

Image Forgery Detection using Supervised Neural Network Based on Feature Extraction

Authors: Ms. Neha Vishwakarma¹, Prof. Pankaj Raghuwanshi²

¹M. Tech Scholar, Alpine Institute of Technology, Ujjain (M.P), India. E-mail: (nvishwakarma60@gmail.com)

²Assistant Professor, Alpine Institute of Technology, Ujjain, (M.P), India.

Abstract—With social media making its presence felt wide and far, its consequences are also far reaching at least in the context of imagery. The amount of information that can be shared by images is enormous as compared to text data. However, there remains a chance of fake and forged image data that can be circulated which can result in disastrous consequences for individuals, firms or communities at large. With the advancements in image editing tools, it is practically impossible to detect fake or forged images by the naked human eye. Moreover, the number of images shared specifically on social media platforms is so large that human intervention is practically infeasible. In this paper, image forgery detection has been carried out using artificial neural networks and image processing techniques. The configuration of the neural networks is gradient descent with momentum. The performance index is the classification accuracy. It has been shown that the proposed technique achieves higher classification accuracy compared to previously existing methods for the same dataset.

Keywords—*Image Processing, Image Forgery, Artificial Neural Network (ANN), Gradient descent with momentum (GDM), Classification Accuracy.*

I. INTRODUCTION

With the ever increasing growth and popularity of social media platforms resorting to visual imagery, the chances of forged images doing the rounds have also increased [1]. Moreover, as the tools used for image forgery have become more advanced, the perceptibility of forgery being done has also become very less. With the enormous amount of data being shared on social media platforms, it is nearly impossible to make humans recognize forgery in images in real time critical applications [2]-[3]. Hence, it becomes mandatory to design automated systems which can detect image forgery with high

accuracy, which is the most stringent need to be met [4].

Digital images can be morphed or manipulated in several forms such as splicing, retouching etc. Every forgery technique needs a different approach to be detected. In general, for artificial intelligence to work, it is necessary to train the system with large enough data sets so as to learn from the features of forged and unforger images. Hence, the training data set is critical and so is the choice of features to distinguish a forged image from an unforger one [5]. In this paper, an image forgery mechanism is put forth with a cascaded back to back connection of neural networks called the ada-boost neural architecture. The substantiated discussions follow in the subsequent sections.

II. CHALLENGES PERTAINING TO IMAGE FORGERY DETECTION

There are fundamental challenges pertaining to image forgery detection among which the most prominent ones are [6]-[7]:

1. Similarity in Pixel Value Distribution: The pixel values of forged and unforger images often bear stack similarity thereby making conventional techniques fail.

2. Effect of Noise and Disturbances: Images are extremely prone to blurring, noise and disturbance effects while capturing, storage and sharing. Hence, it becomes almost impossible to detect whether the noise is injected intentionally or is naturally present. Mathematically, the blurring and degradation effects also make the recognition difficult. Let the original image be designated by I , then,

$$I' = I + N(f) \quad (1)$$

Here,

I represents the original image

I' is the degraded image

N is the noise affecting the image

f is the frequency metric

3. The accuracy of classification is extremely challenging to be high since the previous two factors make the classification problem challenging [8].

III. NEURAL NETWORKS

Due to the size and complexity of the data, neural network design to address the problem becomes almost invariable. In such a case, a neural network model is needed which can address the classification problem with high accuracy. The mathematical model of the neural network is shown in figure 1.

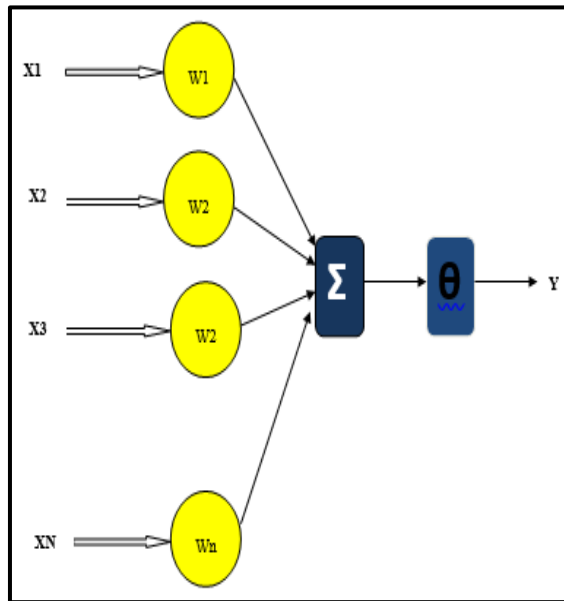


Fig.1 Mathematical Model of ANN

Here,

X represents the parallel input data stream to the ANN

Y represents the output of the ANN

W represents the dynamic weights of the system

θ represents the logic for analysis or bias of the network [9].

