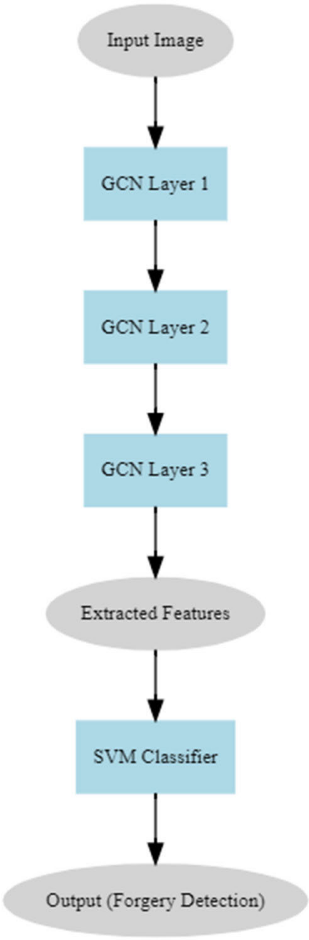

FIGURE 7. SVM classifier for CMFD.

TABLE 1. Hardware and software specification for experimental setup.

Hardware/ Software	Specification
CPU	Intel i7
RAM	16GB
OS	Windows 10
Tool	Python 3 with Torch library

A. ACCURACY

Accuracy is a principal metric that measures the extent of accurately recognized forgeries and non-forgeries out of the add up to number of occasions. It is calculated as in (13).

$$Accuracy = \frac{T_P + T_N}{N} \tag{13}$$

where:
T_P : True Positives
T_N : True Negatives
N : Total Number of Instances

TABLE 2. MICC F220 model training results for different values of epochs.

Epoch	Training Loss (T_loss)	Validation Loss (V_loss)	Training Accuracy (T_acc)	Validation Accuracy (V_acc)	F1-Score Training	F1-Score Validation
20	0.283	0.304	0.626	0.684	0.626	0.684
40	0.198	0.262	0.986	0.977	0.986	0.977
50	0.21	0.268	0.987	0.986	0.987	0.986
60	0.19	0.257	0.986	0.97	0.986	0.97
80	0.07	0.248	0.98	0.982	0.98	0.982
100	0.074	0.24	1	1	1	1

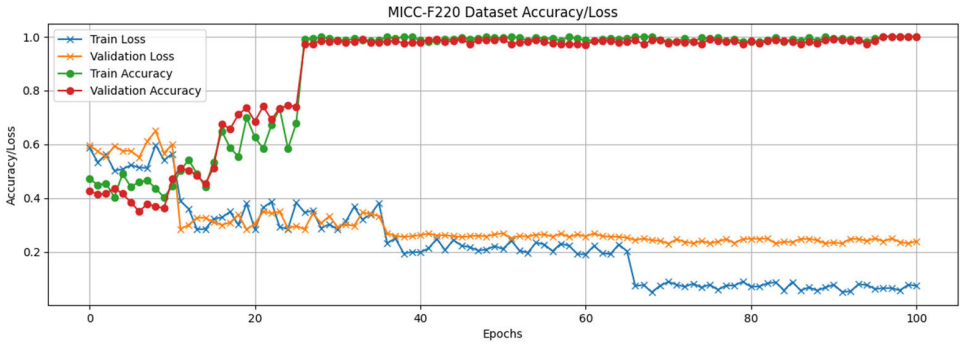

FIGURE 8. Train/validation accuracy and loss for 100 epochs for MICC F220 dataset.

TABLE 3. CoMoFoD model training results for different values of epochs.

Epoch	Training Loss (T_loss)	Validation Loss (V_loss)	Training Accuracy (T_acc)	Validation Accuracy (V_acc)	F1-Score Training	F1-Score Validation
20	0.229	0.274	0.294	0.324	0.294	0.324
40	0.098	0.162	0.818	0.697	0.818	0.697
50	0.11	0.168	0.855	0.772	0.855	0.772
60	0.09	0.157	0.742	0.763	0.742	0.763
80	0.12	0.168	0.819	0.782	0.819	0.782
100	0.126	0.16	0.82	0.78	0.82	0.78

B. F1 SCORE

The F1 score is calculated as shown in (14)

$$F_1 = \frac{2T_P}{2T_P + F_P + F_N} \tag{14}$$

where:

F_P : True Positives

F_N : False Negative

VII. EXPERIMENTAL RESULTS

The proposed GCN-based method for CMFD was evaluated using multiple metrics, including training loss (T_loss), validation loss (V_loss), training accuracy (T_acc), validation accuracy (V_acc), and F1-score. The results are summarized below for the MICC-F220, and CoMoFoD is presented in Table 2 and Table 3 respectively for epoch's values of 20, 30, 40, 50, 60, 80, and 100. The complete results for 0-100 epochs is presented in the Figure 8 and Figure 9.

