A Hybrid Learning Model to Detect Morphed Images

Noble Kumari[1†] and Dr. A K Mohapatra[2††],
noblevashishta@gmail.com mohapatra.amar@gmail.com
PhD Scholar, USICT, GGSIPU, Delhi, India
Professor, Department Of IT IGDTUW, Delhi, India

Summary
Image morphing methods make seamless transition changes in the image and mask the meaningful information attached to it. This can be detected by traditional machine learning algorithms and new emerging deep learning algorithms. In this research work, scope of different Hybrid learning approaches having combination of Deep learning and Machine learning are being analyzed with the public dataset CASIA V1.0, CASIA V2.0 and DVMM to find the most efficient algorithm. The simulated results with CNN (Convolution Neural Network), Hybrid approach of CNN along with SVM (Support Vector Machine) and Hybrid approach of CNN along with Random Forest algorithm produced 96.92 %, 95.98 and 99.18 % accuracy respectively with the CASIA V2.0 dataset having 9555 images. The accuracy pattern of applied algorithms changes with CASIA V1.0 data and DVMM data having 1721 and 1845 set of images presenting minimal accuracy with Hybrid approach of CNN and Random Forest algorithm. It is confirmed that the choice of best algorithm to find image forgery depends on input data type. This paper presents the combination of best suited algorithm to detect image morphing with different input datasets.

Keywords:
Deep learning, Hybrid learning, Neural network, Morphing, Simulation

1. Introduction

Easy availability of huge number of manipulated pictures questions on the credibility of information linked to images. Digital image forensic deals with investigation of image authentication and manipulation. Image manipulation techniques can be classified as splicing and copy move forgery. Splicing forgery is done by combining two or more images and copy move forgery is done by copying a part of image and pasted on another image [1]. The copied region can also be scaled or rotated before pasting to make forgery more complex. These techniques fall under group of Key Points based and Block-Based Copy Move forgery detection. In Key Point detection techniques few key points like high entropy are extracted in few techniques like SIFT, SURF and Harris Corner detector. And the extracted Key Points are matched to identify duplicate region. In Block-Based techniques whole image is broken into small parts and suitable feature is extracted from each block to detect forgery. Technique using Block based are Discrete Cosine transform, Fourier Mellin Transform, Polar Cosine Transform etc. Key Point techniques perform better in jpeg compression, noise addition, brightness change whereas Block-Based techniques perform better in homogeneous region [2,3].

Figure 1 represents the Image Splicing technique where a(x,y) and b(x,y) are original images. Image b(x,y) is merged with c(x,y) image which is part of a(x,y) original image and forms d(x,y) spliced image [4].

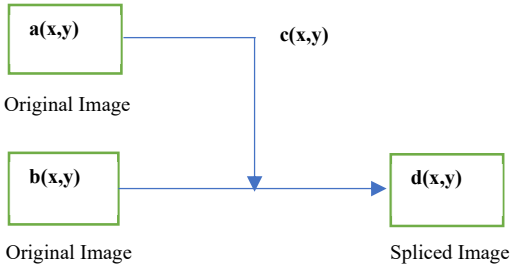

Fig. 1 Image Splicing

Image resizing and resampling process also destroys the information on which classifier rely on. Resizing is generally done in CNN layer on target image to match the input layer. Hence, image resizing should also be avoided while performing image forensic [5].

Forgery detection and forensics follows the pipeline process of feature extraction, learning and then processing. Image feature detectors being executed in the computer vision area having applications like image representation, object detection, image classification, 3D scene construction, activity recognition, text classification and biometric system [6]. Image forgery detection and localization are the fundamental steps which aims to perform image wise and pixel wise classification. Most of the forgery detection uses CNN or Long Short Memory Network to characterize the statistical dependencies among pixels. These network models extract features from all over the images and then selects informative regions within an image to concentrate on computational resource

Manuscript received June 5, 2022
Manuscript revised June 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.6.46

which leads superior performance than traditional approaches [7].

Falsified images mistakenly may be used in several applications which produces dangerous consequences to society. Deep Learning approach is the efficient solution to detect falsified images. Various techniques have been used to detect forgery like Discrete cosine transform, Principal component, Hilbert-Huang transform or multi size block [8].

1.1 ML Technique

ML technique work on the basis of features. If labelled data is provided in training, it becomes supervised learning. In case of non labelled data, it is called non supervised learning. In the process morphed features are taken out of labelled data and applied to training. This knowledge is used at test time when the features are compared to predict image. Support vector machine (SVM) algorithm can be used for it. Figure 2 explains the similar flow of training with label image and then implementing knowledge in test set to predict in model [9].