Next, for the purpose of image forgery detection, two critical aspects need to be understood.

- (i) Neural networks need to be fed with numerical features which have to be extracted from the raw data set.
- (ii) The network should be able to train or learn from the highly uncorrelated data
- (iii) The neural classifier needs to have a holistic approach in regards to classification.

In the proposed approach, the gradient descent with momentum based approach is used to train the neural networks which performs better than the conventional gradient descent based approach.

IV. DATA PRE-PROCESSING

As discussed earlier, the images are prone to noise and disturbance effects while capturing, storage and transfer. Hence, it is necessary to remove the effects of noise and disturbance [10]. The sub-techniques used are explained below:

- a) **RGB to Gray Scale Conversion:** In this method, the colour or R,G,B image is converted to a grayscale image in which the pixel values are functions of intensity alone i.e.

$$I(R, G, B) \xrightarrow{\text{Transform}} I(\text{intensity}) \quad (2)$$

Thus, the transform removes the R,G,B values separately existing to a combined intensity values in binary or 2 state values.

- b) **Binarization:** In this case, the image is converted to a binary form of image in which all the pixel values.
- c)
- d) **The Wavelet Transform:** The wavelet transform is an effective tool for image noise removal. Images generally are not smooth in nature if the pixel variations are considered [11]. Hence conventional Fourier methods do not render good results for image based data sets. This can be understood as:

$$X(f) = \int_{-\infty}^{+\infty} x(t)e^{-j\omega t} dt \quad (3)$$

Here,

$X(f)$ is the signal in the frequency domain

$x(t)$ is the signal in time domain

It can be seen that the kernel of the transform comprises of smooth signals since:

$$e^{-j\omega t} = \cos\omega t - j\sin\omega t \quad (4)$$

Both sin and cos being smooth in nature are incapable of handling non-smooth variations in the

pixels of the images. Hence the Wavelet Transform is to be used.

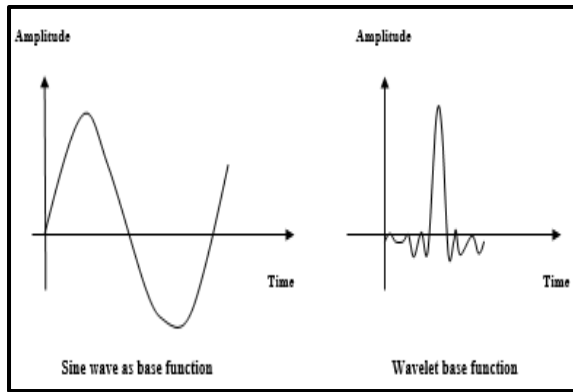


Fig.3 Fourier and Wavelet Base Functions

The difference between the base functions makes it possible for wavelet analysis to cater to the image denoising approach.

Mathematically, the wavelet transform can be given as:

$$Z(S, P) = \int_{-\infty}^{\infty} z(t) ((S, P, t)) dt \quad (5)$$

Here,

S denotes the scaling operation

P denotes the shifting operation

t denotes the time variable

Z is the image in transform domain

z is the image in the spatial domain

The major advantage of the wavelet transform is the fact that it is capable of handling fluctuating natured signals and data and removes noise effects and also local disturbances. The scaling operator is defined for the Wavelet Kernel as:

$$W\Phi(J_0, k) = \frac{1}{\sqrt{M}} \sum_n S(n) \cdot \Phi(n)_{j_0 k} \quad (6)$$

Subsequent to the pre-processing, the feature extraction is done which is explained below.

V. FEATURE EXTRACTION

The neural network understands or is intelligible for numerical data only [12]. Hence it becomes mandatory to feed the neural network with numerical data corresponding to the forged and unforgerd images. The numerical features computed are:

1. Contrast
2. Correlation

3. Energy
4. Homogeneity
5. Mean
6. Standard Deviation
7. Entropy
8. RMS value
9. Variance
10. Smoothness
11. Kurtosis
12. Skewness

The salient features are different for the forged and unforgerd data. Hence it allows the neural networks to classify. The features extracted are then fed to the neural architecture shown in the subsequent figure.

VI. THE GRADIENT DESCENT WITH MOMENTUM (GDM) BASED LEARNING

The gradient descent with momentum is a modified and faster version of the gradient descent algorithm. It is essentially a weighted average of gradients. Subsequently the weighted average is used to update the weights. Generally the GDM approach performs better than the conventional training algorithms employing the gradient descent. It is typically a good classifier that can be used for classification problems. The GDM approach is exemplified using the following illustration.