VIII. COMPARATIVE ANALYSIS

The comparative analysis of our proposed CMFD method is conducted with state of the art CNN based technique proposed by Kuznetsov et al. in [40] and Elaskily et al. [41] in term of Training loss and accuracy, Validation loss and accuracy, and F1 score as presented in Table 3.

By reviewing the Table 4 results of our proposed with the CNN based technique, it is clear that in the initials epochs the CNN based technique perform good but in higher epoch e.g. at 75 and onward out proposed CMFD technique perform well due the GCN superiority over CNN.

IX. DISCUSSION

The execution enhancements accomplished by the proposed GCN-based strategy highlight the significance of leveraging progressed neural organize structures for CMFD. Whereas GCNs have been broadly utilized and have appeared critical victory, the capacity of GCNs to demonstrate connections

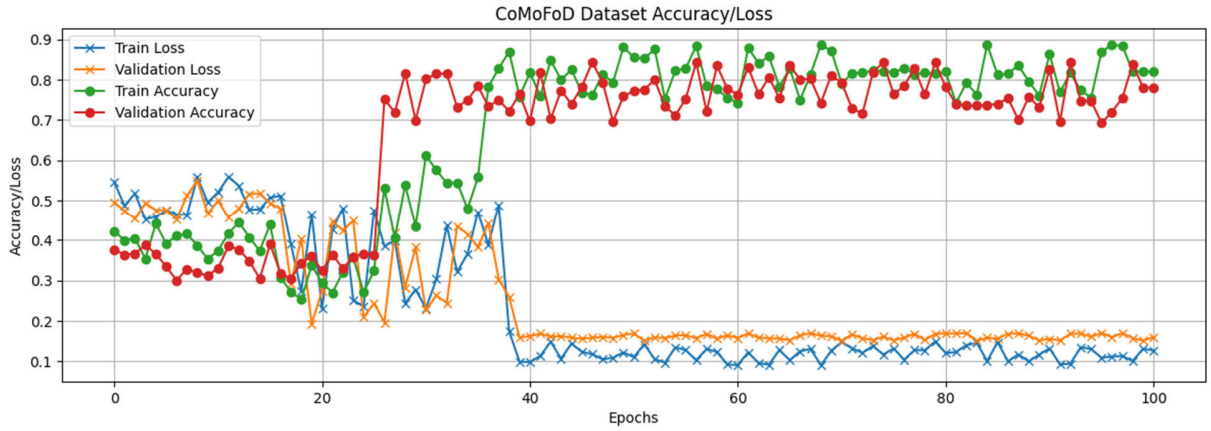

FIGURE 9. Train/validation accuracy and loss for 100 epochs for CoMoFoD dataset.

TABLE 4. Comparative analysis of proposed with Kuznetsov et al. [40], and Elaskily et al. [41] for MICC F220 dataset.

Epochs	CMFD Techniques	Training Loss (T_loss)	Validation Loss (V_loss)	Training Accuracy (T_acc)	Validation Accuracy (V_acc)	F1-Score Training
15	Kuznetsov et al.	0.232	**0.249**	**0.920**	**0.954**	**0.95**
	Elaskily et al.	**0.078**	-	-	0.921	-
	Proposed CMFD Method	0.322	0.310	0.534	0.513	0.534
25	Kuznetsov et al.	**0.147**	0.394	**0.965**	0.954	**0.95**
	Elaskily et al.	0.394	-	-	**0.961**	-
	Proposed CMFD Method	0.383	**0.296**	0.677	***0.738***	0.677
35	Kuznetsov et al.	0.120	0.3161	0.965	0.954	0.95
	Elaskily et al.	0.023	-	-	0.976	-
	Proposed CMFD Method	**0.382**	**0.333**	**0.985**	**0.979**	**0.985**
50	Kuznetsov et al.	0.111	0.3832	0.965	0.954	0.95
	Elaskily et al.	0	-	-	1	-
	Proposed CMFD Method	**0.21**	**0.268**	**0.995**	**0.989**	**0.995**
75	Kuznetsov et al.	**0.039**	0.4729	0.988	0.954	0.95
	Elaskily et al.	0	-	-	**1**	-
	Proposed CMFD Method	0.078	**0.232**	**0.993**	0.99	**0.993**

between distinctive parts of the picture gives a significant advantage.

