International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 13th Apr 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-11&issue=ISSUE-04

DOI: 10.48047/IJIEMR/V11/I04/23

Title **Image Forgery Detection using Alexnet Neural Networks**

Volume 11, Issue 04, Pages: 144-151

Paper Authors

Ch. Naresh, Ch. Pavan Kumar, B.Vasanthi, Ch.Nikhitha Chowdary,

E. Bhala Bhaskara Rao

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Image Forgery Detection using Alexnet Neural Networks

[1]Ch. Naresh, [2]Ch. Pavan Kumar, [3]B.Vasanthi, [4]Ch.Nikhitha Chowdary, [5]E. Bhala Bhaskara Rao

[1,2,3,4]Student, Department of CSE, Seshadri Rao Gudlavalleru Engineering College,Gudlavalleru,Andhra Pradesh,India,

[5]Associate Professor, Department of CSE, Seshadri Rao Gudlavalleru Engineering College, Gudlavalleru, Andhra Pradesh, India,

E-mail: nareshchappidi37@gmail.com, cheemalapavankumar9949@gmail.com, vasanthibolla123@gmail.com, nikhithachowdary062@gmail.com, balabhaskar605@gmail.com

Abstract:
Forgery of photographs has been difficult to differentiate from genuine photographs since it may be achieved with the help of a variety of programmes and is quite straightforward. Each passing day, picture modification gets more difficult to do, and it is increasingly being used to conceal legitimate information in order to gain an advantage over the competition. Forgery photographs are becoming increasingly difficult to distinguish from genuine photographs, and they are also being used as a weapon in illegal activities. The researchers in this study used deep learning, followed by an Alexnet convolutional neural network, to detect counterfeit photos in order to tackle this.

Keywords*: Image, forgery, deep learning, Alexie*

I Introduction

Deep learning is a term used to describe a machine learning system that allows machines to mimic human behavior. Machine learning is a subset of artificial intelligence, and deep learning is a subset of machine learning, and it is one approach for making use of data in this context, among others. Deep learning is a sort of machine learning that is based on the structure of the human brain and is gaining in popularity as a result of its effectiveness. The use of deep learning is becoming increasingly prevalent. Machine learning is a technique for developing artificial intelligence systems through the study of data in artificial intelligence systems, which is used in robotics. Deep learning is performed by the use of ALEXNET, which is equivalent to leNET in terms of performance but far more powerful overall. Moreover, due to the difficulty of the problem and the presence of 60 million parameters, determining a solution is quite challenging. Another enhancement is the increase in the number of convolution layers, which is a significant step forward in terms of performance. A deep neural network is the term used to describe this particular construction (CNN). In this specific case, the Alexnet CNN system is used to recognise the fictitious picture that has been shown. Here, we split the data set into two parts: the training set and the

testing set. We separated the data set into two groups, with one half of the data set being used for training and the other half being utilized for testing purposes. In order to increase accuracy, we utilize 80 percent of the data in training and just 20 percent in testing throughout the development process.

II Literature Survey

A recent study paper[1] asserts that advances in technology have made it possible to modify and change digital content to an extent that was previously unthinkable just a few decades ago. Because of technological breakthroughs that are now inconceivable, it is virtually certain that digital media manipulation will become achievable in the near future. It will become more important for the science of digital forensics to seek to keep up with the times as technology continues to evolve in order to remain relevant. Undoubtedly, as we continue to develop methods for identifying photographic frauds, new ways for generating better fakes that are more difficult to detect will be developed as well, as we continue to develop systems for detecting photographic frauds. Even while certain forensic devices may be more readily tricked than others, some instruments will be more difficult for the average user to overcome than others. For example, a color filter array interpolation may be regenerated by placing a picture back onto its original lattice and then re-interpolating each color channel after it has been disturbed. The process of adjusting for uneven lighting with photo editing software, on the other hand, is not as straightforward as it may seem at first appearance. When it comes to forgery and forensic analysis, an arms race between the two is inescapable in certain situations, just as it is in games of spam vs anti-spam and virus versus anti-virus. As a result of advancements in the field of photo forensics, it has been and will continue to become increasingly difficult and time-consuming (but never impossible) to produce forgeries that will not be recognized in their original form in the future.

