Simulated Analysis of Using Artificial Neural Network to Identify Fake Images Based on Metadata

Rakesh Kumar
Department of Computer Engineering & Applications, GLA University, Mathura
rakesh.kumar@glu.ac.in

Abstract. Many phony pictures are spreading through advanced media these days. Identification of such phony pictures is unavoidable for the revealing of the picture based cybercrimes. Fashioning pictures what's more, recognizing such pictures are promising examination territories in this advanced time. The altered pictures are an identified utilizing neural organize which additionally perceives the locales of the picture that have been controlled and uncovers the sections of the first picture. It tends to be actualized on Android stage and subsequently made accessible to normal clients. The pressure proportion of the remote content in a phony picture is not the same as that of the first picture and is recognized utilizing Error Level Analysis. Another include utilized alongside pressure proportion is picture metadata. Despite the fact that it is conceivable to change metadata content creation it inconsistent all alone, here it is utilized as a supporting parameter for mistake level examination choice.

1. Introduction
In this innovative period an enormous number of individuals have become survivors of picture fraud. Many individuals use innovation to control pictures and use it as confirmations to delude the court. So to stop this, all the pictures that are shared through internet based life ought to be ordered as genuine or on the other hand counterfeit precisely. Current legal strategies require a specialist to investigate the believability of a picture. We actualized a framework that can decide if a picture is phony or not with the assistance of AI and in this manner making it accessible for the basic open. This paper will unfurl into three areas whereby first will concentrate on the subsequent Usage subtleties while the last part grandstand the test result.

The proposal present in this article uses three steps for fake image detection; Metadata Analysis, Error level Analysis, and Artificial Intelligence based machine learning approach. In which Metadata Analysis [1] gives insight of origin of the image that how it was produced and apportioned with. Result of Metadata is the clear distinction between the images with taking through camera, taking from any internet source or tricking something with the image. It helps out to be detect the forgery in image.

Figure 1 shows an altered picture utilizing Photoshop. The adjusted picture depended on the main 75% resave. Books on the rack were copied and a toy dinosaur was added to the rack. The Error Level Analysis (ELA) [2] identifies the headways, since it is the analysis based on zones to compare the negligible error level in original as well as fragile image. Extra zones of the image show a little bit
more shakiness on the dregs that combined from different layers, by dissecting the example in the ELA applied picture, we can figure out which some portion of the picture is perhaps faked. It is difficult for the natural eye to identify little scope changes to picture with the goal that we have chosen to utilize machine figuring out how to distinguish the peculiarities in the blunder level investigated pictures.

![Fig 1. Error level analysed image on the left and fake image on the right](image)

Rest of the paper organize as; section 2 discuss the review of literature proposed by some researchers, section 3 describe the methodology of proposal, followed by performance evaluation in section3, and lastly section 4 depicted the conclusion and future aspects of the proposal.

2. Literature Review

Various artificial intelligence based approaches are proposed by various researchers for detecting fake images and image authentication. This is the need of the day, that an effective and less complex image detection algorithm required. In this section, we review some of the methodology based on machine learning approaches for fake image detection.

In [3], author propose a robust authentication scheme to detect a tampered attack is proposed by using the parity bit and least significant bits. In another scheme [4], author develop passive image splicing detection method based on a new descriptor called Adaptive Threshold Mean Ternary Pattern, in which extraction feature is normally achieved by using proposed mean based thresholding and adaptive ternary thresholding. Similarly, in [5] three level technique is applied to authenticate the image origin, first to extract feature through employing convolutional neural network (CNN), secondly discrete wavelet transform (DWT) is used to represent the input parameters and, lastly classification is done through support vector machine (SVM). Another author [6] propose a copy-move forgery approach for digital images, in which a two dimensional discrete cosine transform is used to create the quantized coefficient matrix. The input is passed through this matrix in form of window for forgery detection. In another proposal [7], author also utilize machine learning technique names Naïve Bayes Classifier to detect suspected images. In [8], author proposed an approach to detect facsimile blocks in an image by using principal component analysis. Similarly, in [9], features are extracted through image statistics and pixel correlation from DCT and DWT domain. In [10], authors also use DWT to extract image features and classify the image in four parts to analyse. In [11], author use 2- level clustering to classify image and analyse.

In next section, we discuss the proposed framework of the Fake Image detection in detail, and in last we, analyses the findings of the proposed model.