The outcomes show that joining basic data through GCNs leads to more compelling and exact feature extraction. This is especially vital in the setting of CMFD, where the produced locales regularly show complex and inconspicuous designs that are challenging to distinguish utilizing conventional methods.

Moreover, the comparative examination underscores the need of creating vigorous models that can generalize well to modern information. The higher validation accuracy and lower validation loss accomplished by the proposed strategy propose that GCNs can give more dependable execution in different and erratic real-world scenarios.

X. CONCLUSION

In this section, we have made and evaluated a novel approach for distinguishing CMF's in computerize pictures utilizing GCNs. Our procedure leverages the capabilities of GCNs to effectively capture the essential and spatial association's interior the picture, driving to advanced highlight extraction and extortion detection.

The test comes approximately outline that our proposed CMFD technique outflanks existing state-of-the-art techniques. The following key disclosures highlight the prevalence of our method:

A. TRAINING AND VALIDATION LOSS

- The proposed strategy accomplishes a quick decrease in training loss, stabilizing at lower values after 75 epochs goes down to 0.78%. This shows that the GCN-based approach learns the information representations more efficiently.
- Similarly, the validation loss for the proposed strategy is reliably lower than that of the reference strategy and goes down to 2.32% at after 75 epochs, appearing way better generalization and vigor in identifying frauds on inconspicuous data.

B. TRAINING AND VALIDATION ACCURACY

- The training precision of the proposed strategy comes to about 100% by 25 epochs. This illustrates the adequacy of the GCN in capturing perplexing designs and connections in the preparing data.

- The validation precision too favors the proposed strategy, which stabilizes over 99% after 25 epochs. This proposes that the proposed strategy generalizes superior to modern information, making it more solid for viable applications.

C. F1-SCORE

- The F1-scores for both preparing and approval are higher for the proposed strategy, stabilizing near to 1 after 35 epochs and goes to 100% after 100 epochs. This demonstrates that our strategy keeps up a way better adjust between accuracy and review, driving to more precise and solid forgery detection.

In conclusion, our proposed CMFD technique illustrates that the utilization of GCNs for CMFD offers critical advantage over conventional CNN-based strategies. The proposed approach not as it were accomplishes higher accuracy and lower loss but too guarantees an adjusted and vigorous execution. Future investigate can encourage investigate the potential of GCNs and other progressed neural arrange designs to improve the detection of different sorts of digital forgeries.

CONFLICT OF INTEREST

None of the authors have a conflict of interest to disclose.

REFERENCES

[1] R. W. Belk, "Extended self in a digital world," *J. Consum. Res.*, vol. 40, no. 3, pp. 477–500, 2013.

[2] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1841–1854, Dec. 2012.

[3] M. Kirchner, P. Schoettle, and C. Riess, "Thinking beyond the block: Block matching for copy-move forgery detection revisited," *Proc. SPIE*, vol. 9404, pp. 11–22, Mar. 2015.

[4] A. M. Atallah, I. I. Mahmoud, and H. S. Ali, "Robust dense-field based copy-move forgery localization using generic radial harmonic Fourier moment invariants," *J. Forensic Sci.*, vol. 69, no. 1, pp. 139–152, Jan. 2024.

[5] K. M. Hosny, A. M. Mortda, M. M. Fouda, and N. A. Lashin, "An efficient CNN model to detect copy-move image forgery," *IEEE Access*, vol. 10, pp. 48622–48632, 2022.

[6] S. Koul, M. Kumar, S. S. Khurana, F. Mushtaq, and K. Kumar, "An efficient approach for copy-move image forgery detection using convolution neural network," *Multimedia Tools Appl.*, vol. 81, no. 8, pp. 11259–11277, Mar. 2022.

[7] Z. J. Barad and M. M. Goswami, "Image forgery detection using deep learning: A survey," in *Proc. 6th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Mar. 2020, pp. 571–576.