The focus of this thesis paper[2] is to examine a number of well-known methodologies for detecting photo fraud in blind situations. Image forgery detection methods are classed in a variety of ways, each of which is discussed in depth below. A more detailed examination of four primary types of forgery detection algorithms is offered, including photo splicing, copy-move detection, resampling detection, and retouching detection. Many current techniques have been explored in each area, and it has been determined that existing tactics are hampered by one or more of the restrictions described below. The following attributes may be found in abundance: (1) High detection accuracy (2) High processing complexity (3) Vulnerability to a broad variety of attacks, including rotation, scaling, JPEG compression, blurring, and brightness change, amongst other things. (4) A substantial number of false matches are occurring against a standard background.

In addition to the limitations discussed above, one significant challenge with these detection systems is the limited range of applications for which they are suitable. For example, a system designed to detect copy-move fraud would not function well with photos that have been spliced or rescaled, and the opposite will be true as well. Despite a large amount of research that has been conducted on the subject of

photo fraud detection, no one detection technique can be called a universal answer for recognising all forms of forgery. The development of a reliable and sophisticated forgery detection technique that is capable of overcoming the limits stated above is thus of paramount importance. Research into the use of these technologies for video forgery detection may potentially be developed by academics and industry in the future. similar to the findings of the research study [3]. A number of comprehensive studies have been published in this vitally important topic of image creation and forensics throughout the course of the last decade. For example, The study published by Farid [5, which was primarily concerned with multimedia security rather than network security], is one of the early surveys that is often cited in the literature. Following the first publication, a number of further surveys, written by a variety of academics [6–11], were released. These investigations look at a variety of types and characteristics of photo forgery detection methods and forensics, as well as the applications of these techniques and forensics. This includes the study presented in [9], which provides a full review of copy-move forgery detection algorithms, which is among the most modern of its kind. As a result of this, the article does not provide a comprehensive analysis of the several feature matching techniques that are often used in the literature. Another way to develop counterfeit detection systems is shown by the survey in [7]. Those tactics are divided into three groups, according to the report: acquisition-based strategies, coding-based strategies, and editing-based strategies. Among the methods mentioned as part of the editing-based category were picture copy-and-move, splicing, and enhancement detection. Additionally, a short review of anti-forensic techniques, which are aimed to hide evidence of tampering, was provided. However, despite the fact that the work contains a large number of references, it does not provide a comprehensive comparison of the different algorithms or a comprehensive study of the several existing methodologies. This research [8] is yet another investigation into picture copy-move, splicing, and retouching detection approaches, with the emphasis this time being on image copy-move detection methods rather than splicing and retouching detection techniques. During the course of their study, the authors go into extensive detail on both the model-based and the transform-based strategies. It is not possible to appreciate the differences between the tactics presented in the surveys since neither survey [7,8] provides adequate quantitative / objective comparisons to enable the reader to comprehend the differences. The most recent research [10] is a good resource since it provides a thorough evaluation of current approaches as well as a range of comparisons offered in the form of tables and figures. Although the basic principles and underlying models of the study were given enough consideration, owing to the nature of the publication, this was not the case. The results of a study report's findings [4] When it comes to photo fraud detection, it's all about figuring out whether or not a digital image is legitimate. According to a general classification, picture authentication systems may be classified into two types. Blindness may be classified into two categories: (1) active and (2) passive. Digital watermarking and digital signatures are active forgery detection systems that embed a recognised authentication code into the picture content before the images are transported over an

insecure public network channel. It is important to verify the presence of such authentication codes and compare them with the codes that were originally submitted in order to ensure authentication. Although this method is straightforward, it requires the use of specialized equipment or software to inject the authentication code into the image before it can be made available to the general public. In contrast to active or blind forgery detection approaches, passive or blind forgery detection techniques depend only on the received picture to determine its legitimacy or integrity, and do not need the existence of a signature or watermark from the sender on the original image. A natural scene image is subjected to digital forgery under the assumption that, while digital forgeries may not leave visible signs of having been tampered with, they are highly likely to disturb the image consistency of the natural scene image due to the introduction of new artifacts and the resulting occurrence of a wide range of inconsistencies. It is possible to detect forgeries in a document by examining these differences. This method is popular since it does not need any prior knowledge about the image in order to be effective. Nowadays, technologies are being used to recognise and discriminate between numerous forms of tampering evidence and to identify each one separately while also locating the site where the evidence was altered.

