AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
E-ISSN:3069-0102
VOL.5, NO. 4(2025)

AN EFFICIENT DEEP LEARNING APPROACHES FOR ENHANCING IMAGE CLASSIFICATION ACCURACY

Mullu Sai Poojitha[1],AlluVenkateswara Rao[2],N. Seshu Kumar[3],P.Sailaja[4]
[1] *M Tech scholar* [2] Associate professor, [3]*Associete professor*, [4]*Assistant professor*
Department of ECE, Miracle Educational Society Group of Institutions

Abstract

*Digital imagemanipulation takes parttodeform thecontentofa picture in ordertoaccomplish some deceit purposes. Such deceits are acknowledged as forgeries. The precise forgery detection plays a key role in digital images. Image forgery detectionapproaches may be active or passive. Copy-move forgery detection (CMFD) is a passive-Blindimageforgerydetectionmethod.CMFDmainlyimpressesonthespeedandrigorousofthedetection method. To detect CMF, many algorithms are published such as segment based, key pointbasedand block-basedmethods. we are obtaining high accuracy from given data set by using Deep learning algorithm. The proposed method is an innovative and efficient algorithm called Generalized Approximate Reasoning-Based Intelligence Control (GARIC) algorithm. Hence, GARIC deep learning approach is used to detect the presence of falsification in images.*The performance of the method is evaluated using classification accuracy.

Keywords: *Digital image authentication,,copy-move forgery, Deep learning approach.*

I. INTRODUCTION

Nowadays, in this digital world, the digital images are playing vital role in manyfields and industries. Today's technology has begun to erode the trust and confidence that was earlier associated with images. Paul Valery's quote in a way makes sense. People find it exceedingly difficult to trust images, which were once indisputably accepted as proofs and evidences in so many fields. Digital image forgery detection approaches [1] are split in to activeauthenticationandpassive authentication.Active authenticationdependsonthe digitalsignature and need an original input image. It works on pre-embedded information or pre-registration. Active authentication is held during image formation and is mainly based onwatermarking[2].Passiveauthenticationisblin danddonotrequirepre-embeddedinformationaboutinputimage.Image forgery/tampering is not something new. Reality is that photographs have been manipulated for nearly as long as photography has been around. Throughout history, images have been manipulated to serve political and personal reasons

TAMPERING CATEGORIES

How does one ensure the authenticity of images? One should be familiar with the ways in which an image can be tampered before delving into solutions for that. Digital image tampering possibilities include,

- Image retouching
- Image splicing / photomontage
- Copy move forgery
- Geometrical Manipulations

The following section gives very brief descriptions of each of these with suitable illustrative examples.

Copy Move Forgery

Copy-move forgery is more or less similar to image splicing, wherein parts of an image are copied and pasted on the same image, with the intention of hiding something in or adding something extra to the existing image. Figure 1.5 is an example for an image tampered in this way where, the tampered image in the bottom shows portions of greenery copied and pasted to conceal the vehicle which is visible in the original image on the top. This is also known as region duplication forgery and the fact that the pasted region is from the same image makes detection more complex since tampered region's characteristics like texture, noise distribution, dynamic range, etc. (figure 1)

Received: 21-09-2025 | Accepted: 25-10-2025 | Published: 04-11-2025 | www.ajaccm.com

Fig.1.(a)Real imagehavingthreemissiles(b)copy-moveimage

Fig1.(a)Originalimage(b)forged image

Image Splicing

Image splicing also known as photo montage is a type of image forgery that involves compositing or combining two or more different images to create a fake image. A large number of fake pornography images are a result of splicing where faces of unassuming and innocent people are composited on to obscene images. Figure 1.4 shows an example of image splicing in which the images of Senator John Kerry and anti-war activist Jane Fonda have been put together to present the public with the false view of them working together.Belowfig.2 shows an example of image splicing [4].

Fig.2.BinLaden'ssplicedimage(combiningthela denfacewithanotherimage).

Geometrical Manipulations

Regions of the image may be subjected to geometrical changes including scaling, rotation, translation and affine transformations. These are usually performed in combination with the above discussed tampering methods and in many occasions this combined effect of tampering adds on to the complexity of tampering detection. Figure 3 shows an image tampered by copy move forgery compounded by rotation. It can be visualized from the figure that the tree has been copied and rotated at an angle and then pasted in another part of the image. Another complication introduced with the intention to conceal traces of tampering is the introduction of noise to the forged regions. Tampering may also involve multiple copy move attacks on the same imageFig.4 shownbelow is anexampleof imageretouching[6].

