IJCAT - International Journal of Computing and Technology, Volume 7, Issue 10, October 2020
ISSN (Online) : 2348-6090
www.IJCAT.org
Impact Factor: 0.835

Dbelm for Image Forgery Detection

[1] Arun Anoop M; [2] Poonkuntran S

[1] PhD Scholar, Department of Computer Science and Engineering
Velammal College of Engineering & Technology
Madurai, Tamilnadu, India

[2] Professor, Department of Computer Science and Engineering
Velammal College of Engineering & Technology
Madurai, Tamilnadu, India

Abstract – Image forgery or manipulation is the removal of interested region from the particular image by the use of freely available manipulation tools. One of the popular attacks is copy move forgery attack. Main aim of image forgery is to hide the interested region or reproducing new region in that particular image in order to falsify the particular image for publicity or saving their individual from danger or fame or earns or cheat or fun An 'Alexnet based Convolutional Neural Network(CNN)' is intended for picture fraud discovery. As the accuracy parameters resulted same in the case of one attack consideration in previous methodologies, this framework concentrate copy move attack and splicing attacks. The experiment results proposed DBELM outperforms existing CMFD frameworks by a significant edge on the five freely available datasets: MIASDBv1, CASIA, CoMoFoD, Kodak & Google and MNIST handwritten dataset. For primer evaluation, MNIST dataset initially processed to check classification accuracy by CNN based on different splits and not processed by DBELM. That motivation helped us to take 90:10 split for DBELM research work. Novelty of the work is the design and implementation of proposed system, and moreover the review of previous algorithm(s) in the area of feature extraction, which aims to explore the different extraction methods, feature determination which is utilized for dimensionality reduction to eliminate repetitive and immaterial features, classifiers which are utilized for supervised or unsupervised machine learning and metrics which are the measures or parameters or accuracy improving methods for evaluation. A small % of accuracy improvement will help to cure patient's health from danger if the important document is altered. And also we located the forged region with the help of moment based algorithm (Zernike Moment) and used bat optimized extreme learning machine for better image forgery classification accuracy. An accuracy of 98% has been accomplished for the four datasets. Proposed framework demonstrates the credibility of the digital image from forgery. For better evaluation, review about all the related terms, comparative results and performance evaluation results are included. And the DBELM outperforms our previous methodologies LORA and LPG. In future, DBELM will process MNIST handwritten dataset and compare with DELM-AE, DELM & DBP methods and find out the best one among those for image forgery detection research field.

Keywords-*Image forgery and detection; BAT ecology algorithm(BAT); Extreme Learning Machine(ELM); Alexnet based Deep CNN; Copy Move Forgery Detection(CMFD*

1. Introduction

Image forgery or manipulation is the forging of region from the some image and pasting it into some other. Image Forgery attacks and detection methods mentioned in the previous papers[1-5]. Image forgery or manipulation is the forging of region from the some image and pasting it into some other. Here we compared the performance of different methods utilized in the approach. Alexnet was originally introduced by Alex for the purpose of image classification. Image forgery or manipulation or alteration normally happening between one person to another person data communication. It may be by third party between two persons. To secure communication between two individuals, there is a need of image authenticity framework or protocols. Two types of attacks are active and passive attacks[1]. Physicians always depend digital images for diagnosis, in these cases, forgery must notice before diagnosis process. If any kind of forgery in the particular document related to patient, will lead patient's life in trouble that may lead him socially down. And this problem is big challenge for digital image authenticity. The results achieved surpass the earlier work in this area mainly Precision, Recall, F-measure and Classification accuracy. A new forgery detection method based on deep learning CNN with BAT-ELM was presented, and was shown to produce good result in forged region localization and accurate detection. But before moving to optimization algorithm we have processed collected features based on banding and sub-banding process in the previous methodology as we mentioned in our LPG[1] and same mentioned in the below Fig. 7. But in this DBELM approach, we have not followed any banding and sub-banding process; we have processed CNN algorithm to extract features "feature map", for further investigation analysis work. The major problem we identified is the existing methods lacking some dimensionality reduction method, which causes accuracy in terms of classification and epochs have the great contribution to get more accuracy in the experiments. Most intelligent methods have been made by several authors using Alexnet architectures. Furthermore, this work is also limited by its consideration of different datasets processing for forgery detection. Since several issues remain in unaddressed, future directions are related to the improvement of the boosting of accuracy in terms of different kind of forgery attacks and classifiers on different datasets.

In this process identify the forgery image in genuine. Here we use CNN for extract the feature map, using BAT optimization

to select the best feature and using ELM to classify the authenticity of the image. Here we use the genuine image to training sets, and give the input image it is in train database it is genuine else it is forgery for typical dataset. And finally we have calculated 'Precision, Recall , F-measure and also evaluated based on different kind of splits' that's 70:30,80:20 and 90:10 training and testing splits.

Recently, there are lots of researchers are going on in "the field of image forgery detection", Fig. 1, specifies the clear picture of recent researches in the area we specified.

Here we proposed an accurate classification method for image authenticity proving which relies upon joining the quality of two methods. To begin with, deep learning strategy alexnet based feature extraction. Second, a feature determination strategy BAT calculation handled and supplanted softmax by ELM classifier that is last fully connected (fc) layer of the Deep CNN is connected to ELM. In this work, we proposed a technique for picture falsification based group cation(binary characterization). The proposed technique removes the features from unique and manufactured pictures utilizing Alexnet based deep CNN. At that point the separated features are isolated into testing and training sets. Followed by utilizing the BAT calculation to lessen these features and eliminate the excess and insignificant features. This cycle accomplished by best feature set choice and the ELM classifier which sorted either authentic or not.

The main contributions of this research work are the following:

1. Proposed a "Genuine(or)Forgery classification method(Figure 9)" which depends on the "CNN based feature extraction" and "BAT feature selection technique(Section IVc.)".
2. Inferring another arrangement of feature vector, Alexnet based CNN , to extricate the features from the first and phony pictures.
3. Set parameters of BAT feature selection method for evaluation of best features from extracted features to boost classification accuracy.
4. Evaluate the performance of the proposed DBELM using $D^{1,2,3,4}$. As same attack results same Precision, Recall considered more than one attacks for evaluation process.
5. Compared the results with other methods.

We considered some splits name for our research work and based on their ratios used for evaluation purpose. That names and details, mentioned in Table. II.

The organization of this paper is as follows. In Section 2, Related works about some subsections arranged, Section 3, the proposed $_{algorithm}$, $flow_{diagram}$ & working details, Section 4, Experimental analysis and Results based on splits and previous methods and Finally, the paper concluded in Section 5.