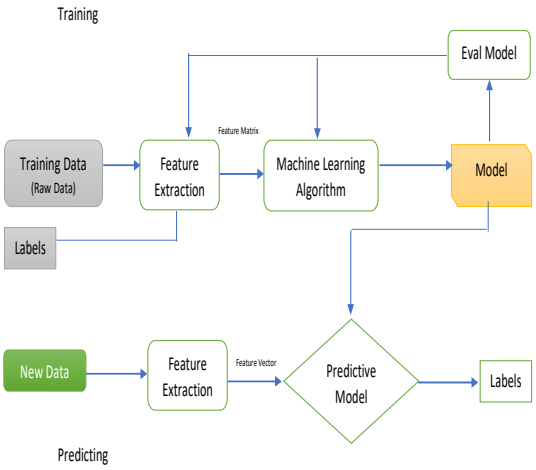

Fig. 2 Block diagram of ML based Algorithm

1.2 Deep learning (DL) technique

Deep learning (DL) or Deep neural network (DNN) are equipped with multiple layers and is being considered as one of the most powerful tools with huge data. Hidden layers have surpassed the classical approach with more accurate result. Convolution neural network (CNN) is one of the most popular DL methods. CNN comprises of mathematical functions, matrix, non-linearity, fully connected layer and pooling, the combination of which provides better performance [10]. In this work combination of CNN and ML is applied to test better accuracy in morphed image data set.

Deep Learning algorithm achieves high accuracy but also have limitation of sometimes leaving important features on the basis of numbers given in deep learning [11]. There is scope of improving the available learning algorithms to detect forgery.

Image forgery can be taken as two class problem with morphed and non-morphed set of images and hence this problem can be solved by machine learning (ML) classification technique [12].

This paper works in the approach of below mentioned steps.

1. To model a Hybrid DNN using the supervised learning in combination with different ML (SVM and Random Forest)
2. To classify morphed image and non-morphed image from data set.

The following sections of paper are arranged as, Section 2 of this paper provides literature survey of various forgery detection algorithms. Section 3 provides the flowchart of proposed algorithm with Hybrid learning. Section 4 presents the implementation and results with morphed datasets. Section 5 provides the conclusion part.

2. Literature Review

Different approaches have been proposed to detect morphed images. Table 1 provides the brief of various feature-based approach which are being used to detect morphed images [13].

Table 1: Different approaches to detect morphed Images

Feature Type	Advantage	Disadvantage
Text Feature	Easy to implement. Low cost.	Sensitive to image resolution.
Image Quality Feature	Easy to implement. Low cost.	Sensitive to Compressed Data.
Hybrid Feature	Good detection in different morphed data types.	High Cost. Difficult to implement.
Residual Noise Feature	Easy to implement. Low cost.	Applicable only to digital data.
Deep CNN Feature	Good performance. No need to train CNN from scratch.	High Cost. Need large database for training.

Reyna et al. [14] implemented SVM algorithm for image processing based on statistical learning theory. Raghavendra et al. [15] proposed the micro texture based morphing detection model using the statistical features of face image data set with SVM classifier.

Makrushin et al. [16] proposed Benford feature based approach using discrete cosine transform of images. According to the Benford's law, naturally generated data have logarithmic distribution and morphed image violates this law and this helps in classifying the image dataset. Hildebrandt et al. [17] used the anti-forensic method like StirTrace and claimed like it has impact on morph detection. The method was based on the approach of adding noise in morphed image to classify them then as genuine ones. Tom Neubert [18] used the image compression or degradation method to claim that compression works effectively on non-morphed images than morphed images. Bunk et al. [19] implemented the approach of utilizing resampling feature and then using them for classification. Tarman [20] used the scale invariant feature transform (SIFT) method with 98% accuracy but time taking algorithm. Fengli and Qinghua [21] observed the irregular pattern due to forgery using forurier transform in network. Kumar and Thirunavukkarasu [22] used the approach of fast retina keypoint descriptor (FREAK). The descriptors are then used by 'k' means algorithm. Meng and Cheng [23] used the method by having edge detection networks. First different features are taken to train edge network and then output of this is fed to whole model. Li and Liu [24] presented result of SIFT features to minimize distortion of image.

The approach provided better result than many methods. Amerini et al. [25] also followed the SIFT approach in using the geometrical transformation concept. Husain et al. [26] proposed technique by DNN to detect indoor scenes on combining geometric and semantic features. Li et al. [27] presented the approach of hyperspectral image classification based on DL with large data base. Zhao et al. [28] implemented the approach of DL along with object-based classification method for efficient image classification. Shen and Wang [29] presented a DL method for videos frame. To prevent overfitting in this model limited number of videos are given in training. Jassim, Sabah, and Asaad [30] proposed a new approach of Topological Data Analysis (TDA) to understand Bigdata. The distance threshold is used to find out the morphed image from genuine images. Jaiswal, Ankit and Srivastava [12] implemented the splicing technique. The ML algorithm is used to find whether the image is spliced or not. The feature vector is extracted and then trained with logistic regression classification model. Mellouli, Dorra, et al. [31] proposed new approach using deep learning having two key ingredients. Firstly, CNN is applied and then morphological feature extraction is done.