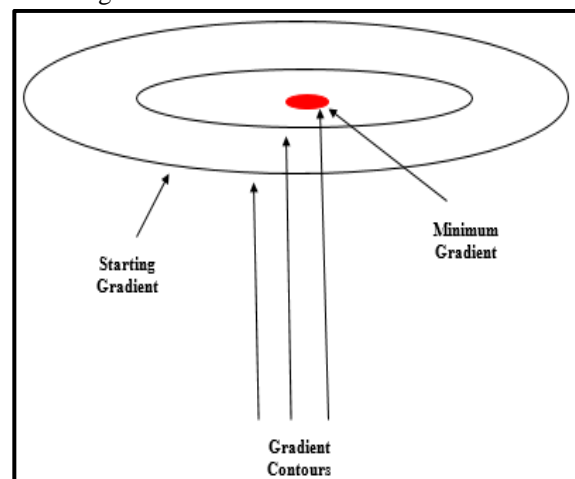


Fig. 4 The gradient contour representation

The gradient descent starts with k=1 and tries to reach the minimum gradient contour. However, in this process, the gradient oscillates. The weight is updated as:

$$w_{k+1} = w_k - \alpha v \partial w \quad (7)$$

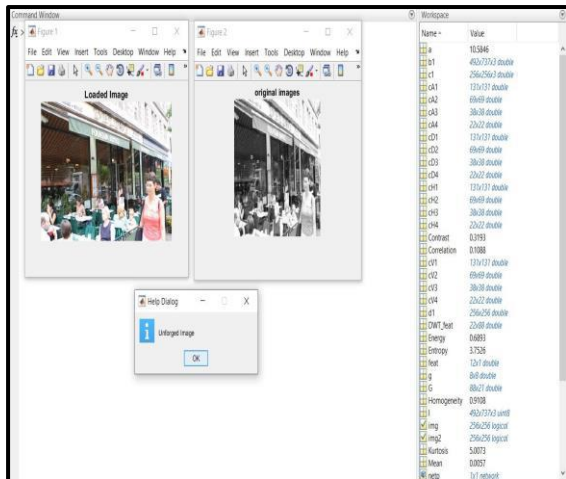


Fig.8 GUI for Non-Forgery Detection

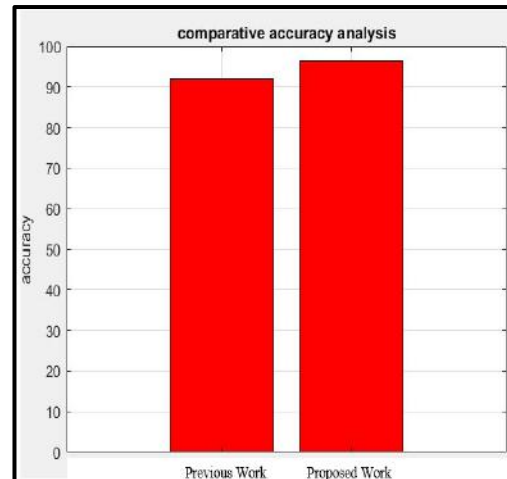


Fig.14 Comparative Accuracy Analysis

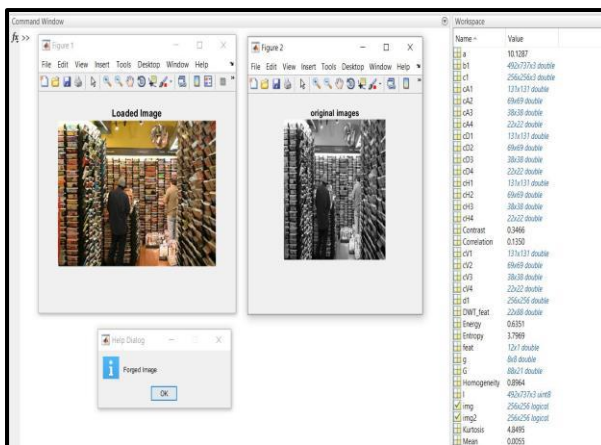


Fig.9 GUI for Forgery Detection

The accuracy of the system for the tested data set is found to be:

$$Ac = \frac{\text{True Classifications}}{\text{Total Cases}}$$

$$Ac = \frac{212}{220} = 96.36\%$$

Thus the accuracy of the proposed system is found to be 96.36%. This is significantly higher compared to the previous work [1] which attained a classification accuracy of 92%

CONCLUSION:

It can be concluded from the previous discussions that the process of image forgery detection is complex in nature owing to the complexity and size of the data for real time critical applications, Hence the need for artificial intelligence based techniques is invariable. The proposed approach presents an approach comprising of statistical feature selection and gradient descent with momentum based approach. The performance of the proposed system is better compared to previous work.