Fig.3.Originalimage(left)followed bytwo altered images

II. RELATEDWORK

In recent years the digital image forgeries are increasingly widespread, from that themost common one is the CMF.It is nothing but the image copying from one part andpasting it in other part. Hence, Choudhary Shyam Prakash *et al* [19] proposed an AKAZEtechnique for the forged region detection in smooth regions. It is a CMFD technique of keypoint. This technique is robust compared to distortion and post-processing operations. The most popular key-point based algorithms are ;nearest neighbor (2NN,g2NN)andclustering (HAC, WPGMC). For detecting forged multiple regions the g2NN matchingprocessis taken. This methodattained better accuracyandefficiency.

In digital era images play a main role in communication which creates interaction tothe people. Yet there is a big problem occurs such as Copy-move forgery and the detectionof this forgery is very difficult. From this reason, Mohamed A. Elaskily*et al* [6] proposedclosemorphologicalprocesslinked withConnectedComponentLabeling(CCL)

formatching stage, which is used to subdivide the desire image into various objects and forthe objectcatalogue construction the SpeededUp RobustFeatures (SURF) isutilized.Based on this method, it has the ability to detect the copy-move forgery beneath variousgeometricalattacks andoutcomes shownbetter executiontime andaccuracy.

In digital life the digital image forensics detection is the main task in research field.Therefore Zeinab F. Elsharkawy *et al* [20] proposed a blind tampering detection approach;it is based on the homomorphic image processing for the images taken from the scannersand cameras. Moreover the classifiers such as Support Vector Machine (SVM) and NeuralNetwork (NN) [21] are used for the tampered images classification which depends upon theclarification of the component. The performance of the classifier is shown by the ReceiverOperating Characteristic (ROC) method. The SVM classifier attained better accuracy at96.93%forthe detectionand proved fasterthan theotherclassifiers.

In image forgery the influenced images are visually identical from the real image, itis difficult to detect. From this reason, Jawadul H. Bappy *et al* [22] proposed a Convolutionneuralnetwork(CNN)architecturewhichishigh-confidenceinfluencelocalizationwhichis utilized by features of resembling, Long-Short Term Memory (LSTM) unit; also anencoder-decodersystemtosectionout forgery regionsfromnotinfluencedones.Thedifferent types of forgeries such as copy-move, splicing and object removal can segmenteffectively.

Theimageusagesintoday'slifeareincreasingsothecopy-moveforgeryconsequently occurs. Therefore, Behnaz Elhaminia *et al* [23] proposed a Markov RandomFiledbasedCMFDapproach.Theforgedareaisdetectedeffectivelyandwithbetteraccuracy by this method of approach. The energy function is minimized by using IteratedConditionalModes (ICM)algorithm, whichis straightforwardnessandefficient.

Table1.Performancecomparison ofdifferenttechniques

COPY MOVE FORGERY DETECTION BASE HYBRID METHOD

The main aim of the image forgery detection is to develop techniques to determine the authenticity and integrity of digital images with the support of automatic detection technologies based certain image processing techniques. In this research forgery detection based copy move key based techniques is implemented to classify the forgery images. Copymove forgery is the process of copying and pasting from one segment to another segment within the same image. In this section copy-move forgery detection based hybrid method includes neural network and decision tree to classify the forgery image. The flowchart for proposed GARIC is shown below in Figure 5.1.

The input image undergoes preprocessing, feature extraction and similarity matching for efficient classification. Initially, the input image is preprocessed by Prewitt & MM type filter to remove the noise and to improve the image quality. The feature vector from the preprocessed image is extracted by Speeded-up Robust highlights (SURF) the process is further improved by applying the Principal Component Analysis (PCA). The similarity matching for feature vectors by Manhattan distance to identify the exact match of the original image. The matched image is trained by Hybrid integration of Neural Network and Decision Tree (GARIC) to classify the forgery image.