Table 2 presents the brief of the few of the recent related work summary regarding morphed image detection.

Table 2: The related Work Summary

Reference	Approach	Advantages	Limitations
Raghavendra et al. [32]	Transferable Features fusion based DCNN Viola-Jones algorithm, DCNN, Binary Statistical Image Features (BSIF)-SVM	Robust in detecting morphed images in print and digital both modes.	-
Makrushin et al. [33]	Human vs Algorithm Keypoint-based morphing detector and DCNN-based detector	At least one of the approached used is able to find morphed images.	Low Sample for evaluation
Neubert et al. [34]	ICAO-aligned pre-processing module, feature extraction module and classification module Feature Detection	Detecting morphed passport images	More sample number required for data accuracy
Aghdaie et al. [35]	2D Wavelet Decomposition Supervised feature selection	Morphed data set detected accurately in VISAPP17 data set	Morphed data set detected less accurately in LMA data set
Ferrara et al. [36]	Print Scanned Images with Data augmentation strategy Deep Neural network	Performing better than other approaches for several datasets.	Need to know the factor influencing network decision.
Aghdaie et al. [37]	Attention-based deep neural network Integrating attention weighted features	Morphed data set detected accurately in VISAPP17 data set	Morphed data set detected less accurately in LMA data set

Seibolda et al. [38]	Layer-wise relevance propagation Differently Trained Network	More robust to detect morphed face	-
Venkatesh et al. [39]	Single Image Morphing Attack Detection by using individual morphing score Local Binary Patterns (LBP), Histogram of gradients (HOG) and Binarized Statistical Image Features (BSIF).	Proposed better result with chosen data sets.	Need to verify result with multiple datasets.
Scherhag et al. [40]	Laplace operator	Information can be extracted about edges in the image.	Cannot be used for Solitary system
Scherhag et al. [41]	Facial Landmarks Random Forest classifier	New approach	Need to be more accurate.

From various survey reports it is concluded that initially traditional methods were being used to find the morphed images but gradually it moved to ML and then to DL method. The huge amount of data further accelerated the need of DL like method. With current scenario having huge data there is always scope to work for better techniques and methods with DL techniques.

3. Proposed Approach

In this work, Deep Learning algorithm and combination of Deep learning with Machine learning (SVM and Random Forest algorithm) is applied on CASIA V1.0, CASIA V2.0 and DVMM image data set [42,43]. As per the simulated result it is perceived that result accuracy is dependent on the availability of size and type of data set.

All the simulated models are compared by having same number of mesh layer, filter number, batch size, epochs number and activation function. It is analyzed that the choice of algorithm producing better accuracy changes with number of epochs on same data between CNN and CNN with SVM algorithm. CNN with Random Forest generates most accurate result in minimal time with large input dataset. Result accuracy is also affected by size of Input data set. Performance is compared with the result accuracy and time taken to execute [9-10]. Specificity and Sensitivity are also factors to compare result of models, having

$$Specificity\ (S) = TN/(TN + FP) \quad (1)$$

$$Sensitivity(St) = TP/(FN + TP) \quad (2)$$

Where, TP represents True Positive, FP represents False Positive, TN represents True Negative and FN represents False Negative.

3.1 Proposed Algorithm

In this work transfer learning approach trains model with multiple datasets with each set having train and test data folder. The models acquire learning of image using the training data comprising of morphed and non-morphed images. CNN get trained by the extensive data and extract features from it. Three models are being analyzed with various input sets.

Model 1 comprises of CNN layers for feature extraction and classification, Model 2 is having CNN algorithm for feature extraction and then SVM algorithm as classifier and Model 3 is having CNN algorithm for feature extraction and then with Random Forest Algorithm as classifier. Proposed models predict categories as morphed or non-morphed images. Images are taken in training and testing are both morphed and non-morphed. In morphed category CMF and SF images are available. Training and testing of models are done on CASIA V1.0, CASIA V2.0 and DVMM datasets with batch size of 32. CASIA V1.0 dataset has 921 morphed images and 800 non morphed images in .jpg format. CASIA V2.0 dataset has 2064 morphed images and 7491 non morphed images in .jpg format. DVMM dataset has 912 morphed images and 933 non morphed images in .bmp format. The DCNN method helps to detect forgery by having minimal complexity and computation for the huge data set. The concepts of overfitting may increase complexity of the network and hence high-end GPU is used to resolve this issue. Models are in layered structure with layers consisting of convolutional layer, input layer, ReLU layer, max-pooling layer and fully connected layer. For training and testing purpose size of the image is $256 \times 256 \times 3$ pixel. Pseudocode for the proposed approach is mentioned below:

Pseudo Code: Morphed_Image_detection

Input: CASIA V1.0, CASIA V2.0 and DVMM image data set

Output: Result (Accuracy, Morphed image detection)

1. For each image in data set
1. Read Image
2. Apply CNN layer with 16 filter, Relu activation function and Max Pooling.
1. Apply CNN layer with 32 filter, Relu activation function and Max Pooling.
2. Apply CNN layer with 64 filter, Relu activation function and Max Pooling.
3. Apply classifier //CNN, SVM or Random Forest
4. IF classifier applied is CNN or SVM
5. Run classifier with different epochs value
6. Increase Epochs value till maximum accuracy achieved
7. ELSE
8. Apply Random state classifier
9. ENDIF
10. Result=Classification (Accuracy % and morphed/non-morphed Image)

3.2 Convolution

CNN consists of input layer, hidden layers and output layers. Input layer is connected to hidden layer with neurons. The input color image has 3 color channels with thickness as 3. M is column number and N is rows number with 3 color channels, the total pixels in image would be $M * N * 3$. Similarly, this function in kernel level is $i * j * 3$. The output channel size is $2 * (M - i + 1) * (N - j + 1)$, where '2' represents the number of color channel, M represents Width of image, N represents height of image and similarly i and j: represents the kernel [9-10].

3.3 Stride

CNN has many options to decrease number of parameters and also some side effects. Stride is one of those options. Figure 3.1 provides the stride example with 7x7 matrix. If the filter is moved one node, 5x5 output is generated. If stride =2, output is 3x3 matrix. This reduces the size of output [9-10].

$$O = 1 + (N - F)/S \quad (3)$$

Where, N represents Input size, F represents Filter size and S represents Stride Size.

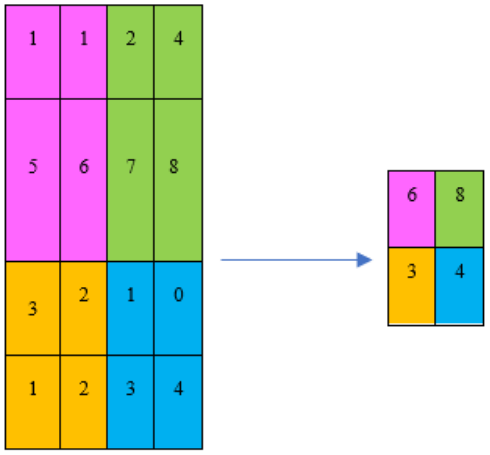

Fig. 3 Stride Effect

3.4 Padding

The limitation of convolution is information loss which may be present on image border. Zero padding is used to handle the size of output. Taking F=3, N =7 and S =1, output would be from 7x7 to 5x5 matrix [12-13].

$$O = 1 + (N + 2P - F)/S \quad (4)$$

Where P represents number of zero padding layers.

However, if '1' is added to zero padding it makes the output 7x7 only which is same as input. Equation 4 provides the modified formula. Padding makes it possible to have any number of DCNN [9-10].

3.5 Pooling

Pooling operation helps in reducing image size. In this process small neighborhood is taken, aggregated and pooling is done to single value. Pooling process makes the system less complex layer by layer like in image processing reducing resolution. Number of filters are not affected by Pooling. Max Pooling is one of the mostly used pooling method. This method processes the sub section of rectangle and returns the max value of that section. One of the most used sizes in pooling is 2x2. Down Sampling method could not preserve the information position. Hence, it should be used when generic information is more important than the spatial information [9-10].

3.6 Rectified linear unit (ReLU)

The nonlinear function ReLU converts the positive values and negative values to 1 and 0 respectively. Input to output information mapping is done in supervised learning. The Relu function is defined below [9-10].

$$\text{ReLU}(y) = \max(0,y) \quad (5)$$

$$d/dy\text{Relu}(y) = \{1 \text{ if } y>0 \text{ ,0 otherwise}\} \quad (6)$$

3.7 Non-Linearity

Non linearity is next layer of convolution to adjust the generated output. This layer is applied for output saturation. Relu, tanh and sigmoid are mostly used non-linear function. However, Relu-Rectified Linear Unit is known for its simple definition in function [9-10].

3.8 Image forgery classification

Image forgery classification is done in Copy move and SF morphed images using the CNN algorithm classifying the images into morphed or not morphed images. After classification, performance is checked on test set and produces the result of classification [9-10].