[8] O. Mayer and M. C. Stamm, "Exposing fake images with forensic similarity graphs," *IEEE J. Sel. Topics Signal Process.*, vol. 14, no. 5, pp. 1049–1064, Aug. 2020.

[9] C. Selvarathi, M. Bharath, J. Gowrishankar, and R. Karthikeyan, "Copy move counterfeiting identification based on CNN using scalar invariant feature technique," in *Proc. 2nd Int. Conf. Electron. Renew. Syst. (ICEARS)*, Mar. 2023, pp. 1019–1025.

[10] P. Zhou, B. Zhang, B. Wu, Y. Luo, N. Ning, and J. Gong, "A novel event detection model based on graph convolutional network," in *Proc. Int. Conf. Web Inf. Syst. Eng.* Germany: Springer, 2020, pp. 172–184.

[11] K. M. Hosny, H. M. Hamza, and N. A. Lashin, "Copy-for-duplication forgery detection in colour images using QPCETMs and sub-image approach," *IET Image Process.*, vol. 13, no. 9, pp. 1437–1446, Jul. 2019.

[12] E. U. H. Qazi, T. Zia, and A. Almorjan, "Deep learning-based digital image forgery detection system," *Appl. Sci.*, vol. 12, no. 6, p. 2851, Mar. 2022.

[13] F. Gharibi, J. RavanJamjah, F. Akhlaghian, B. Z. Azami, and J. Alirezaie, "Robust detection of copy-move forgery using texture features," in *Proc. 19th Iranian Conf. Electr. Eng.*, May 2011, pp. 1–4.

[14] I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, L. D. Tongo, and G. Serra, "Copy-move forgery detection and localization by means of robust clustering with J-linkage," *Signal Process., Image Commun.*, vol. 28, no. 6, pp. 659–669, Jul. 2013.

[15] O. M. Al-Qershi and B. E. Khoo, "Passive detection of copy-move forgery in digital images: State-of-the-art," *Forensic Sci. Int.*, vol. 231, nos. 1–3, pp. 284–295, Sep. 2013.

[16] Z. L. Xue, L. Tian, and C. Li, "Passive image copy-move forgery detection based on orb features," in *Proc. Recent Develop. Intell. Comput., Commun. Devices (ICCD)*. Germany: Springer, 2019, pp. 312–317.

[17] K. M. Hosny, H. M. Hamza, and N. A. Lashin, "Copy-move forgery detection of duplicated objects using accurate PCET moments and morphological operators," *Imag. Sci. J.*, vol. 66, no. 6, pp. 330–345, Aug. 2018.

[18] S. K. Narasimhamurthy, V. K. Mahadevachar, and R. K. T. Narasimhamurthy, "A copy-move image forgery detection using modified SURF features and AKAZE detector," *Int. J. Intell. Eng. Syst.*, vol. 16, no. 4, pp. 12–24, 2023.

[19] M. Zimba and S. Xingming, "DWT-PCA (EVD) based copy-move image forgery detection," *Int. J. Digit. Content Technol. Appl.*, vol. 5, no. 1, pp. 251–258, Jan. 2011.

[20] N. B. A. Warif, A. W. A. Wahab, M. Y. I. Idris, R. Ramli, R. Salleh, S. Shamshirband, and K.-K.-R. Choo, "Copy-move forgery detection: Survey, challenges and future directions," *J. Netw. Comput. Appl.*, vol. 75, pp. 259–278, Nov. 2016.

[21] L. Chen, W. Lu, J. Ni, W. Sun, and J. Huang, "Region duplication detection based on Harris corner points and step sector statistics," *J. Vis. Commun. Image Represent.*, vol. 24, no. 3, pp. 244–254, Apr. 2013.

[22] A. Shahroudnejad and M. Rahmati, "Copy-move forgery detection in digital images using affine-SIFT," in *Proc. 2nd Int. Conf. Signal Process. Intell. Syst. (ICSPIS)*, Dec. 2016, pp. 1–5.

[23] H. C. Nguyen and S. Katzenbeisser, "Detection of copy-move forgery in digital images using radon transformation and phase correlation," in *Proc. 8th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Jul. 2012, pp. 134–137.

