JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Fake Image Detection using deep learning and local binary patterns

Gosangi Alekhya, A.Mary Sowjanya, J.Aruna Devi
Department of Computer Science and Systems Engineering, Andhra University College of Engineering(A), Visakhapatanam, Andhra Pradesh

Abstract Biometric technology are helpful in identifying people today, but criminals alter their look, behaviour, and psychological makeup to trick identification systems. We are employing a novel method called Deep Texture Features extraction from photos to solve this challenge, followed by the construction of a machine learning model using the CNN (Convolution Neural Networks) algorithm. This method is also known as LBPNet or NLBPNet since it relies so heavily on the LBP (Local Binary Pattern) algorithm for features extraction. LBPNET, a machine learning convolution neural network, is the name of the network we created for this research to identify fraudulent face photographs. Here, we will first extract LBP from the photos, and then we will train the convolution neural network on the LBP descriptor images to produce the training model. Every time a new test image is uploaded, the training model will use that image to determine if the test image contains fraudulent images or not.

Keywords: - LBP,CNN,LBPNET, biometric

I Introduction

This project's goal is to recognise false photos (Fake images are the images that are digitally altered images). The issue with current fake picture detection systems is that they can only be used to detect particular types of tampering, such as cutting, colouring, and so on. To solve the issue, we used machine learning and neural networks to identify practically all types of picture manipulation.It is possible to make changes to images that are too subtle for the human eye to notice by using the most recent image editing software. Without discovering a common characteristic that almost all fraudulent photographs have, it is impossible to tell if an image is phoney or not, not even with a sophisticated neural network. As a result, we provided an image with the error level assessed rather than just the raw pixels to the neural network.

This project offers a two-level picture analysis. It initially examines the image metadata. Given that it may be changed with a few simple tools, image metadata is not very dependable. However, the majority of the photographs we encounter include non-altered metadata, which makes it easier to spot the changes. If an image is modified with AdobePhotoshop, for instance, the metadata will also include the version of Adobe Photoshop that was used.The image is changed into an error level-analyzed format and downsized to a 100px by 100px image in the second level. Following that, 30,000 inputs totaling 10,000 RGB-valued pixels are provided to the input layer of a multilayer perceptron network. Contains two neurons in the output layer. a fake image and a real image, respectively. We decide whether the image is false or real and how likely it is that the provided image has

been altered based on the value of these neuron outputs and the output from the metadata analyzer.

2 Literature survey

Hsu, C ; Lee C et al. [1] have proposed a novel deep forgery discriminator(DeepFD) to detect fake images generated by state of the art GANS based on contrastive loss.To address the existing shortcomings they had adopted contrastive loss in extracting the typical features of fake/generated images generated by different GANS.Their results have shown that their proposed system DeepFD had detected 94.7% fake images which are generated by several state of the art GANS.

Hsuan T. Chang, Chih-Chung Hsu et al. [2] have introduced a blind watermarking theme to perform image authentication and change of state localization within the receiver.So based on the extracted watermark, they had determined whether the received image is tampered or not.so to detect whether the image is tampered or not, they have proposed methods like Sequential watermark alignment based on coefficient stamping(SWACS) and morphological region growing and subband duplication(MRGSD) which determine the positions of modified pixels in the misreported watermark and to identify the tampered region.

Chih-Chung Hsu,Tzu-Yi Hung et al. [3] have proposed a new system for detecting forged regions in video in which they have got used correlation of noise residue.They modeled the system as GMM(Gaussian mixture model),where they have got proposed two-step scheme to estimate model parameters and they have extensively utilized Bayesian classifer to find best threshold value.In their experiments, two video inpainting schemes are used to simulate two unique sorts of tampering procees.Their experimental outcomes have shown that their proposed system had achieved higher accuracy for the videos.

Zheng et al. [5] found that it is particularly challenging to spot fake news and photographs since it is impossible to verify content on a pure basis and there aren't many models for doing so. can be utilised to fix the issue. It has been suggested that the issue of "detecting bogus news" be studied. Many useful characteristics of the language, words, and images utilised in fake news are discovered through a thorough analysis. A collection of hidden attributes produced from this model across several layers can be used to identify some hidden traits in the words and visuals used in fake news. The TI-CNN pattern has been suggested. By presenting distinct and integrated features in a same area, TI-CNN is trained simultaneously using text and image data.