2. Related works

Digital image forgery detection comes under "digital-image-forensics" and for image authenticity proving. There are lots of digital image forensics available, some fields are normally forgery in audio, video, voip, social media.

A. IEEE year wise statistics

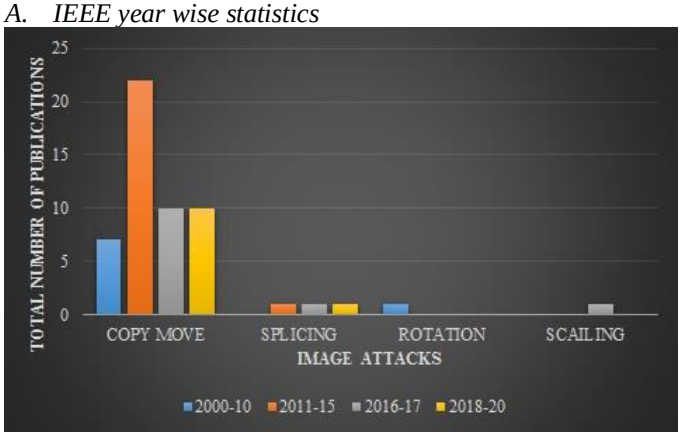

Figure 1. Study about Image Forgery in IEEE

B. Attacks in Image Forgery

The template Main attacks in the area are in the Table 1 which is noted below,

Table I: Image Attacks detailed Description

Image Attacks	Description
COPY-MOVE	Copying a region from anywhere in the same image and pasting it into any desired part in the same$_{image}$[1].
SPLICING	It is image compositing attacks, which is combinations of images, that's merging of different images fused to and form a new innocent image[1].
ROTATION	Finding out the region which is interested by the manipulator , rotate and form a new innocent image[1].
SCALING	Finding out the interested region and scale and form a genuine looking innocent image[1].

Details of these attacks are mentioned in [1-4].

C. Training and testing splits and details (Used in research methodologies)

Table II: Training and testing splits and details

Splits	Details
70:30	Revenue split[4]
80:20	Pareto Principle[2]
90:10	Warren Buffet's Rule of thumb[DBELM]

D. Datasets(A brief existing summary)

Table III: Dataset and details

Dataset Name	Web source Details
CASIA V1,2	[64-65]
NB-CASIA	[66]
USC-SIPI	[67]

CoMoFoD	[68]
RAISE	[13]
Dresden	[19]
Kodak and Google	[69-70]
MICC-F220	[71]
GRIP	[72]
FAU	[73]
SMIFD	[74]
WILD WEB	[75]
PS-Battles	[76]
COVERAGE	[77]
Columbia Image Splicing	[78]
FFCMF	[79]
OICIO	[80]
Deepfakes	[81]
DDSM	[82-83]
CBIS-DDSM	[84]
MIASDBv1	[85]
Chest x-ray	[86]
Novel CORONA virus	[87]
DRIVE	[61]
MESSIDOR	[62]
STARE	[63]
CATARACT	[88]
Glaucoma(RIGA)	[89]

E. Image Forensics and processing methods(A brief existing summary)

Table IV: Image Attacks detection methods detailed Description

Image Attacks detection Tools	Description
ELA	Error Level Analysis is an Image Forensics Tool[1].
GAN(Generative adversarial network) Descriminator	AI based fake face generation. One of the motivations to us to do Image forgery detection research. GAN based fake face generator and descriminator. Lets have a look on some websites, 1) https://thispersondoesnotexist.com/ 2) https://www.whichfaceisreal.com/ 3) https://generated.photos/ 4) https://deepfakesweb.com/ 5)[60].
Reverse Image Search	https://tineye.com/
Metadata view tool	https://www.verexif.com/en/
Poisson Image editing	Gradient domain image processing.
Attentional heatmap.	Method in Image processing.
Key point based methods	SIFT,SURF
Block based methods	HOG,GLCM,ZM,LBP,WLD
Hybrid methods	Combination of more than one algorithms. Example is LPG[2].

F. Based on Feature extraction algorithms and related terms (A brief existing summary)

Table V: Feature Extraction Algorithms

Algorithms	Description
HOG[48]	Histogram of Gradient
GLCM[45]	Gray-level Co-ocurrence Matrix
ZM	Zernike Moment
LBP[49] is Local Binary Pattern.	
CNN	ConvolutionalNeuralNetwork
WLD	Weber Local Descriptor
Hu Moment	Moment based feature extraction.
DCT is Discrete Cosine Transform , FMT is Fourier Mellin Transform & DWT is Discrete Wavelet Transform	
BRAVO	Intensity based techniques
CIRCLE	
LUO	
Key point based Image Forgery detection methods are , scale-invariant feature transform,SIFT[50], Speeded up robust features(SURF)[50], Fast Retina Key-point(FREAK Descriptor), Binary Robust Invariant Scalable Keypoints(BRISK Descriptor).	
FAST	Both are Local feature Descriptors. Features from accelerated segment test(FAST Descriptor). Binary Robust Independent Elementary Features(BRIEF Descriptor)
BRIEF	
ILBP[43] is “Improved Local Binary Pattern”. MBP[47] is “Median Binary Patterns”. LTP[46] is “Local Ternary Pattern”. ILTP[47] is “Improved LTP”.	
RLBP[47] is “Robust LBP”. SLBP[44] is “Soft LBP”.	
LBP-HF	LBP Histogram Fourier highlights
GLTP	Gradient LTP
FLBP is Fuzzy Local Binary Pattern	
NTLBP is Noise Tolerant Local Binary Pattern	
Haralick	[34]
Auto Encoder	[35]
GLDM & GLRLM are Gray Level Difference & Run Length Matrix.	
ANN	Artificial Neural Network.
RNN	Residual Neural Network.
Region based CNN	[38]
CONV	Convolutional layer.
POOL is Pooling layer[59] in CNN.	
ReLu Rectified Linear Unit and FC is a Fully Connected Layer in CNN[59].	

Softmax	[36]
Global average Pooling	[39]
Epochs	[40]
Stochastic gradient descent is iterative strategy for streamlining a goal function[41].	
ELBP	Extended LBP
MB-LBP	Multi Block LBP
VLBP	[42]
3-D LBP	Three dimensional LBP.
CS-LBP	[51]
Extended LBP	[52]
CLBP	[53]
RIFT	[54]
GLOH	[55]
Le NET	CNN Architectures
Alexnet	
Resnet	
GoogLe Net	
Inception	
Xception	
VGGNet	
CaffeNet	
DenseNet	
ConvNet	
SqueezeNet	
SGDM	[41]
ImageNet	Database.
ZfNet	Classic CNN.