References

[1] Araz Rajab Abraham, Mohd Shafry Mohd Rahim, Ghazali Bin Sulong “Splicing image forgery identification based on artificial neural network approach and texture features”, Springer 2018
 [2] T Pomari, G Ruppert, E Rezende “Image Splicing Detection Through Illumination Inconsistencies and Deep Learning”, IEEE 2018
 [3] J Bunk, JH Bappy, TM Mohammed, “Detection and Localization of Image Forgeries Using Resampling Features and Deep Learning”, IEEE 2017
 [4] C Seibold, W Samek, A Hilsmann, P Eisert., “Detection of Face Morphing Attacks by Deep Learning”, Springer 2017
 [5] Yuan Rao ; Jiangqun Ni, “A deep learning approach to detection of splicing and copy-move forgeries in images”, IEEE 2016
 [6] Belhassen Bayar, Matthew C. Stamm, “A Deep Learning Approach to Universal Image Manipulation Detection Using a New Convolutional Layer”, IEEE 2016.

- [7] Jiansheng Chen ; Xiangui Kang ; Ye Liu ; Z. Jane Wang, "Median Filtering Forensics Based on Convolutional Neural Networks", IEEE 2015.
- [8] Chi-Man Pun , Xiao-Chen Yuan , Xiu-Li Bi, "Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching", IEEE 2015.
- [9] Davide Cozzolino ; Diego Gragnaniello ; Luisa Verdoliva, "Segmentation-Based Image Copy-Move Forgery Detection Scheme", IEEE 2014
- [10] Davide Cozzolino ; Diego Gragnaniello ; Luisa Verdoliva, "Image forgery detection through residual-based local descriptors and block-matching", IEEE 2014
- [11] GK Birajdar, VH Mankar, "Digital image forgery detection using passive techniques: A survey", Elsevier 2013
- [12] G Lynch, FY Shih, HYM Liao, "An efficient expanding block algorithm for image copy-move forgery detection", Elsevier 2013
- [13] M Hussain, G Muhammad, SQ Saleh, AM Mirza, "Image forgery detection using multi-resolution Weber local descriptors", IEEE 2013
- [14] MF Hashmi, AR Hambarde, "Copy move forgery detection using DWT and SIFT features", IEEE 2013
- [15] G Muhammad, M Hussain, G Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform", Elsevier 2012
- [16] W Fan, K Wang, F Cayre, Z Xiong, "3D lighting-based image forgery detection using shape-from-shading", IEEE 2012
- [17] M Hussain, G Muhammad, SQ Saleh, "Copy-move image forgery detection using multi-resolution weber descriptors", IEEE 2012
- [18] H Yao, S Wang, Y Zhao, X Zhang, "Detecting image forgery using perspective constraints", IEEE 2011
- [19] G Muhammad, M Hussain, K Khawaji, "Blind copy move image forgery detection using dyadic undecimated wavelet transform", IEEE 2011
- [20] H Yao, S Wang, Y Zhao, X Zhang, "Detecting image forgery using perspective constraints", IEEE 2011
- [21] AP Tafti, MV Malakooti, M Ashourian, "Digital image forgery detection through data embedding in spatial domain and cellular automata", IEEE 2011
- [22] G Chierchia, S Parrilli, G Pogg, "PRNU-based detection of small-size image forgeries", IEEE 2011
- [23] I Yerushalmy, H Hel-Or, "Digital image forgery detection based on lens and sensor aberration", Springer 2011
- [23] BL Shivakumar, SS Baboo, "Detection of region duplication forgery in digital images using SURF", Citeseer 2011
- [24] G Muhammad, MS Hossain, "Robust copy-move image forgery detection using undecimated wavelets and Zernike moments", ACM 2011
- [25] X Pan, X Zhang, S Lyu, "Exposing image forgery with blind noise estimation", ACM 2011
- [26] B Mahdian, S Saic, "A bibliography on blind methods for identifying image forgery", Elsevier 2010
- [27] P Sutthiwan, YQ Shi, W Su, "Rake transform and edge statistics for image forgery detection", IEEE 2010
- [28] W Wei, S Wang, X Zhang, Z Tang, "Estimation of image rotation angle using interpolation-related spectral signatures with application to blind detection of image forgery", IEEE 2010
- [29] G Chierchia, S Parrilli, G Poggi, C Sansone, "On the influence of denoising in PRNU based forgery detection", Citeseer 2010
- [30] E Ardizzone, A Bruno, G Mazzola, "Copy-move forgery detection via texture description", ACM 2010
- [31] S Math, R Tripathi, "Digital forgeries: Problems and challenges", Citeseer 2010
- [32] J Grim, P Somol, P Pudil, "Digital image forgery detection by local statistical models", IEEE 2010
- [33] S Bayram, HT Sencar, N Memon, "An efficient and robust method for detecting copy-move forgery", IEEE 2009
- [34] B Mahdian, S Saic, "Using noise inconsistencies for blind image forensics", Elsevier 2009
- [35] AE Dirik, N Memon, "Image tamper detection based on demosaicing artifacts", IEEE 2009