[24] B. Chen, M. Yu, Q. Su, and L. Li, "Fractional quaternion cosine transform and its application in color image copy-move forgery detection," *Multimedia Tools Appl.*, vol. 78, no. 7, pp. 8057–8073, Apr. 2019.

[25] M. H. Farhan, K. Shaker, and S. Al-Janabi, "Copy-move forgery detection in digital image forensics: A survey," *Multimedia Tools Appl.*, vol. 83, pp. 70603–70635, Feb. 2024.

[26] B. Yang, X. Sun, H. Guo, Z. Xia, and X. Chen, "A copy-move forgery detection method based on CMFD-SIFT," *Multimedia Tools Appl.*, vol. 77, no. 1, pp. 837–855, Jan. 2018.

[27] K. Mahmoud and A. Husien, "Copy-move forgery detection using Zernike and pseudo Zernike moments," *Int. Arab J. Inf. Technol.*, vol. 13, no. 6A, pp. 930–937, 2016.

[28] S. Dhivya, J. Sangeetha, and B. Sudhakar, "Copy-move forgery detection using SURF feature extraction and SVM supervised learning technique," *Soft Comput.*, vol. 24, no. 19, pp. 14429–14440, Aug. 2024.

[29] X.-Y. Wang, X.-Q. Wang, P.-P. Niu, and H.-Y. Yang, "Accurate and robust image copy-move forgery detection using adaptive keypoints and FQGPCET-GLCM feature," *Multimedia Tools Appl.*, vol. 83, no. 1, pp. 2203–2235, Jan. 2024.

[30] I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, and G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 1099–1110, Sep. 2011.

[31] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic., "CoMoFoD-new database for copy-move forgery detection," in *Proc. 55th Int. Symp. (ELMAR)*, Zadar, Croatia, Sep. 2013, pp. 49–54.

[32] C. Saravanan, "Color image to grayscale image conversion," in *Proc. 2nd Int. Conf. Comput. Eng. Appl.*, Mar. 2010, pp. 196–199.

[33] S. Bai, C. Liang, Z. Wang, and W. Pan, "Information entropy induced graph convolutional network for semantic segmentation," *J. Vis. Commun. Image Represent.*, vol. 103, Aug. 2024, Art. no. 104217.

[34] Q. Zhang, J. Chang, G. Meng, S. Xu, S. Xiang, and C. Pan, "Learning graph structure via graph convolutional networks," *Pattern Recognit.*, vol. 95, pp. 308–318, Nov. 2019.

[35] L. Zhang, H. Song, N. Aletras, and H. Lu, "Node-feature convolution for graph convolutional networks," *Pattern Recognit.*, vol. 128, Aug. 2022, Art. no. 108661.
[36] Z. Zhang and M. Sabuncu, "Generalized cross entropy loss for training deep neural networks with noisy labels," in *Proc. Adv. Neural Inf. Process. Syst.*, 2018, pp. 1–11.
[37] A. Tato and R. Nkambou, "Improving Adam optimizer," in *Proc. Workshop Track—ICLR*, 2018, pp. 1–4.
[38] S. Yue, P. Li, and P. Hao, "SVM classification: Its contents and challenges," *Appl. Math. J. Chin. Universities*, vol. 18, pp. 332–342, Sep. 2003.
[39] M. Sokolova, N. Japkowicz, and S. Szpakowicz, "Beyond accuracy, F-score and ROC: A family of discriminant measures for performance evaluation," in *Proc. Australas. Joint Conf. Artif. Intell.* Germany: Springer, 2006, pp. 1015–1021.
[40] O. Kuznetsov, E. Frontoni, L. Romeo, and R. Rosati, "Enhancing copy-move forgery detection through a novel CNN architecture and comprehensive dataset analysis," *Multimedia Tools Appl.*, vol. 83, no. 21, pp. 59783–59817, Jan. 2024.
[41] M. A. Elaskily, H. A. Elnemr, A. Sedik, M. M. Dessouky, G. M. E. Banby, O. A. Elshakankiry, A. A. M. Khalaf, H. K. Aslan, O. S. Faragallah, and F. E. A. El-Samie, "A novel deep learning framework for copy-moveforgery detection in images," *Multimedia Tools Appl.*, vol. 79, nos. 27–28, pp. 19167–19192, Jul. 2020.