To detect fake accounts on social networks, particularly Facebook, Raturi's 2018 design [6] was developed. Based on the posts and their location on social networking walls, a machine learning feature was utilised in this study to more accurately forecast bogus accounts. In order to validate content based on text classification and data analysis, Support Vector Machine (SVM) and Complement Nave Bayes (CNB) were utilised. The gathering of derogatory words and their frequency of occurrence were the main topics of the data analysis. For Facebook, SVM displays a 97% resolution, whilst CNB displays a 95% accuracy in Bag of Words recognition (BOW) counterfeit accounts with a basis. The study's findings demonstrated that the primary issue was safety of The problem with social networks is that published data is not thoroughly verified.

Two approaches were suggested in a 2017 study by Bunk et al [7] to detect and pinpoint fraudulent photos using a combination of resampling attributes and deep learning. In the original system, overlapping picture adjustments are used to estimate the Radon conversion of resampling parameters. A heat map is then created using deep learning classifiers and a Gaussian conditional domain pattern. Total areas are used in a Random Walker segmentation technique. Software resampling attributes are passed on overlapping object patches over an LSTM-based network in the following system for identification and localization. The effectiveness of both systems' detection and localization capabilities was also contrasted. The outcomes demonstrated the effectiveness of both systems in identifying and resolving digital picture fraud.

The goal of Aphiwongsophon and Chongstitvatana [8] was to identify fake news using machine learning

approaches. In the experiments, Nave Bayes, Neural Networks, and Support Vector Machines were three widely employed methods (SVM). Prior to applying the machine learning method to sort data, the normalisation method is a crucial stage in data cleaning. The findings indicate that Nave Bayes has a 96.08% accuracy in identifying fake news. The Neural Network Machine and the Support Network (SVM) are two other sophisticated techniques that attain 99.90% accuracy.

A neural network was successfully trained in [9] by Kuruvilla et al. by comparing the error levels of 4000 real photos and 4000 fake images. With an impressive 83% success rate, the trained neural network was able to determine whether the image was real or phoney. According to the findings, spreading of false photos on social networks is dramatically decreased when using this software on mobile platforms. Furthermore, this can be applied as a fake image verification technique in digital authentication, the evaluation of court evidence, etc. By merging the output of the neural network (80%) with the findings of the metadata analysis (80%), it creates and tests a reliable false picture detecting algorithm.

Digital forensics techniques are required, according to [10] Kim's and Lee's, to identify alteration and phoney photos used for criminal activities. Because deep learning technology has produced impressive results in recent research, the researchers in this study have been developing an algorithm to detect false photos using it. An altered neural network is used to process images first. In addition, hidden features rather than semantic data in the image are sought after using a high pass filter. Using an intermediate filter, a Gaussian blurring effect, and additional white Gaussian noise, modified images are produced for experimentation.

The method being developed in this study uses the CNN model to classify input images. CNNs are excellent feature extractors for tasks or problems that are entirely new. By feeding your data at each level and slightly adjusting the CNN for the particular task, it pulls usable attributes from an already trained CNN with its taught weights. In order to expand on current networks, a CNN can be retrained for new recognition tasks. This process of saving time by not training a CNN from scratch is known as pre-training. For the specified task, CNN can do automatic feature extraction. Since the features are directly learned by the CNN, manual feature extraction is not necessary. For image recognition tasks and many other tasks where it provides a high accuracy and accurate result, CNNs exceed several approaches in terms of performance. Weight sharing, which essentially means using the same weight for two layers of the model, is another important characteristic of CNNs. Due to the aforementioned benefits and features, CNN is chosen in this study over other deep learning algorithms.

3. Methodology

This technique involved using Complement Nave Bayes (CNB) and Support Vector Machines (SVM) to validate content based on text classification and data analysis. The gathering of objectionable terms and the frequency with which they were used were the main topics of the data analysis.

CNN type. CNNs are excellent feature extractors for tasks or problems that are entirely new. By feeding your data at each level and slightly adjusting the CNN for the particular task, it pulls usable attributes from an already trained CNN with its taught weights. In order to expand on current networks, a CNN can be retrained for new recognition tasks. This process of saving time by not training a CNN from scratch is known as pre-training. For the specified task, CNN can do automatic feature extraction. Since the features are directly learned by the CNN, it does not require manual feature extraction..

For image recognition tasks and many other tasks where it provides a high accuracy and accurate result, CNNs exceed several approaches in terms of performance. Weight sharing, which essentially means using the same weight for two layers of the model, is another important characteristic of CNNs. Due to the aforementioned benefits and features, CNN is chosen in this study over other deep learning algorithms.

LBP-Local Binary Pattern is a type of visual descriptor used for classification in computer vision and is a simple yet very effiecient texture operator

which labels the pixels of an image by thresholding the neighborhood of each pixel and considers the result as binary number.In our project we are designing LBP based machine learninig Convolution Neural Network called LBPNET to detect fake images.