3. Proposed Framework for Fake Image Detection

This section describes proposed framework to identify fake image in three steps; Meta Data Analysis, Error level Analysis, and Machine Learning Model for training. The framework is shown in Figure 2.
3.1. Metadata Analysis
The first step in the proposed framework is to extract metadata from images using metadata extractor library Metadata-extractor have dispersed metadata data of huge no of various picture types. Metadata contents extracted from images of interested area chosen for examination, then input to the metadata examination module to extract the features for analysis purposes.

Secondly, metadata analyser, analyse the featured content of the images and labelled them according to some logical background features of the image. On the off chance that catchphrases like Photoshop, Gimp, Adobe and so forth is found in the content and afterward the chance of being altered is expanded. Two separate factors are kept up which are called phoniness and realness. Every factor speaks to the heaviness of being genuine or counterfeit picture. While tag is taken in to account, it is investigated and concerning variable is increased by an assured weight. The accompanying Table 1 speaks to catchphrases and comparing weight increases. Subsequent to preparing the whole labels, last estimations of phoniness and realness variable is taken care of into the yield stage.

Table 1: Keyword listing

| Keyword   | Realness / Fakeness | Inc. Value |
|-----------|---------------------|------------|
| Photoshop | Fakeness            | 5          |
| Gimp      | Fakeness            | 5          |
| Corel     | Fakeness            | 5          |
| Adobe     | Fakeness            | 3          |
| Exit Info | Realness            | 2          |
| Camera Tags | Realness        | 2          |

3.2. Error Level Analysis
Image gives alternative to spare picture in JPEG group with certain level of pressure. The framework first spares a picture at 100% quality. At that point a similar picture is changed over into 90% quality picture utilizing Image. The distinction between these two is discovered however distinction strategy. The subsequent picture is the necessary ELA picture of the information picture. This picture is spared as a cushioned picture and sent to the neural organize for additional preparing.

3.3. Machine Learning
AI is executed utilizing Neuroph library for java. Neuroph is chosen in view of the effortlessness and effortlessness to execute neural systems. We have executed a multilayer perceptron coordinate with energy back proliferation learning rule.
In this step, image chosen for examine, first, it is handover to ELA stage to error level interpretation. More images are used to form ELA image, and whenever ELA image is pre-processed to convert and form it to 100 x100 pixel size. In the wake of pre-processing, the picture is serialized into an exhibit. The cluster contains 30,000 number qualities discourse to 10,000 pixels. 10,000 pixels will have 30,000 qualities, due to fact that, every pixel has red, green and blue segments. During preparing, the exhibit is given as contribution to the multilayer perceptron system and yield neurons likewise set.

A Multilayer Perceptron Neural (MLP) system is utilized for the testing purpose. Its having one input layer, 3 concealed layers and 1 yield layer. The MLP is a completely associated neural system. There are 2 yield neurons. First neuron is for speaking to counterfeit and the second one without a doubt picture. On the off chance that the given picture is phony one, at that point the phony neuron is set to one and genuine is set to zero. Else counterfeit is set to zero and genuine set to one. We have utilized force back propagation learning rule change the neuron association loads. It is a managed learning decides that attempts to limit the blunder work. The picked learning rate and force alongside accomplished effectiveness is given in Table 2. During testing, the picture cluster is taken care of into the info neurons also, estimations of yield neurons are taken. We have utilized sigmoid enactment work.

Table 2. Structure of MLP

| Layer               | Remarks                                |
|---------------------|----------------------------------------|
| Input Layer         | 30,000 neurons                         |
| Concealed Layer 1   | 5000 neurons, Sigmoid activation function |
| Concealed Layer 2   | 1000 neurons, Sigmoid activation function |
| Concealed Layer 3   | 100 neurons, Sigmoid activation function |
| Yield Layer         | 2 neurons                              |

4. Experimental Results and Discussion

The metadata investigation has indicated promising outcome in non-shared pictures. It can recognize abnormality taking all things together 'photo shopped' or 'gimped' pictures under a little preparing. It flopped on pictures shared through WhatsApp, Google+ and so forth. In addition, it turned out to be totally wrong when pictures with controlled metadata given.