3. Proposed System

New approach DBELM (Deep BAT Optimized ELM for Image forgery detection) approach is done by Alexnet CNN for feature extraction, and feature map processed with BAT ecology algorithm and ELM classifier. The examination work of the paper is to recognize the altered segment of the picture. The proposed work contains (i) Dataset of images (ii) Preprocessing (iii) Feature Extraction, (iv) Feature Matching (v) Forgery Localization. And Feature-Extraction is implemented based on Alexnet CNN.

G. Proposed algorithm

- Input image acquisition: The information images gathered from dataset storage such as MIAS, CASIA, USC-SIPI, Kodak and Google Images is considered as dataset for the proposed system.
- Preprocessing stage: Is for converting Color image to gray scale and Wiener filter is processed based on image quality. Wiener filter only used for bad quality images.
- Feature Extraction: Extracts the features from the input images based on CNN. Three layers of <Conv,ReLu,Pool> used. Last FC is connected to ELM classifier. Output is binary classifier framework which results either original or Forged.
- Forgery Localization: Forged region is located by moment based feature extraction algorithm Zernike moment.
- Best Feature vector production: Best features calculated by BAT ecology algorithm.
- Classification process: And best features finally processed by ELM classifier and produced better classification accuracy, based on its ratio system classified how many images are genuine or forged.

H. Proposed Flow diagrams

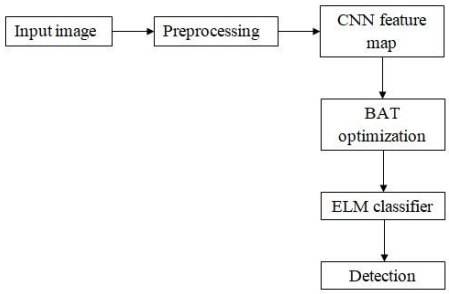

Figure 2. DBELM Approach (Block diagram of Proposed System)- General Proposed System without Localization.

In Figure 2., is a general proposed flow without forged region localization. In below added a Figure 3., which consists of forged region localization.

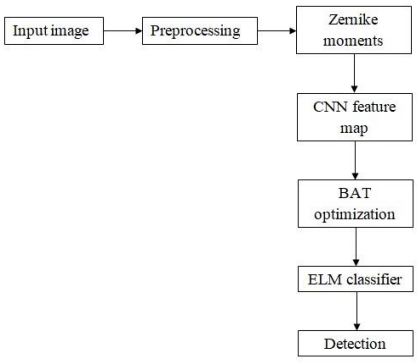

Figure 3. DBELM Approach (Flow of Proposed System)- General Proposed System with Localization of forged region.

In Figure 7., general architecture redrawn based on layering approaches of Convolutional neural network (CNN), Fully connected Layer(FC) and binary classifier which categorize either 1 or 0, Extreme Learning Machine(ELM). Figure 8., is combined with BAT optimized ELM classifier.

Working Mechanism: Input image is processed and resize is done in the pre-processing stage. Feature extraction depends on {Iw X Ih X Ic X K}, where, w is width, h is height, c is number of filters in every layer and K is number of collected samples. CONV1 followed by max pooling and rest two followed by average pooling. BAT ecology algorithm used for features reduction. Finally ELM, a binary classifier used to classify original(1) or Forged(0). For feature extraction, three CONV layers used and produced feature maps. For feature matching, ELM classifier used.

Datasets used are MIASDBv1[21] which consists of 322 original images(both healthy and unhealthy breast cancer images, which is in PGM format, converted to JPEG for research purpose). We formed 322*2=644 Forged images by duplicate move and grafting assaults for picture fabrication recognition assessment measure. CASIA V1 dataset comprises of 800 unique and 921 fashioned pictures. CASIA V2 dataset comprises of {7421 unique and 5123 produced} pictures. From CASIA V2, have chosen {1000 original and 1000 forged}. CASIA dataset[14] total of 1800 original and 1921 forged formed. CoMoFoD[12] dataset chosen 200 original and 400 forged images. In Kodak and google, original of 40 and forged of 80 from Kodak and google dataset forming is mainly concentrated some random selection from Flickr dataset, a total of 50 original and 100 forged collected. Finally MNIST handwritten digits dataset[37] collected and processed with CNN program and check the accuracy, chosen as primer research activity before setting up proposed system.

J. LPG[2], our previous methodology,

I. Description of layers in Proposed CNN structure

Table VI: Proposed CNN structure details

Layers	Description
Image	Input Image
Preprocessing	Resize the input Image
Feature Extraction	CONV1, ReLu1, Max Pooling1; CONV2,ReLu2, Average Pooling2; CONV3,ReLu3, Average Pooling3. Extracted features. Collected and visualized the feature maps.
FC	Fully Connected layers, FC1 and 2.
Optimization	BAT ecology optimization algorithm for best features.
Classification	Extreme Learning Machine classifier outputs either 1 or 0.