3.9 Fully Connected Layer

This layer is as similar as arrangement of neurons in traditional neural network. And hence each and every node in this model is connected to each and every node of next and previous layer. CNN using most of parameters with this implements the training of model. Also, numerous numbers of parameters in this layer sometimes makes the computation complex in training. Therefore, number of nodes and few connections are eliminated using the dropout technique [9-10].

3.10 Performance Checking

The accuracy of algorithm is checked at testing level in image forgery classification. The algorithm is trained with multiple data set of splicing and CMF morphed image and also with non-morphed images. After training the algorithm predicts the loss and accuracy of system. For performance checking public dataset is used which is having sub set of morphed and non-morphed images [9-10].

3.11 Support Vector Machines

SVM algorithm is well known in the pattern recognition consisting of object recognizing, speaker finding, face detection and text recognition. The advantage of this algorithm exists in using the approach of learning algorithm for controlling the system. The decision function of SVM is as mentioned below:

$$f(x,a) = sign(\sum_{supportVector}(y_i a_i \, \text{k}(x_i.x) - \text{b})) \quad (7)$$

Here, k(x_i,x) represents convolution function for kernel or inner product [14].

3.12 Random Forest Algorithm

Random Forest is a supervised and tree-based machine learning approach. The algorithm follows the below mentioned steps [44]:

1. Randomly select n features from total k features, where n<k
2. Among n features the node ‘n’ is calculated using best split method
3. Categorize the node into daughter’s node using best split
4. Repeat steps 1 to 3 until ‘1’ number of node is reached
5. Repeat step 1 to 4 to build Forest ‘n’ times to create ‘n’ number of trees
6.

4. Result Analysis

In this work, research has been done on CASIA V1.0, CASIA V2.0 and DVMM public data set. Forgery detection algorithms are run on Intel i5 processor and 8 GB RAM specification. Forgery classification is done using the proposed approach on image dataset on Spyder3 software using Python language. The database is classified as morphed and non-morphed images in training data set. Data set is cleaned by removing all .tif images from CASIA V2.0 data set and the experiment is done on .jpg images only. DVMM image data set has black and white images in .bmp format. Public data sets consist of CMF and splicing forgeries.

Table 3: Accuracy comparison on CASIA V2 data

Epoch	*CNN accuracy*	*Time Elapsed In CNN (min)*	*CNN + SVM accuracy*	*Time Elapsed in CNN+ SVM(min)*
10	86.6	31.2	88.56	30.0
25	91.45	78	91.5	75
40	93.87	124.8	93.21	121.2
60	95.92	187.2	94.62	181.8
80	96.92	242.4	95.98	240

Table 3 presents the comparative accuracy result on CASIA V2.0 data with different epochs value in CNN (Model 1) and CNN + SVM algorithm (Model 2). As per result, accuracy of CNN+SVM is more than CNN algorithm accuracy in epochs number 10 and 25 whereas for epochs number 40,60 and 80 CNN algorithm outperformed CNN+SVM. Average time taken by CNN+SVM algorithm is lesser than CNN algorithm.

The number of epochs represents the number of times learning algorithm will work. Number of epochs provides opportunity to update internal model parameters and overfitting and underfitting of model [45]. As per data analysis it is concluded that CNN+SVM algorithm outperforms CNN in a smaller number of epochs.

The Hybrid learning method is implemented using the CNN and SVM combination model. The last layer of CNN model is made to work as SVM using the linear model with regularizer L2 and hinge loss method. This makes the model a combination of CNN and SVM. The Hybrid model uses the functionality of SVM algorithm's decision plane that distinguishes from one set of data to other. The algorithm searches the vector point called support vector which defines the boundary line between classes and classifies the morphed and non-morphed images.

Model 3 having combination of CNN and Random Forest on CASIA V2 data produced the most accurate result with 99.18% accuracy and 45 sec execution time. Random forest algorithm as a classifier works on the basis of decision tree. The algorithm with powerful randomized function produces more accurate result and resistant to overfitting. The algorithm has the capability to handle the mixed or unbalanced data set effectively [46].

Table 4: Accuracy comparison on CASIA V1 data

Epoch	**CNN accuracy**	**Time Elapsed In CNN (min)**	**CNN + SVM accuracy**	**Time Elapsed in CNN+ SVM(min)**
10	65.25	5	61.07	5
25	79.14	12.7	78.85	12.7
40	87.39	21	86.93	21
60	98.26	31.5	92.39	31.5
80	98.49	42	95.41	42

Table 4 presents the comparative accuracy result on CASIA V1.0 data with different epochs value in CNN (Model 1) and CNN + SVM algorithm (Model 2). As per result it is observed that accuracy of CNN algorithm outperformed CNN+SVM algorithm for all values of epochs. Average time taken by CNN+SVM algorithm and CNN algorithm is similar.