III Proposed Work

The proposed approach, which is based on the CNN-based AlexNet model and uses publically available Boston published data sets, has been created in order to detect and discriminate whether a digital image under investigation has been fabricated or not. It has been shown that the deep learning features based on the AlexNet model outperform their counterparts in terms of overall performance and efficiency. With this technique, the number of input photos corresponds to the number of images that must be processed using AlexNet-based convolutional operations and pooling with the Relu activation function in order to extract deep features from the images, and the number of images is proportional to the number of input photos. In this study, we employed the CNN Architecture and AlexNet model to analyze the Boston dataset, and the findings were compared to those obtained using six different state of the art methods.

When it came to image level forgery detection, this research made use of the boston dataset, which is available for public use. It is necessary to physically attach labels to the products. Photo features are extracted from the fully connected f7 layer of the AlexNet model using the first input layer of the AlexNet model, which is pre-processed in accordance with the first input layer of the AlexNet model. The average classification accuracy of the images in the dataset is determined after five iterations across the images in the dataset in order to minimize the impact of random samples on the classification performance of the deep features.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

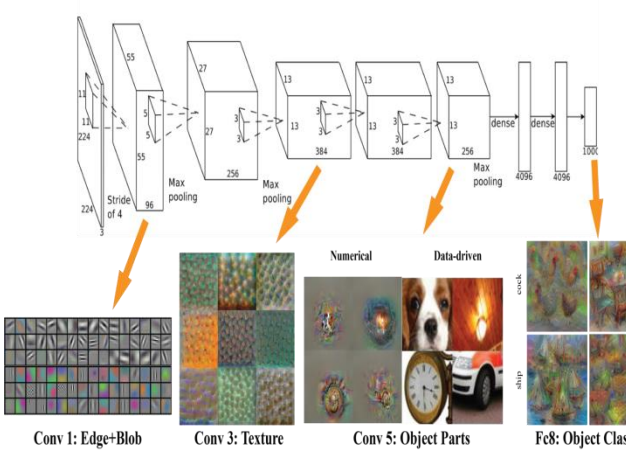

Figure – 1: Alexnet Architecture

IV Algorithm Implementation

4.1 AlexNet Architecture

Deep learning, and more especially convolutional neural networks, have made significant strides in recent years, with convolutional neural networks serving as the most noteworthy illustration of this acceleration. What a CNN's architecture looks like, how many layers it has, what each of those layers is doing, and how the layers are connected to one another are all dictated by CNN's design. When it comes to employing a CNN for learning, selecting the appropriate architecture is important to attaining success. We used the previously taught CNN-based AlexNet architecture for our major training tasks, which was pre-trained for these tasks. The network is made up of a number of layers, each of which has its own set of parameters that may be learned. The AlexNet model was proposed by Krizhevsky and colleagues earlier this year (Krizhevsky et al., 2012). The AlexNet model is composed of 25 layers, each of which is discussed in detail below. A short description of each layer is provided in Table 1, which displays the AlexNet model layers and their relationships. In the AlexNet model, the major layers are the convolutional, pooling, fully connected, and softmax layers; the secondary layers are the activation function ReLU and the activation function ReLU.

4.2 CNN(Convolutional Neural Network)

LeCun and colleagues originally introduced the convolutional neural network for handwriting recognition; they had no idea how well it would perform for other tasks such as image identification, detection, and segmentation. They were right. CNN is quite adept in categorizing photographs on a vast scale, which makes it a valuable resource. Convolutional neural networks are constructed of three layers: a convolutional layer, a pooling layer, and a fully connected layer. Convolutional neural networks may be divided into two types: convolutional and pooling layers. Convolutional layers are the most important layers in a CNN since they serve as both the pooling layer and the most significant layer. A convolutional layer is used to extract features from an image by combining the picture region with many filters and then applying the mixture to the image. The use of a pooling layer, which reduces the size of the output map of the convolution layer, helps to avoid overfitting from occurring. The number of neurons, parameters, and connections established by these two layers is much less than that of a CNN model. General terms, an MLP layer is a kind of data transformation that is often used in the context of the implementation of MLP. In order to categorize data in a logical way, it is necessary to adjust the dimensions of data. Before each neuron in the convolution layer can be put into a fully connected layer in order for it to work correctly, it is essential to transform each neuron in the convolution layer into one-dimensional data. As a result of the fact that it causes geographical information to be lost in data while simultaneously being non-reversible, the fully connected