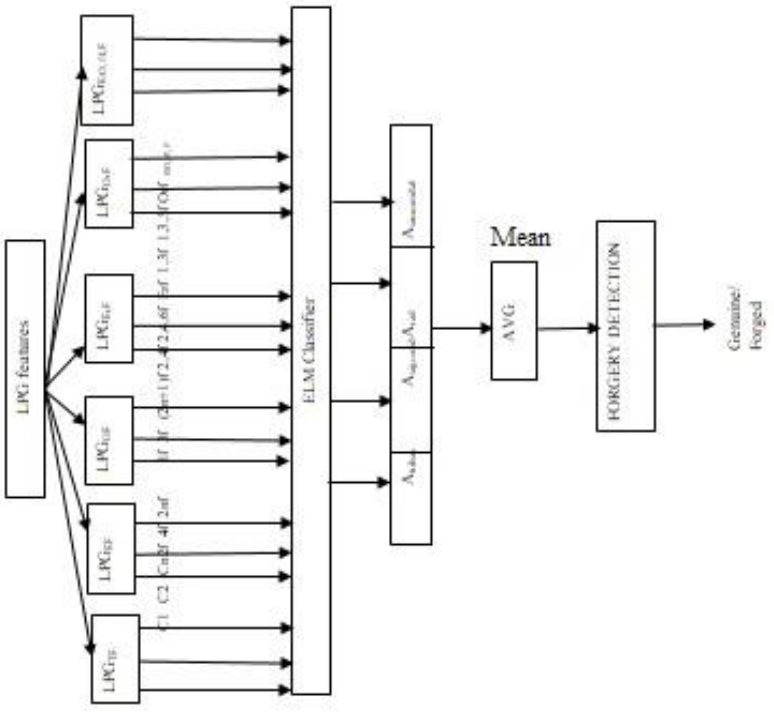

Figure 4. Banding and sub-banding concept of LPG

K. Dataset and digital image attack(s):

Figure 5. Dataset Images

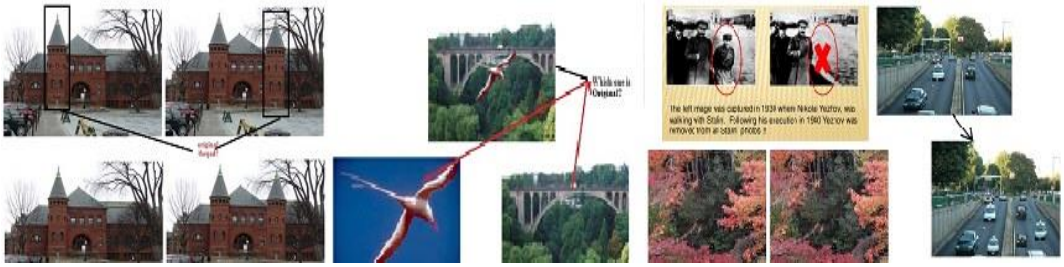

Figure 6. Attacks in Digital Images(Copy move$_{single\&multiple}$ forgeries; Splicing attack)

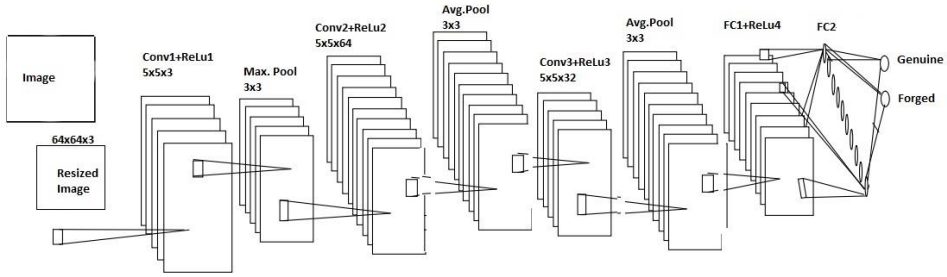

Figure 7. Proposed System general diagram

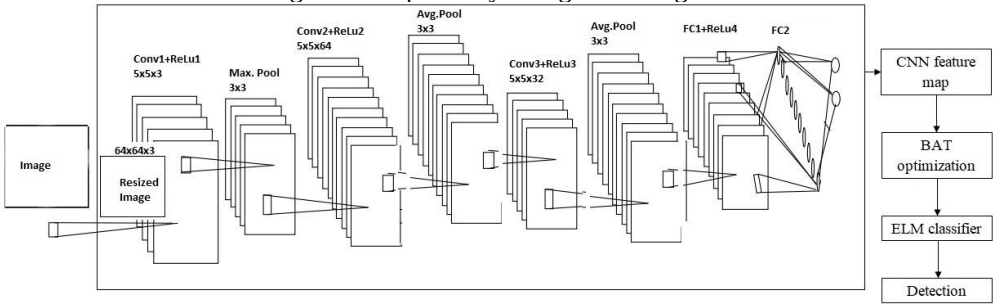

Figure 8. Proposed System BELM

L. Requirements for Proposed system:

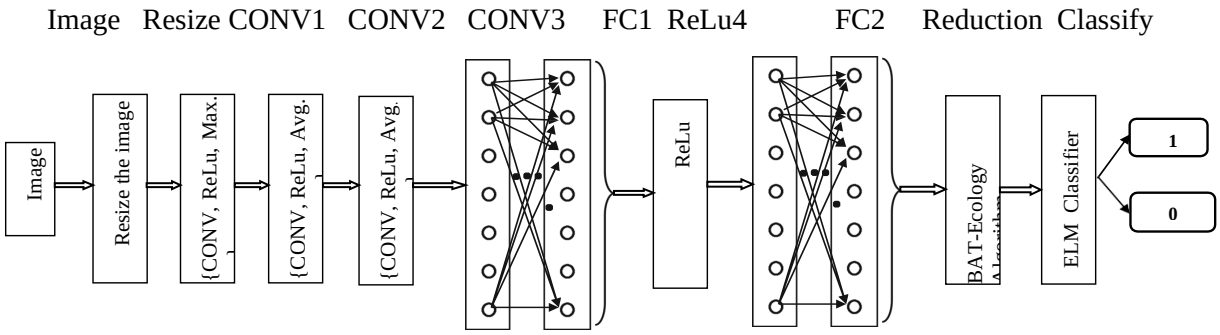

Figure 9. DBELM for Image Forgery detection

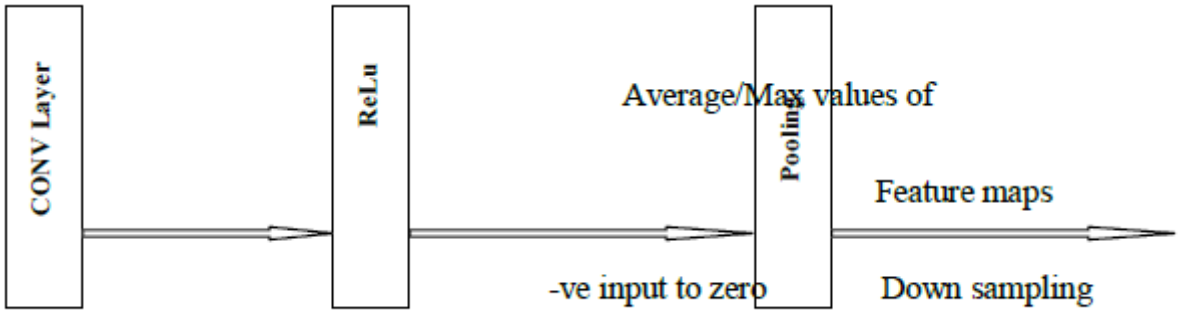

Figure 10. Layers of CNN for Image Forgery detection

4. EXPERIMENTS AND RESULTS

This part gives the assessment of results acquired by DBELM proposed strategy for picture phony discovery. Gotten results are contrasted and various splits of training, testing pictures. The investigations have been executed on a machine with Intel center i3, GPU NVIDIA driver, 64 bits-processor; 4 GB RAM, working by Windows 10. The proposed calculation is actualized by MATLAB 2020 trial version for DBELM implementation. And Python 3.8.5 and Jupyter Notebook for MNIST handwritten digits classification using CNN as primer research.