Model 3 having combination of CNN and Random Forest on CASIA V1 data produced the least accurate result with 53.57% accuracy and 25 sec execution time.

Table 5: Accuracy comparison on DVMM data

Epoch	**CNN accuracy**	**Time Elapsed In CNN (min)**	**CNN + SVM accuracy**	**Time Elapsed in CNN+ SVM(min)**
10	97.99	5.1	94.25	5.1
25	97.83	12.7	99.24	12.7

Table 5 presents the comparative accuracy result on DVMM data with different epochs value in CNN (Model 1) and CNN + SVM algorithm (Model 2). As per result it is observed that accuracy of CNN+SVM algorithm outperformed CNN algorithm in epoch value 25 and after which accuracy degradation starts. Here like Table 1 result, number of epochs affects the overfitting and change iteration in input parameters.

Model 3 having combination of CNN and Random Forest on DVMM data produced result with 52.43 % accuracy and 25 sec execution time.

CNN + Random Forest algorithm produced the best accuracy result in CASIA V2.0 data set having 9555 images whereas least in CASIA V1.0 having 1721 images and DVMM having 1845 images. Random forest Algorithm works better with large input space which provides potentially improved classifier diversity and hence algorithm works by reducing number of inputs to each classifier and constructing multiple random input space [47]. Therefore, CNN and Random Forest algorithm produced most effective accuracy with CASIA V2.0 dataset.

Table 6: Comparative accuracy result on CASIA V2 data

Author	Approach	Accuracy	Sensitivity	Specificity
Model1 (Proposed at epoch 80)	CNN	96.92	98	81.2
Model 2 (proposed at epoch 80)	CNN + SVM	95.98	99	81.2
Model 3 (proposed)	CNN+ Random Forest	99.18	99.6	99.4
Jaiswal [48]	MultiClass Model	70.26	63.39	74.97
Jaiswal [48]	Naïve Bayes	59.91	50.47	71.47
Jaiswal [48]	K Nearest Neighbor	59.91	50.71	65.33
Zhongwei et.al. [49]	DCT & DWT	89.76	-	-
Thakur [9]	Hybrid	98	-	-

Table 6 presents comparative brief of different approaches by various authors on CASIA V2.0 data set. Proposed Models are presented with accuracy results. Model 3 having combination of CNN and Random Forest performed best out of all 3 models. Model 1 having 96. 92 % accuracy at epochs 80 after which the model reaches to overfitting, model 2 produced 95.98% accuracy and model 3 produced 99.18 % accuracy. Model 3 performed better than Thakur [9] proposed algorithm on similar data set with 98 % accuracy. As per result provided by Jaiswal [48] the multiclass model showed the 70.26% accuracy, Naïve Baise and K nearest neighbor approach showed 59.91% of accuracy, Zhongwei [49] showed the accuracy of 89.76% by using DCT and DWT approach on the same data set. With this it is concluded that various algorithms produce varied accuracy result depending on nature of data and other constraints.

5. Conclusion

In this paper passive image forgery detection is done by CNN, CNN+SVM and CNN + Random Forest approach on CASIA V1.0, CASIA V2.0 and DVMM public dataset. The forgery detection accuracy result depends on the approach used, data set format and size. The simulated results with CNN, Hybrid approach of CNN along with SVM and Hybrid approach of CNN along with Random Forest algorithm produced 96.92 %, 95.98 and 99.18 % accuracy with the CASIA V2.0 dataset having 9555 images. With this data set CNN + Random Forest algorithm produced the best result. The accuracy pattern of these algorithms changed with CASIA V1.0 data and DVMM data having 1721 and 1845 set of images presenting minimal accuracy with Hybrid approach of CNN and Random Forest algorithm. In these data sets CNN+SVM performed better than CNN with small number of epochs whereas CNN outperformed in large number of epochs. CNN + Random Forest Algorithm works best with large number of input data set giving scope to improve classifier diversity. As per analysis this is concluded that the choice of best algorithm to find image forgery depends on the data type, data size, epoch value and hardware dependency for execution time.

References

[1] Dua, Shilpa, Jyotsna Singh, and Harish Parthasarathy. "Image forgery detection based on statistical features of block DCT coefficients." Procedia Computer Science 171 (2020): 369-378.

[2] Meena, Kunj Bihari, and Vipin Tyagi. "A hybrid copy-move image forgery detection technique based on Fourier-Mellin and scale invariant feature transforms." Multimedia Tools and Applications 79.11 (2020): 8197-8212.

[3] Al_Azrak, Faten Maher, et al. "An efficient method for image forgery detection based on trigonometric transforms and deep learning." Multimedia Tools and Applications 79.25 (2020): 18221-18243.