VARUN SHINDE (Member, IEEE) received the bachelor's degree in computer engineering from Pune University, India, in 2009, and the master's degree in information technology management from The University of Texas at Dallas, USA, in 2015. Currently, he is a Cloud Solutions Architect with Cloudera Inc. His research interests include deep learning, cloud computing, and generative AI. A significant portion of his earlier career was devoted to working on designing solutions at scale for large enterprises across areas, such as data lakehouse, data warehouse, machine learning, and MLOps.

VINEET DHANAWAT (Member, IEEE) received the bachelor's degree in computer engineering from Birla Institute of Technology and Science, Pilani, India, in 2011, and the master's degree in computer science from The University of Texas at Dallas, USA, in 2015. Currently, he is a Software Engineer with Meta Platforms Inc., where he's been entrusted with leading teams and tackling complex challenges head-on. He has held leadership roles in various organizations, driving innovation, and growth through strategic technology implementations. His interests include machine learning, artificial intelligence, and integrity.

AHMAD ALMOGREN (Senior Member, IEEE) received the Ph.D. degree in computer science from Southern Methodist University, Dallas, TX, USA, in 2002. He is currently a Professor with the Computer Science Department, College of Computer and Information Sciences (CCIS), King Saud University (KSU), Riyadh, Saudi Arabia, where he is the Director of the Cyber Security Chair, CCIS. Previously, he was the Vice Dean of the Development and Quality, CCIS. His research interests include mobile pervasive computing and cyber security. He also served as the Dean for the College of Computer and Information Sciences and the Head of the Academic Accreditation Council, Al Yamamah University. He served as the General Chair for the IEEE Smart World Symposium and a Technical Program Committee Member of numerous international conferences/workshops, such as IEEE CCNC, ACM BodyNets, and IEEE HPCC.

ANJANAVA BISWAS received the Engineering degree in computer science from Sikkim Manipal University of Health, Medical, and Technological Sciences (SMU), India, in 2006. Currently, he is a Senior AI Specialist Solutions Architect with Amazon Web Services (AWS). He is a fellow of BCS, U.K., IET, U.K., IETE, India, and a Senior Member of the IEEE Computational Intelligence Society. His research interests include machine learning, generative AI, NLP, deep learning, data analytics, and cloud architecture.

MUHAMMAD BILAL received the bachelor's degree in computer engineering from COMSATS Wah, Pakistan, in 2008, the master's degree in computer engineering from NUST, EME College Rawalpindi, Pakistan, in 2013, and the Ph.D. degree in software engineering from the University of Engineering and Technology (UET), Taxila, Pakistan, in 2022. Currently, he is the Head of the Program of Computer Engineering, HITEC University, Taxila. He has more than four years of IT industry experience and more than ten years in academia. His research interests include computer vision, digital image processing, forensic investigation, embedded systems, and artificial intelligence.

RIZWAN ALI NAQVI received the B.S. degree in computer engineering from COMSATS University, Pakistan, in 2008, the M.S. degree in electrical engineering from Karlstad University, Sweden, in 2011, and the Ph.D. degree in electronics and electrical engineering from Dongguk University, South Korea, in 2018. From 2011 to 2012, he was a Lecturer with the Department of Computer Science, Sharif College of Engineering and Technology, Pakistan. He joined the Faculty of Engineering and Technology, Superior College, Pakistan, as a Senior Lecturer, in 2012. From 2018 to 2019, he was a Postdoctoral Researcher with Gachon University, South Korea. He is currently an Assistant Professor with Sejong University, South Korea. His research interests include gaze tracking, biometrics, computer vision, artificial intelligence, machine learning, deep learning, and medical imaging analysis.

ATEEQ UR REHMAN (Senior Member, IEEE) received the B.S. degree in electrical (telecommunication) engineering from the COMSATS Institute of Information Technology, Lahore, Pakistan, in 2009, the M.S. degree in electrical engineering with a specialization in telecommunications from Blekinge Institute of Technology (BTH), Karlskrona, Sweden, in 2011, and the Ph.D. degree from the College of Internet of Things (IoT) Engineering, Hohai University (HHU), Changzhou Campus, China, in 2022. Currently, he is an Assistant Professor with the Faculty of Computing, Gachon University, South Korea. He has contributed to various international IEEE conferences and journals of repute. His research interests include but are not limited to biomedical signal processing, the Internet of Things (IoTs), the Social Internet of Things (SIoTs), big data, and renewable energy technologies.