A.Dataset description

Table VII: Dataset description

Dataset Name	$^{*}C_{Original}$	$^{+}C_{Forged}$
MIASDbv1(D^1)	322	644
CASIA(D^2)	1800	1921
CoMoFoD(D^3)	200	400
Kodak and Google(D^4)	90	180
Total Images	*2412*	*3445*

Where, $^{*}C$ or ^{+}C denotes count.

BMetrics used are,

- Precision, P: Probability that a detected region is truly a altered[4].
  $Precision_{(P)}=\{Tp/(Tp+Fp)\}$ (1)
- Recall, R: Probability that a forged region is located[4]
  $Recall_{(R)}=\{Tp/(Tp+F_N)\}$ (2)
- $F1_{measure}$:Combination of above two[4]
  $F_m=\{(2*P*R)/(P+R)\}$ (3)

We considered 'Classification accuracy': the mean of accuracy in terms of ELM
Classifier's Activation functions.

Below 1,2,3,4 denotes based on image forgery detection[4],

- Tp is the $Number\_of\_altered_{Image}$ that are truly detected as $tampered_{images}$.
- Fp is the $Number\_of\_Original_{Image}$ that are falsely detected as $tampered_{images}$.
- F_N is the $Number\_of\_altered_{Image}$ that are falsely detected as $original_{images}$.
- T_N is the $Number\_of\_Original_{Image}$ that are truly detected as $original_{images}$.

M. BAT Ecology Algorithm

BAT[6-8] algorithm is metaheauristic algorithm for worldwide optimization. It was motivated by the echolocation conduct of micro-bats, with changing pulse paces of discharge and commotion. The Bat algorithm was created by Xin-She Yang in 2010.

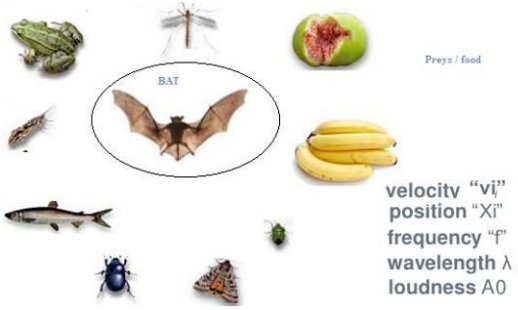

Figure 11. BAT and preys
(BAT food source:[58])

The term 'Echolocation'[8] is,

Initially	: Virtual bat
Flies	: Randomly
Conditions	: {vi at xi with a varying ff or ƛ & A0}.
What they do	: {Search {Prey or food};Echoes for *Dr & *Di}
Finds	: It adjusts { ff , A0 & 'pulse-emission-rate{r}'}.
Loudness varies	: {A0 to Amin}

Where, Dr is direction, Di is Distance.

BAT optimization algorithm[6-8] selects the optimal or best features from the feature vector of proposed CNN and those features processed for training and testing pair with the help of ELM classifier for original and forgery classification.

The advantages of using the BAT algorithm[8] is it is very efficient, frequency is tuned randomly and, gives promising optimal arrangements and functions admirably with muddled issues. Also, additionally best advantage of BAT algorithm is automatic

parameter tuning it is essential to work with complex problems in any area.

BAT Psuedo code(Based on[8]):

1) Start
2) Initialize the neurons (BAT)
3) Initialize the Loudness, frequency, Pulse rate, velocity
4) Evaluate the fitness function
5) Calculate the best value
6) Calculate the classification accuracy(Ac)
7) Stop Criterion
   If Ac<At
   Select best features
   Update the loudness, Frequency,Pulse rate, velocity
   else

goto step 3 and repeat it until to reach best match results.

8) End.

N. ELM Classifier

ELM algorithm based on proposed algorithm:

- Input : Feature map generated by CNN three layering mechanism
- Activation function : Based on ELM kernels are Tribas, Sigmoid, Rad, Sinusoidal
- Number of hidden nodes : We have selected 30 hidden nodes for entire research work. And the details regarding the hidden nodes we mentioned clearly in [2].
- Output : Binary Classification [1/0] that's [Genuine/Forged].

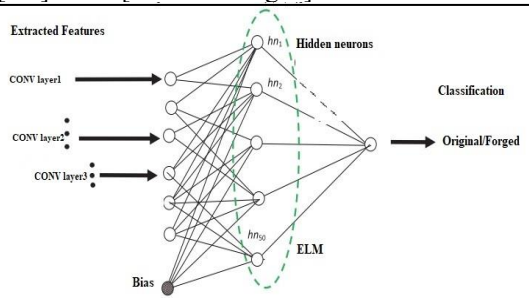

Figure 12. Modified ELM Classifier for DBELM[90]

BATELM based on proposed algorithm:

- Input :Image Acquisition.
- Pre-processing :RGB to gray conversion. If quality less, go for noise filtering and resizing image.
- Feature Extraction :Feature maps.
- Training and Testing :Splits rules.
- Feature Selection :Fitness checking for best optimal features selection.
- BAT feature selection :Set parameters for proposed algorithm.
- Stopping criterion :Classification Accuracy less than Threshold value.
- ELM Classifier : Check with activation function, hidden nodes and kernels. If output is 90%, Genuine is 90 out of 100.

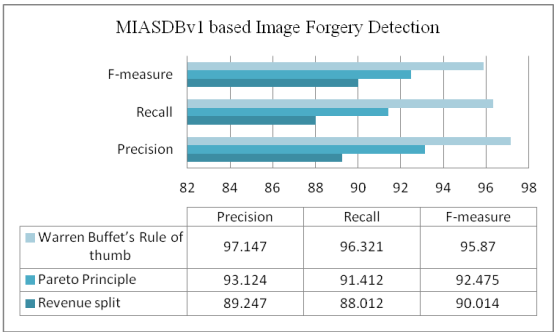

Figure 13. Splits compared of D[1]