CASIA dataset [12] is used for training on MLP. It contains 7491 genuine pictures and 5123 altered pictures under instable sizes. First of all, the input images are pre-processed to 100x100 pixels with the objective that all processing images will be of 30,000, which can be taken into the neural system for training. 4000 genuine and phony images are considered for training dataset, and remaining images are utilizing to test the neural system. Table 3 shows different neural system setups and comparing neural arrange effectiveness. Best is accomplished when learning rate set to 0.2 and energy to 0.7.
Table 3. Neural Network Training Results

| Learning Rate | Momentum | Epoch | Efficiency |
|---------------|----------|-------|------------|
| 0.01          | 0.5      | 500   | 60%        |
| 0.05          | 0.5      | 500   | 62%        |
| 0.1           | 0.5      | 500   | 68%        |
| 0.2           | 0.5      | 500   | 66%        |
| 0.1           | 0.4      | 500   | 69%        |
| 0.1           | 0.3      | 500   | 68%        |
| 0.1           | 0.6      | 500   | 75%        |
| 0.1           | 0.7      | 500   | 76%        |
| 0.2           | 0.7      | 500   | 82%        |
| 0.2           | 0.7      | 1000  | 83%        |

5. Conclusion
Neural system has been effectively prepared utilizing the mistake level investigation with 4000 phony and 4000 genuine pictures. The prepared neural system had the option to perceive the picture as phony or then again genuine at a most extreme achievement pace of 83%. The utilization of this application in versatile stages will incredibly diminish the spreading of phony pictures through online life. This task can likewise be utilized as a bogus confirmation strategy in computerized verification, court proof assessment and so on. By joining the aftereffects of metadata examination (40%) and neural system yield (60%) a solid phony picture identification program is created what's more, tried.

References
[1] Darmawan, I. Gede Nengah Bayu, Gusti Made Arya Sasmita, and Putu Wira Buana. "Pengembangan Metode Pendeteksi Modifikasi Citra Menggunakan Metode Error Level Analysis." MERPATI VOL 7 (2019): 29-36.
[2] Troncy, R., Huet, B., & Schenk, S. (Eds.). (2011). Multimedia semantics: metadata, analysis and interaction. John Wiley & Sons.
[3] Jung, Ki-Hyun. (2016). Block-Based Authentication Scheme for Forgery Attacks on Digital Images. Advanced Science Letters. 22. 2583-2587. 10.1166/asl.2016.7784.
[4] A. A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad and G. Bebis, "Splicing image forgery detection based on DCT and Local Binary Pattern," 2013 IEEE Global Conference on Signal and Information Processing, Austin,TX, 2013, pp. 253-256.
[5] Abd El-Latif, E. I., Taha, A., & Zayed, H. H. (2020). A Passive Approach for Detecting Image Splicing Based on Deep Learning and Wavelet Transform. Arabian Journal for Science and Engineering, 1-8.
[6] Kaushik, Rajeev, Bajaj, Rakesh Kumar, Mathew, Jimson, “On Image Forgery Detection Using Two Dimensional Discrete Cosine Transform and Statistical Moments,” 2015 Proceedings of the 4th International Conference on Eco-friendly Computing and Communication Systems, 2015, SN 1877-0509.
[7] A. Hilal, T. Hamzeh and S. Chantaf, "Copy-move forgery detection using principal component analysis and discrete cosine transform," 2017 Sensors Networks Smart and Emerging Technologies (SENSSET), Beirut, 2017, pp. 1-4.
[8] M. F. Hashmi, A. R. Hambarde and A. G. Keskar, "Copy move forgery detection using DWT and SIFT features," 2013 13th International Conference on Intelligent Systems Design and
Applications, Bangi, 2013, pp. 188-193.

[9] Babu, S. T., & Rao, C. S. (2020, July). Statistical Features based Optimized Technique for Copy Move Forgery Detection. In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.

[10] Jaiprakash, S. P., Desai, M. B., Prakash, C. S., Mistry, V. H., & Radadiya, K. L. (2020). Low dimensional DCT and DWT feature based model for detection of image splicing and copy-move forgery. Multimedia Tools and Applications, 79(39), 29977-30005.

[11] Abdel-Basset, M., Manogaran, G., Fakhry, A. E., & El-Henawy, I. (2020). 2-Levels of clustering strategy to detect and locate copy-move forgery in digital images. Multimedia Tools and Applications, 79(7), 5419-5437.

[12] Dong, J., Wang, W., & Tan, T. (2013, July). Casia image tampering detection evaluation database. In 2013 IEEE China Summit and International Conference on Signal and Information Processing (pp. 422-426). IEEE.