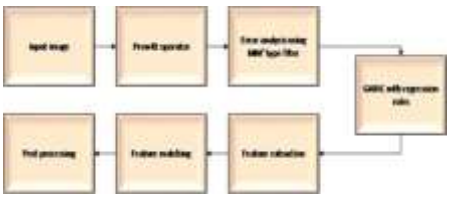

Figure :Block diagram for GARIC

PREPROCESSING BY PREWITT & MM TYPE FILTER

Pre-processing is the method of reducing the background noise and to enhance the image contrast and visual appearance. It also includes the process of image resizing and RGB to grey conversion to enhance image features by eradicating the unwanted distortions. Mainly pre-processing is employed to improve the background image contrast as well as blurringfrom the degradation function so that the feature extraction became more consistent. Prewitt MM type filter is chosen to smoothen the input image with variance change so reduce salt and white addictive noise .

Prewitt & MM type filter is mainly utilized in the frequency domain which is the process of the Mean Squared Error (MSE) optimal stationary linear filter for images which is corrupted by additive noise and blurring by the hypothesis of the signal and noise process which are 2nd order stationary. The effect of noise distribution has not been considered in the inverse filter operation.

III. RESULTS

In this project, the proposed method based on GARIC deep learning algorithm compared with the other schemes proposed by other authors to obtain better performance. The proposed CMFD is evaluated under the performance analysis of pression, recall and F1 measure. This method works properly when the tampered area is altered by scaling and rotation. Here the precision , recall and accuracy of proposed method based on fuzzy system is implemented on python.

The performance analysis of the proposed CMFD based on GARIC algorithm is done by using three parameters like Precision, Recall and F1 measure.

- True positive t_p : The number of forged images that are detected correctly as forged.
- True negative tn : The number of original images that are detected correctly as original.
- False positive f_p : The number of original images that aredetected erroneously as forged.
- False negative f_n : The number of forged images that are detected erroneously as original

(a)

(b)

(c)

(d)

Fig7.(a)originalimage(b)forgedimage(c)resiged image(d)cropped image.

Belowtablesshowstheperformanceanalysia(pression,recall,F1measure)ofproposedmethodbasedon GARIC.

Methods	Precision(%)	Recall(%)	F1-measure(%)
ZernikeMoments[27]	88.37	79.17	83.52
Combinedfeatures[28]	81.82	93.75	87.38
A-KAZE and SURF Features [29]	91.76	97.50	94.54
Proposed method	**95.38**	**98.15**	**96.75**

The proposed approach is implemented in Python. Experimental evaluation depicts that the proposed CMFD approach obtains better performance based on Precision, F1-measure, and Recall. Thus the proposed CMFD approach obtains the precision of 95.38%, recall of 98.15%, F1-measureof 96.75% and an improved Accuracy of 98.82% than the other state-of-art techniques

IV. CONCLUSION

Inthissummary,theworkcontributestoward stheareaofforgerydetectiontechniques in much number of ways. The forgery detection techniques categorized on thebasis of modelling methods and different approaches. In image segmentation, the copymoveforgerdregionsaredetectedmainl ybycomparingthekeypointsextractedinthe image. The most important challenges in this CMFD are the robustness in front of all typesof attacks, improving the slow feature learning rate and development of robust statisticalfeatures. CMF in digital images leaves edges or little spikes. Edge detection, error analysis,and deep learning mechanism are to be performed to identify the falsificationin digitalimages.

The feature work must overcome the obstacles by the development of more reliableand robust detection algorithms. In this research for the edge detectionPrewitt operator isdeveloped to make the edge detection operation as powerful as designed MM1 type filter(Double-m-derivedfilter)forerroranalysis.Subsequentl y,deeplearningalgorithmsmaybe considered with regression rules for feature extraction, to improve the learning rate, toreducethecomputationalcomplexity,feat urematchingandpost processing.

REFERENCES

[1] Ulian,D.M.;jalab,H.A.;wahaba.AW. A.;Shivakumar,p.;Sadaghi,S“Anovel forgedblurredregiondetectionsystemf orimageforensicapplications”,Exp.Sy st.Appl,64(2016):1-10.

[2] Stanton, Jamie,KeigoHirakawa,andScottMcCl oskey."DetectingImage ForgeryBased On Color Phenomenology." Proceedings of the IEEE Conference on ComputerVisionand Pattern Recognition Workshops(2019).