[4] Z Zhang, Y Zhou, J Kang and Y Ren, Study of image splicing detection., International Conference on Intelligent Computing. Springer, Berlin, Heidelberg, 2008

[5] Marra, Francesco, et al. "A full-image full-resolution end-to-end-trainable CNN framework for image forgery detection." IEEE Access 8 (2020): 133488-133502.

[6] Geetha, M., et al. "A novel approach for image forgery detection using improved crow search algorithm." Materials Today: Proceedings (2021).

[7] Rao, Yuan, Jiangqun Ni, and Hao Xie. "Multi-semantic CRF-based attention model for image forgery detection and localization." Signal Processing 183 (2021): 108051.

[8] El Biach, Fatima Zahra, et al. "Encoder-decoder based convolutional neural networks for image forgery detection." Multimedia Tools and Applications (2021): 1-18.

[9] A Thakur and N Jindal, Hybrid deep learning and machine learning approach for passive image forensic, IET Image Processing 14.10 (2020): 1952-1959

[10] Albawi, Saad, Tareq Abed Mohammed, and Saad Al-Zawi., Understanding of a convolutional neural network, 2017

International Conference on Engineering and Technology (ICET). Ieee, 2017

[11] Kadam, Kalyani, Swati Ahirrao, and Ketan Kotecha. "AHP validated literature review of forgery type dependent passive image forgery detection with explainable AI." International Journal of Electrical & Computer Engineering (2088-8708) 11.5 (2021).

[12] Jaiswal, A Kumar, and R Srivastava, A technique for image splicing detection using Hybrid feature set, Multimedia Tools and Applications 79.17 (2020): 11837-11860

[13] Venkatesh, Sushma, et al. "Face morphing attack generation & detection: A comprehensive survey." IEEE Transactions on Technology and Society (2021).

[14] Reyna, Roberto A., et al. "Implementation of the SVM neural network generalization function for image processing." Proceedings Fifth IEEE International Workshop on Computer Architectures for Machine Perception. IEEE, 2000.

[15] R Raghavendra, K B Raja, S Marcel and C Busch, Face presentation attack detection across spectrum using time-frequency descriptors of maximal response in laplacian scale-space, 2016 Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA). IEEE, 2016

[16] Makrushin, Andrey, Tom Neubert, and Jana Dittmann., Automatic generation and detection of visually faultless facial morphs, International Conference on Computer Vision Theory and Applications. Vol. 7. SCITEPRESS, 2017

[17] M Hildebrandt, T Neubert, A Makrushin and J Dittmann , Benchmarking face morphing forgery detection: Application of stirtrace for impact simulation of different processing steps, 2017 5th International Workshop on Biometrics and Forensics (IWBF). IEEE, 2017

[18] Neubert, Tom, Face morphing detection: An approach based on image degradation analysis, International Workshop on Digital Watermarking. Springer, Cham, 2017

[19] J Bunk, J H Bappy, T M Mohammed, L Nataraj, A Flenner, B S Manjunath, S Chandrasekaran, A Chowdhury and L Peterson, Detection and localization of image forgeries using resampling features and deep learning, 2017 IEEE conference on computer vision and pattern recognition workshops (CVPRW). IEEE, 2017

[20] Saini, Hardeep, M-SIFT: A detection algorithm for copy move image forgery, 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC). IEEE, 2017

[21] Zhang, Fengli, and Qinghua Li., Deep learning-based data forgery detection in automatic generation control, 2017 IEEE Conference on Communications and Network Security (CNS). IEEE, 2017

[22] V Thirunavukkarasu, and J S Kumar, Passive image tamper detection based on fast retina key point descriptor, 2016 IEEE International Conference on Advances in Computer Applications (ICACA). IEEE, 2016.

[23] D Cheng, G Meng, S Xiang and C Pan, FusionNet: Edge aware deep convolutional networks for semantic segmentation of remote sensing harbor images, IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing 10.12 (2017): 5769-5783

[24] Y Li, J Zhou, A Cheng, X Liu and Y Y Tang, SIFT keypoint removal and injection via convex relaxation, IEEE Transactions on Information Forensics and Security 11.8 (2016): 1722-1735

[25] I Amerini, L Ballan, R Caldelli, A D Bimbo, G Serra, A sift-based forensic method for copy–move attack detection and transformation recovery, IEEE transactions on information forensics and security 6.3 (2011): 1099-1110

[26] F Husain, H Schulz, B Dellen, C Torras and S Behnke, Combining semantic and geometric features for object class segmentation of indoor scenes, IEEE Robotics and Automation Letters 2.1 (2016): 49-55

[27] Li, Jiming, Active learning for hyperspectral image classification with a stacked autoencoders based neural network, 2015 7th Workshop on Hyperspectral Image and Signal Processing: Evolution in Remote Sensing (WHISPERS). IEEE, 2015