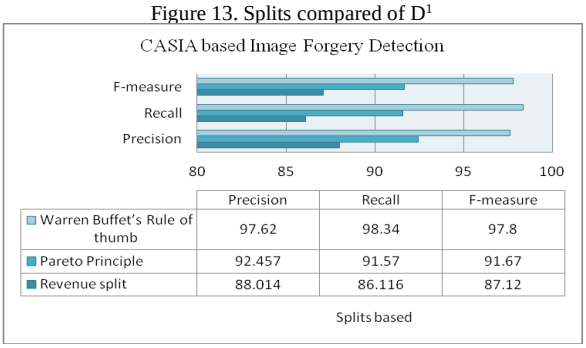

Figure 14. splits compared of D[2]

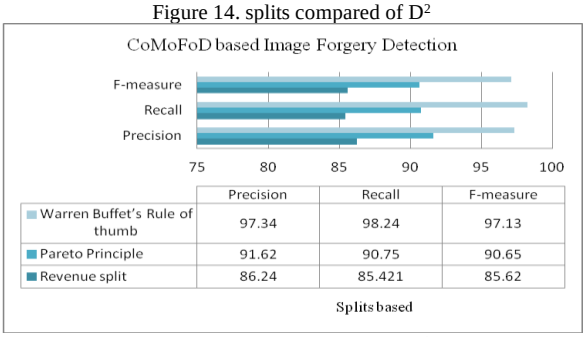

Figure 15. splits compared of D[3]

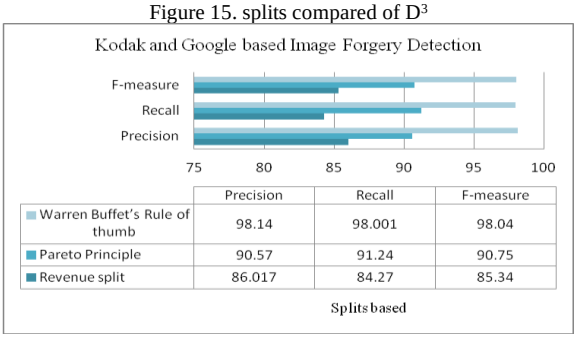

Figure 16. splits compared of D[4]

In table 7., dataset details and count of images we taken for evaluation to detect image forgery. In table 8.,we evaluated Precision, Recall and F-measure based on splits. Splits details mentioned in Table 2. Suppose split is 90:10 denote the ratio of training and testing.

As metrics shows same results in the case of copy-move forgery, considered other attacks also.

From the above Figure, for the different datasets the image forgery detection exactness for the proposed model has been kept up between the 98% to 96% in 90:10 split, whereas the other splits algorithms varies from 93 % to 94% for the CNN trained with BAT-ELM respectively. Hence the proposed

model has better efficiency in the accuracy of detecting the different image forgery systems.

Traditional Methods	Accuracy (%)
FCID-HIST [89]	76.33
FCID-FE [89]	79.22
BusterNet [90]	78.00
LORA+ELM[3]	85.12
LPG+ELM[4]	88.61
LPG+BAT+ELM[4]	96.01
Proposed System	98.00

5. CONCLUSION

Authenticity expectation of a picture has ended up being basic these days in each field. Trial results have indicated that this technique gives high classification accuracy regarding various splits as we considered all through our exploration work. In the tests, the proposed technique beats some current strategies for our past exploration approaches and furthermore conventional techniques. Among four classifiers ELM demonstrated as productive in work with high classification accuracy rate. With BATELM algorithm, accomplished 98%. In future, we will do likewise with some auto-encoders ideas with various epochs.