layer can only be implemented at the end of a network's route. The use of CNN for fake picture classification, as well as turning the real image into error level form on the computer screen. We know from previous research that CNN can achieve competitive performance, and in some cases, can outperform humans in certain visual tasks. We wanted to test CNN's ability to distinguish between counterfeit and genuine images using Error Level Analysis to see if it could tell the difference between the two types of images.

V Dataset

The experimental findings presented in this section are based on data made available by the Boston Police Department, which was used to conduct the experiments. It can be seen in Figures 2 and 3 that this dataset comprises a small number of non-forged photos as well as small numbers of forged images that have been subjected to different combinations of geometrical and transformational assaults on the original picture. Forgeries of photographs via cloning or copy-move forgery are identified using this dataset, which is utilized for the identification of forged photographs.

VI Results and Discussion

As part of the first experiment, a classifier approach for two classes of objects was evaluated: the original and the fake. We were able to do this by splitting the collection of photos into training and test samples in the ratio of 80:20. This illustrates that the technique we utilize is capable of examining the data despite the fact that there is a restricted amount of information accessible. As a result of the training that we have done, we have seen some improvements.

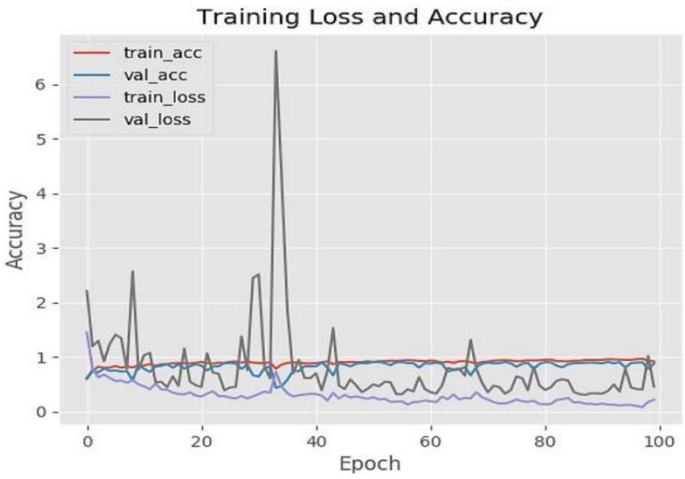

Figure-2: Accuracy vs loss of forgery detection

Following the model's training accuracy, which reached up to 92 percent when using 100 epochs, the validation accuracy reached up to 88.46 percent while using 100 epochs, as shown in the picture above. In this approach, the deep learning architecture of CNN can be used to photo forgeries, and outstanding results in recognition may be obtained by analyzing error level image analysis at the error level level level level level.

VII Conclusion

Our study suggested an image fraud detection strategy that relied on a CNN-based AlexNet model to extract deep features without the need to spend a significant amount of time training.

Comparing the results of this study to earlier work on the MICC-F220 dataset, the best accuracy of picture forgery detection was achieved with an accuracy of 92.%.

In this study, the Boston dataset, which contains few photos of forged and non-forged images, is identified using machine learning techniques.

We were able to develop an effective image forgery detection system utilizing Alexnet Neural Networks as a result of this study.

References

[1] Farid, H., 2009. Image forgery detection. *IEEE Signal processing magazine*, *26*(2), pp.16-25.

[2] Birajdar, G.K. and Mankar, V.H., 2013. Digital image forgery detection using passive techniques: A survey. *Digital investigation*, *10*(3), pp.226-245.