[28] Zhao, Wenzhi, Shihong Du, and William J. Emery, Object-based convolutional neural network for high-resolution imagery classification, IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing 10.7 (2017): 3386-3396

[29] Wang, Wenguan, Jianbing Shen, and Ling Shao, Video salient object detection via fully convolutional networks, IEEE Transactions on Image Processing 27.1 (2017): 38-49

[30] Jassim, Sabah, and Aras Asaad, Automatic detection of image morphing by topology-based analysis, 2018 26th European Signal Processing Conference (EUSIPCO). IEEE, 2018

[31] D Mellouli, TM Hamdani, MB Ayed and AM Alimi, Morph-CNN: a morphological convolutional neural network for image classification, International Conference on Neural Information Processing. Springer, Cham, 2017

[32] Raja, Kiran, Sushma Venkatesh, and R. B. Christoph Busch. "Transferable deep-cnn features for detecting digital and print-scanned morphed face images." Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops. 2017.

[33] Makrushin, Andrey, Tom Neubert, and Jana Dittmann. "Humans Vs. Algorithms: Assessment of Security Risks Posed by Facial Morphing to Identity Verification at Border Control." VISIGRAPP (4: VISAPP). 2019.

[34] Neubert, Tom, Christian Kraetzer, and Jana Dittmann. "A face morphing detection concept with a frequency and a spatial domain feature space for images on

eMRTD." Proceedings of the ACM Workshop on Information Hiding and Multimedia Security. 2019.
[35] Aghdaie, Poorya, et al. "Morph Detection Enhanced by Structured Group Sparsity." Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision. 2022.
[36] Ferrara, Matteo, Annalisa Franco, and Davide Maltoni. "Face morphing detection in the presence of printing/scanning and heterogeneous image sources." IET Biometrics 10.3 (2021): 290-303.
[37] Aghdaie, Poorya, et al. "Attention aware wavelet-based detection of morphed face images." 2021 IEEE International Joint Conference on Biometrics (IJCB). IEEE, 2021.
[38] Seibold, Clemens, et al. "Accurate and robust neural networks for face morphing attack detection." Journal of Information Security and Applications 53 (2020): 102526.
[39] Venkatesh, Sushma, et al. "Single image face morphing attack detection using ensemble of features." 2020 IEEE 23rd International Conference on Information Fusion (FUSION). IEEE, 2020.
[40] Scherhag, Ulrich, et al. "Morphing Attack Detection using Laplace operator based features." Norsk IKT-konferanse for forskning og utdanning. No. 3. 2020.
[41] Scherhag, Ulrich, et al. "Detecting morphed face images using facial landmarks." International Conference on Image and Signal Processing. Springer, Cham, 2018.
[42] https://www.kaggle.com/sophatvathana/casia-dataset
[43] https://www.ee.columbia.edu/ln/dvmm/downloads/AuthSplicedDataSet/AuthSplicedDataSet.htm
[44] Jackins, V., et al. "AI-based smart prediction of clinical disease using random forest classifier and Naive Bayes." The Journal of Supercomputing 77.5 (2021): 5198-5219.
[45] Brownlee, Jason. "What is the Difference Between a Batch and an Epoch in a Neural Network?." Machine Learning Mastery 20 (2018).
[46] de Santana, Felipe Bachion, Waldomiro Borges Neto, and Ronei J. Poppi. "Random forest as one-class classifier and infrared spectroscopy for food adulteration detection." Food chemistry 293 (2019): 323-332.
[47] Ham, Jisoo, et al. "Investigation of the random forest framework for classification of hyperspectral data." IEEE Transactions on Geoscience and Remote Sensing 43.3 (2005): 492-501
[48] Jaiswal, Ankit Kumar, and Rajeev Srivastava, Image splicing detection using deep residual network, Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE). 2019
[49] Z He, W Lu, W Sun and J Huang, Digital image splicing detection based on Markov features in DCT and DWT domain, Pattern recognition 45.12 (2012): 4292-4299

Biographies

Noble Kumari received her M.Tech degree in IT from Guru Gobind Singh Indraprastha University, Delhi, in 2014. She is pursuing Ph.D in Digital Forensic domain including Image Forensic and Information Security topics.

Prof. Amar Kumar Mohapatra received his M.Tech. degree in Computer Application from ISM Dhanbad in 2001 and Ph.D. in Information Technology from GGSIP University, Delhi, in 2010. He is working as a Professor in Department of IT at Indira Gandhi Delhi Technical University for Women, Delhi, India. Presently, he is on deputation to work with Delhi Police as Chief Technical Adviser. His research interests include Cryptography, Information Security and Cloud Computing. He is a member of professional bodies like Computer Society of India (CSI) and Institute of Electronics and Electrical Engineers (IEEE), USA.