REFERENCES

[1] Mr.Arun Anoop M,"Review on Image forgery and its detection",ICIIECS,2015,IEEE,10.1109/ ICIIECS.2015.719 3253
[2] Arun Anoop M, Poonkuntran S,"Certain investigation on Biomedical impression and Image Forgery Detection," International Journal of Biomedical Engineering and Technology , DOI:10.1504/ IJBET. 2018. 1 0023469 unpublished
[3] Arun Anoop M, Poonkuntran S,"LORA APPROACH FOR IMAGE FORGERY DETECTION AND LOCALIZATION IN DIGITAL IMAGES", CnR's International Journal of Social & Scientific Research, India, Vol.04 Issue (III) ISSN: 2454-3187,Jan2019.
[4] Arun Anoop M, Poonkuntran S,"LPG-A NOVEL APPROACH FOR MEDICAL FORGERY DETECTION IN IMAGE TRANSMISSION," Journal of Ambient Intelligence and Humanized Computing (2020), DOI: 10.1007/s12652-020-01932-0
[5] Arun Anoop M, Dr.S.Poonkuntran, Dr.V.Vasudevan, Dr.P.Alli,"Study of the importance of digital forensics and deep learning tools", International Journal of Advanced Science and Technology ,Vol. 28, No. 20, (2019), pp. 963-978
[6] J. D. Altringham, Bats: Biology and Behaviour, Oxford University Press, (1996).
[7] P. Richardson, Bats. Natural History Museum, London, (2008)
[8] Yang, X. S. (2010). "A New Metaheuristic Bat-Inspired Algorithm, in: Nature Inspired Cooperative Strategies for Optimization (NISCO 2010)". Studies in Computational Intelligence. 284: 65–74.
[9] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, G. Serra, A SIFT-based forensic method for copy-move attack detection and transformation recovery, IEEE Trans. Inf. Forensics Secur. 6 (2011) 1099-1110.https://doi.org/10.1109/TIFS.2011.2129512.
[10] H. Farid, Photo Tampering Throughout History, [Online] Http//Www. Cs.Dartmouth. Edu/Farid/Research/Digitaltampering. (2011).
[11] B. Wen, Y. Zhu, R. Subramanian, T.T. Ng, X. Shen, S. Win-kler, COVERAGE - A novel database for copy-move forgery detection,Proc. - Int. Conf. Image Process. ICIP. 2016-Augus (2016) 161-165.580 https://doi.org/10.1109/ICIP.2016.7532339.
[12] Dijana Tralic, Ivan Zupancic, Sonja Grgic, Mislav Grgic, CoMoFoD - New Database for Copy-Move Forgery Detection, 55th International Symposium ELMAR-2013, 25-27 September 2013,pp 49-54, Zadar, Croatia
[13] D.T. Dang-Nguyen, C. Pasquini, V. Conotter, G. Boato, RAISE - A raw images dataset for digital image forensics, Proc. 6th ACM Multimed. Syst. Conf. MMSys 2015. (2015) 219-224.https://doi.org/10.1145/2713168.2713194.
[14] CASIA Image Tampering Detection Evaluation Database, National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Science, available at: forensics.idealtest.org
[15] T. Ng and S. Chang, "A Data Set of Authentic and Spliced Image Blocks," Columbia University, Tech. Rep. 203-2004-3, January 2004
[16] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches," IEEE Transactions on Information Forensics and Security, vol. 7, no. 6, pp. 1841-1854, December 2012
[17] S. Battiato and G. Messina, "Digital Forgery Estimation into DCT Domain - A Critical Analysis," in ACM Multimedia Workshop Multimedia in Forensics, pp. 37-42, October 2009
[18] M. Goljan, J. Fridrich, and T. Filler, "Large Scale Test of Sensor Fingerprint Camera Identification," in SPIE Media Forensics and Security, vol. 7254, pp. 0I 01-12, January 2009
[19] T. Gloe and R. Böhme, "The 'Dresden Image Database' for benchmarking digital image forensics," in 25th Symposium on Applied Computing, vol. 2, pp. 1585-1591, March 2010
[20] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy-move forgery in digital images," in Proceedings of Digital Forensic Research Workshop, pp. 55-61, August 2003
[21] Suckling J, Parker J, Dance D, Astley S, Hutt I, Boggis C, Ricketts I, Stamatakis E, Cerneaz N, Kok S-L, Taylor P, Betal D, Savage J (1994) Mammographic image analysis society digit
[22] Yaseen ZM, Deo RC, Hilal A, Abd AM, Bueno LC, Salcedo-Sanz S, Nehdi ML (2017) Predicting compressive strength of lightweight foamed concrete using extreme learning machine model. Adv Eng Softw. https://doi.org/10.1016/j.advengsoft.2017.09.004
[23] Feng G, Huang G-B, Lin Q, Gay R (2009) Error minimized extreme learning machine with growth of hidden nodes and incremental learning. IEEE Trans Neural Netw 20(8):1352–1357
[24] I. Amerini, T. Uricchio, L. Ballan, R. Caldelli, Localization of JPEG Dou-ble Compression Through Multi-domain Convolutional Neural Networks,710 IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.Work. 2017-July (2017) 1865-1871. https://doi.org/10.1109/ CVPRW.2017.233.
[25] Q. Wang, R. Zhang, Double JPEG compression forensics based on a convolutional neural network, Eurasip J. Inf. Secur. 2016 (2016). https://doi.org/10.1186/s13635-016-0047-y.
[26] V. Verma, N. Agarwal, N. Khanna, DCT-domain deep convolutional neural networks for multiple JPEG compression classification, Signal Process. Image Commun. 67 (2018) 22-33.https://doi.org/10.1016/j.image.2018.04.014.
[27] Gu J, Wang Z, Kuen J, Ma L, Shahroudy A, Shuai B, Liu T, Wang X, Wang G, Cai J, Chen T (2018) Recent advances in convolutional neural networks. Pattern Recogn 77:354–377
[28] Kim D-H, Lee H-Y (2017) Image manipulation detection using convolutional neural network. Int J Appl Eng Res 12(21):11640–11646
[29] Liu Y, Yin B, Yu J, Wang Z (2016) Image classification based on convolutional neural networks with crosslevel strategy. Multimed Tool Appl 76(8):11065–11079
[30] Tran DT, Iosifidis A, Gabbouj M (2018) Improving efficiency in convolutional neural networks with multilinear filters. Neural Networks 105:328–339
[31] Zeiler MD, Fergus R (2014) Visualizing and understanding convolutional networks. European Conference on Computer Vision (ECCV), pp 818–833
[32] Akshay Agarwal, Richa Singh, and Mayank Vatsa (2017), Face Anti-Spoofing using Haralick Features, IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), DOI: 10.1109/BTAS.2016.7791171
[33] D'Avino, Dario & Cozzolino, Davide & Poggi, Giovanni & Verdoliva, Luisa. (2017). Autoencoder with recurrent neural networks for video forgery detection. Electronic Imaging. 2017. 92-99. 10.2352/ISSN.2470-1173.2017.7.MWSF-330.