[3] Qureshi, M.A. and Deriche, M., 2015. A bibliography of pixel-based blind image forgery detection techniques. *Signal Processing: Image Communication*, *39*, pp.46-74.

[4] Meena, K.B. and Tyagi, V., 2019. Image forgery detection: survey and future directions. In *Data, Engineering and applications* (pp. 163-194). Springer, Singapore.

[5] Tralic, D., Zupancic, I., Grgic, S. and Grgic, M., 2013, September. CoMoFoD—New database for copy-move forgery detection. In *Proceedings ELMAR-2013* (pp. 49-54). IEEE.

[6] J. A. Redi, W. Taktak, and J.-L. Dugelay, "Digital image forensics: A booklet for beginners," Multimedia Tool Appl., Vol. 51, no. 1, pp. 13362, Jan. 2011.

[7] J. Wang, G. Liu, Z. Zhang, Y. Dai, and Z. Wang, "Fast and robust forensics for image region-duplication forgery," Acta Automatica Sinica, Vol. 35, no. 12, pp. 148895, Dec. 2009.

[8] G. H. Li, Q. Wu, D. Tu, and S. J. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," in Proceedings of IEEE International Conference on Multimedia and Expo, Beijing, Jul. 2007, pp. 17503.

[9] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," in Proceedings of Digital Forensic Research Workshop, 2003.

[10] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, 2004.

[11] 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, pp. 1841-1854, Dec 2012

[12] R. Achanta, A. Shaji, K. Smith, A. Lucchi, P. Fua, and S. Susstrunk, "SLIC superpixels compared to state-of-the-art superpixel methods," IEEE Trans Pattern

Anal Mach Intell, vol. 34, pp. 2274-82, Nov 2012.

[13] P. Lester, Photojournalism: An Ethical Approach, Lawrence Erlbaum Q4 Associates Inc., 1991.

[14] M.C. Stamm, M. Wu, K. Liu, Information forensics: an overview of the first decade, IEEE Access 1 (2013) 167–200.

[15] T. Qazi, K. Hayat, S.U. Khan, S.A. Madani, I.A. Khan, J. Kołodziej, H. Li, W. Lin, K.C. Yow, C.-Z. Xu, Survey on blind image forgery detection, IET Image Process. 7 (7) (2013) 660–670.

[16] Jopseph Casers: Sin Photoshop Y Con Photoshop, ⟨http://merengala. blogspot.com/2010/12/sin-photoshop-y-con-photoshop.html⟩, Accessed: 2015-03-27, April 2013.

[17] I. Amerini, L. Ballan, R. Caldelli, A. del Bimbo, , G. Serra, Geometric tampering estimation by means of a sif-based forensic analysis, in: International Conference on Acoustics, Speech, and Signal Processing (ICASSP), Dallas, TX, USA, 2010, pp. 1702–1705.

[18] J. Wang, G. Liu, H. Li, Y. Dai, Z. Wang, Detection of image region duplication forgery using model with circle block, in: International Conference on Multimedia Information Networking and Security (MINES), vol. 1, IEEE, 2009, pp. 25–29.

[19] D. Fu, Y.Q. Shi, W. Su, Detection of image splicing based on Hilbert– Huang transform and moments of characteristic functions with wavelet decomposition, in: 5th International Workshop on Digital Watermarking, vol. 4283, Springer, 2006, pp. 177–187.

[20] M. Zimba, S. Xingming, DWT-PCA (EVD) based copy-move image forgery detection, Int. J. Digit. Content Technol. Appl. 5 (1) (2011) 251–258.

[21] J.N.V.R. Swarup Kumar et al. "Quality Monitoring of Drinking Water with Selected Parameters Using Sensor Assembly Integrated with IoT- A Comparative Study" on International Journal of Grid and Distributed Computing (IJGDC), Vol. 13, No. 1, (2020), pp. 1049-1060 ISSN: 2005-4262 (Online).

[22] J.N.V.R.Swarup Kumar et.al, "Smart City Concept Based on the Internet of Things
Using Cloud Data Analytics" on Journal of Advanced Research in Dynamical & Control Systems (JARDCS), IS SN (Online): 1943-023X, Vol. 10, 07-Special Issue, 2018.