[3] Savitavalia,andKrishnakumar."Digit alimageforgerydetection:asystematic scrutiny."Australian journal of forensicsciences(2018).

[4] HussainMirandsabamushtaq."Digital imageforgeriesandpassiveimageauthe ntication techniques”: A survey, International journal of advanced science andtechnology,vol73 (2014): 457-463.

[5] Jalab, Hamid A., et al. "New Texture Descriptor Based on Modified Fractional EntropyforDigitalImageSplicingForg eryDetection."Entropy21.4 (2019): 371.

[6] Mohamed M. Dessouky, Mohamad A .Elaskily and Heba A.Elnemr "Two stages objectrecognitionbasedcopy-moveforgerydetectionalgorithm."Mu

ltimediaandapplications.Springer 78.11(2019):15353-15373

[7] Khaled W.Mohamad, Arwa Husien Abu Al-Rukab, “Moment based copy move forgeryindigitalimages”,ForensicScienceInternational214 (2012):33-43.

[8] Tiegang Gao, Yanjun Cao, Li Fan and yang "A Robust detection algorithm for Copy-MoveForgeryDetectionExploitingStatisticalImageFeatures."DigitalImage Forensics.Springer, Singapore(2020): 57-64.

[9] Khaled W.Mohamad,Arwa Husien Abu Al-Rukab, “ Moment based copy move forgerydetection methods”, International journal of computer science and information security,14.7(2016):28-35.

[10] Huynh KV, Huynh TK, Le-Tien T, Nguyen SC , “A survey on image forgery detectiontechniques”, IEEE RIVF international conference on computing and communicationtechnologiesResearch ,Innovation ,andVision forFeature(RIVF),(2015).

[11] A.makandar,B.Halalli,“Areviewpaper onprocessingtechniquesfordigital mammographyimages”, Internationaljournalofcomputerapplications(2015):887-975.

[12] A.Pwan,M.Barah,“Asurveypaper onthefeatureextractionmodelofoffline handwriting character recognition”, International journal of computer engineering andapplications.(2014):51-60.

[13] MahadianB.saicS,“Detectionofcopy-moveforgeryusingamethodbasedonblur momentinvariants“,ForensicSciInt(2007)171:189,.

[14] Malathi,J.,andNarasimhaSwamy."ImageForgeryDetectionbyUsingMachineLearning." International Journal of Advanced Science and Technology. 127.1 (2019):105-108.

[15] Jaiswal, Ankit Kumar, and Rajeev Srivastava. "Image Splicing Detection using DeepResidualNetwork."Availableat SSRN 3351072 (2019).

[16] J.Li,X.Li,yang.B,X.sun,:“Segment-basedimagecopy-moveforgerydetection scheme”,IEEETrans.Inf.ForensicsSecur.10.3(2015):507-518.

[17] Sexena.N,Guptha.A,vasisthaS.K., “Detecting copy- move forgery using DCT”,Int.j.Sci.Res.publications.3.5(2013):3-6.

[18] Jagan.D,Sunil.K,Shaktidev.M,“DCT-PCAbasedmethodforcopy-moveforgerydection”.ICT and critical infrastructure: proceedings of the 48th annual convention ofcomputersocityofIndia,vol.2 :577-583.

[19] Prakash, Choudhary Shyam, et al. "Detection of copy-move forgery using AKAZE andSIFTkeypoint extraction."MultimediaTools andApplications(2019): 1-24.

[20] Elsharkawy, Zeinab F., et al. "New and efficient blind detection algorithm for digitalimageforgeryusinghomomorphicimageprocessing."MultimediaTool sandApplications(2019): 1-27.

[21] JianghongZhou,JiangquiNi,YunaRao,“Block-Basedconvolutionalneuralnetwork forimageforgerydetection”Springerinternational publishing.10431(2017):65-76.

[22] Bappy,JawadulH.,etal."HybridLSTM andEncoder–DecoderArchitectureforDetection of Image Forgeries." IEEE Transactions on Image Processing 28.7 (2019):3286-3300.

[23] Elhaminia,Behnaz,AhadHarati,andA

mirhosseinTaherinia."Aprobabilisticframeworkforcopy-moveforgerydetectionbasedonMarkovRandomField."MultimediaTools and Applications (2019): 1-19.