[34] Liao, Bin & Xu, Jungang & Lv, Jintao & Zhou, Shilong. (2015). An Image Retrieval Method for Binary Images Based on DBN and Softmax Classifier. IETE Technical Review. 32. 294-303. 10.1080/02564602.2015.1015631.
[35] Fatahi, Mazdak. (2014). MNIST handwritten digits Description and using. 10.13140/2.1.4601.1681.
[36] Bao, Yu & Li, Haojie & Fan, Xin & Liu, Risheng & Jia, Qi. (2016). Region-based CNN for Logo Detection. 319-322. 10.1145/3007669.3007728.
[37] Elaskily, Mohamed & Elnemr, Heba & Sedik, Ahmed & Dessouky, Mohamed & El Banby, Ghada & Elaskily, Osama & Khalaf, Ashraf A. M. & Aslan, Heba & Faragallah, Osama & Abd El-Samie, Fathi. (2020). A novel deep learning framework for copy-move forgery detection in images. Multimedia Tools and Applications. 10.1007/s11042-020-08751-7.
[38] Maeda, Toshiyuki & Bryzgalov, Peter & Shigeto, Y. (2020). Impact of changes in the Mini-batch size on CNN Training Epoch Time. 10.13140/RG.2.2.19390.51521.
[39] Zhuo, Li'an & Zhang, Baochang & Chen, Chen & Ye, Qixiang & Liu, Jianzhuang & Doermann, David. (2019). Calibrated Stochastic Gradient Descent for Convolutional Neural Networks. Proceedings of the AAAI Conference on Artificial Intelligence. 33. 9348-9355. 10.1609/aaai.v33i01.33019348.
[40] Guoying Zhao and Matti Pietik¨ainen(2007), Dynamic Texture Recognition Using Local Binary Patterns with an Application to Facial Expressions, IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, 2007
[41] Kylberg G, Sintorn IM (2013) Evaluation of noise robustness for local binary pattern descriptors in texture classifcation. EURASIP J Image Video Process 1:17
[42] Kylberg G, Sintorn I-M (2016) On the influence of interpolation method on rotation invariance in texture recognition. EURASIP J Image Video Process 2016:17
[43] Girisha AB, Chandrashekhar MC, Kurian MZ (2013) Texture feature extraction of video frames using GLCM. Int J Eng Trends Technol 4(6):2718–2721
[44] Tan X, Triggs B (2007) Enhanced local texture feature sets for face recognition under difcult lighting conditions. IEEE Trans Image Process 19(6):635–1650
[45] Nanni L, Brahnam S, Lumini A (2010) A local approach based on a local binary patterns variant texture descriptor for classifying pain states. Expert Syst Appl 37(12):7888–7894
[46] Lee JC, Chang CP, Chen WK (2015) Detection of copy–move image forgery using histogram of orientated gradients. Inf Sci. https://doi.org/10.1016/j.ins.2015.03.009
[47] Soni B, Das PK, Thounaojam DM (2017) Copy-move tampering detection based on local binary pattern histogram Fourier feature. In: ICCCT-2017: proceedings of the 7th international conference on computer and communication technology, November 2017, pp 78–83
[48] Yang F, Li J, Lu W, Weng J (2017) Copy-move forgery detection based on hybrid features. Eng Appl Artif Intell 59(2017):73–83. https://doi.org/10.1016/j.engappai.2016.12.022
[49] Baber, Junaid & Satoh, Shin'ichi & Afzulpurkar, Nitin & Bakhtyar, Maheen. (2012). Q-CSLBP: Compression of CSLBP descriptor. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 7674 LNCS. 513-521. 10.1007/978-3-642-34778-8_48.
[50] Huang, di & Wang, Yiding. (2007). A Robust Method for Near Infrared Face Recognition Based on Extended Local Binary Pattern. 437-446. 10.1007/978-3-540-76856-2_43.
[51] Ahmed, Faisal & Hossain, Emam & Bari, A. & Shihavuddin, A.. (2011). Compound local binary pattern (CLBP) for robust facial expression recognition. 12th IEEE International Symposium on Computational Intelligence and Informatics, CINTI 2011 - Proceedings. 10.1109/CINTI.2011.6108536.
[52] Li, Jiayuan & Hu, Qingwu & Ai, Mingyao. (2018). RIFT: Multi-modal Image Matching Based on Radiation-invariant Feature Transform.
[53] Liang, Yixiong & Liu, Lingbo & Xu, Ying & Xiang, Yao & Zou, Beiji. (2011). Multi-task GLOH feature selection for human age estimation. Proceedings - International Conference on Image Processing, ICIP. 10.1109/ICIP.2011.6116611
[54] Guo Y, Cao X, Zhang W, Wang R (2018) Fake colorized image detection. IEEE Trans Inf Forensics Secur 13(8):1932–1944
[55] Wu Y, Abd-Almageed W, Natarajan P (2018) BusterNet: detecting copy-move image forgery with source/target localization. In: European conference on computer vision (ECCV)
[56] BAT food source: Available : https://askabiologist.asu.edu/bat-food
[57] CNN Cheatsheet: Available: https://stanford.edu/~shervine/teaching/cs-230/cheatsheet-convolutional-neural-networks
[58] Deep fake detection challenge :Available: https://www.kaggle.com/c/deepfake-detection-challenge/overview/prizes
[59] DRIVE: Available: http://www.isi.uu.nl/Research/Databases/DRIVE/
[60] MESSICOR, Available: http://www.adcis.net/en/third-party/messidor/
[61] STARE Available: https://cecas.clemson.edu/~ahoover/stare/images/all-images.zip
[62] CASIA V1, Available:https://www.kaggle.com/sophatvathana/casia-dataset?
[63] CASIA V2, Available: https://www.kaggle.com/shaft49/real-vs-fake-images-casia-dataset
[64] NB-CASIA,Available:https://github.com/nurbaqiyah/CMF-Dataset/tree/master/NB-CASIA
[65] USC-SIPI,Available:http://sipi.usc.edu/database/
[66] CoMoFoD,Available: https://www.vcl.fer.hr/comofod/
[67] Kodakand Google, ,Available:http://www.cs.albany.edu/~xypan/research/snr/Kodak.html
[68] Flickr,Available:https://www.kaggle.com/hsankesara/flickr-image-dataset
[69] MICC-F220, Available:https://github.com/niyishakapatrick/Copy-move-forgery-detection-Image-Blobs_AKAZE-ORB-BRISK-SURF-SIFT-results-on-MICCF220-MICCF2000
[70] GRIP,Available:http://www.grip.unina.it/download/prog/CMFD/CMFDdb_grip.zip
[71] FAU,Available:http://www5.cs.fau.de/our-team
[72] SMIFD,Available:https://github.com/Rana110223/SMIFD-500
[73] WILD WEB,Available:https://mklab.iti.gr/results/the-wild-web-tampered-image-dataset/
[74] PS-Battles,Available:https://github.com/dbisUnibas/ps-battles
[75] COVERAGE,Available:https://1drv.ms/f/s!AggVhXcCj1FLhUUyUrqSpV_yI_GH
[76] Columbia Image Splicing, Available: http://www.ee.columbia.edu/ln/dvmm/downloads/AuthSplicedDataSet/dlform.html
[77] FFCMF,Available:http://emregurbuz.tc/research/imagedatasets/ffcmf/ffcmf_dataset.rar
[78] OICIO,Available:http://emregurbuz.tc/research/imagedatasets/oicio/oicio_dataset.rar
[79] Deepfakes,Available:https://github.com/ondyari/FaceForensics
[80] DDSM,Available:https://www.kaggle.com/skooch/ddsm-mammography
[81] DDSM,Available:http://www.eng.usf.edu/cvprg/Mammography/Database.html
[82] CBIS-DDSM, ,Available:https://wiki.canceri magingarchive.net/display/Public/CBIS-DDSM
[83] MIASDBv1,Available:https://www.repository.cam.ac.uk/bitstream/handle/1810/250394/miasdbv1.21.zip?sequence=3&isAllowed=y
[84] Chestx-ray,Available:https://www.kaggle.com/paultimo thymooney /chest-xray-pneumonia
[85] Novel CORONA virus,Available:https://www.kaggle.com /sudalairajkumar/novel-corona-virus-2019-dataset
[86] CATARACT,Available:https://github.com/KrishnaRauniyar/CataractDetectionApp-UsingCNN-NeuralNetwork/tree/master/Cataract
[87] Glaucoma(RIGA) ,Available:https://deepblue.lib.umich.edu/data/downloads/g732d957m
[88] Yaseen ZM, Deo RC, Hilal A, Abd AM, Bueno LC, Salcedo-Sanz S, Nehdi ML (2017) Predicting compressive strength of lightweight foamed concrete using extreme learning machine model. Adv Eng Softw. https://doi.org/10.1016/j.advengsoft.2017.09.004
[89] Guo Y, Cao X, Zhang W, Wang R (2018) Fake colorized image detection. IEEE Trans Inf Forensics Secur 13(8):1932–1944
[90] Wu Y, Abd-Almageed W, Natarajan P (2018) BusterNet: detecting copy-move image forgery with source/target localization. In: European conference on computer vision (ECCV)