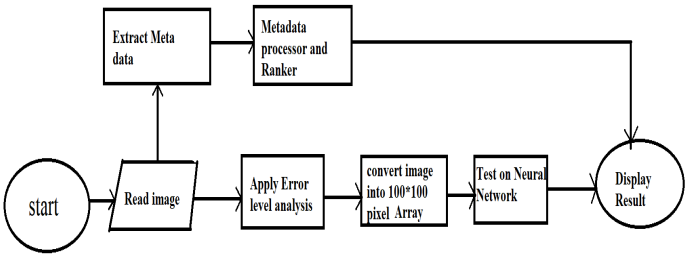

Fig 1: Proposed System

MODULES

1) Load and analyze image data: As a data store for the image, load the sample's data. Data is stored as an object of the picture data store and automatically tagged photographs depending on the name of the folder. When training a convolution neural network, an image data storage makes it easier to store and understand big image batches.

2) Define the network architecture:

Establish the network layers and neural network architecture.

3) Define training options:

After specifying the network's architecture, defines the training possibilities. epochs, batch size, momentum, and learning rate.

4) Train the network: Utilize the training options, training data, and layer-defined architecture to train the network.

5) Predict new data labels and assess classification accuracy

Algorithm 1. LBP – based using a sliding window implementation

Input: $Im + + + age\ I$
$LBP - based\ techniques\ T = [\ LBP, ULBP, CS - LBP, CS - LTP, CS - LMP]$
$sliding\ window\ overlaps\ O = 0.5$
output: $Histograms\ of\ LBP - based\ techniques\ using\ a\ sliding\ window\ approach$
$[HIST_{LBP}, HIST_{ULBP}, HIST_{CS-LBP}, HIST_{CS-LTP}, HIST_{CS-LMP}]$
Begin
$Resize\ I\ to\ be\ H \times W, where\ W = 32, H = 32$
$Sliding\ windows\ S = [(W/2, H/2), (W/2, H/4), (W/4, H/2), (W/4, H/4)].$
For $i = 1\ to\ length\ (S)$
$number\ of\ windows\ in\ x - axis\ \ X = (W/(S(i,1) * O) - 1)$
$number\ of\ windows\ in\ y - axis\ \ Y = (H/(S(i,2) * O) - 1)$
For $j = 1\ to\ X$
$sliding\ window\ start\ point\ in\ x - axis\ XS = (j-1) * S(i,1) * O + 1;$
$sliding\ window\ end\ point\ in\ x - axis\ XE = ST + 2 * S(i,1) * O - 1;$
For $k = 1\ to\ Y$
$sliding\ window\ start\ point\ in\ y - axis\ YS = (k-1) * S(i,2) * O + 1;$
$sliding\ window\ end\ point\ in\ x - axis\ YE = YS + 2 * S(i,2) * O - 1;$
$the\ part\ of\ image\ extracted\ via\ sliding\ window\ PI$
$= I(XS\ to\ XE, YS\ to\ YE)$
$HIST_{LBP}(i) = LBP(PI)$
$HIST_{ULBP}(i) = ULBP(PI)$
$HIST_{CS-LBP}(i) = CS - LBP(PI)$
$HIST_{CS-LTP}(i) = CS - LTP(PI)$
$HIST_{CS-LMP}(i) = CS - LMP(PI)$
End
End
End
End

Fig 2: lbpnet alogritham

4 Results and Evolution Metrics

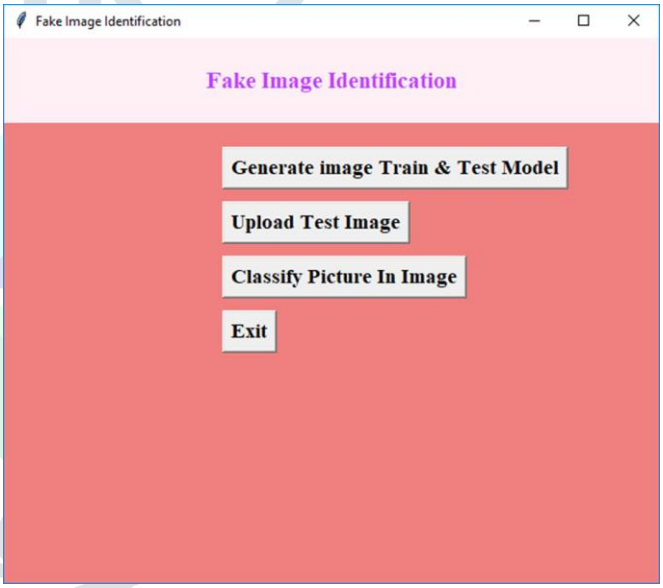

Fig 3: home page

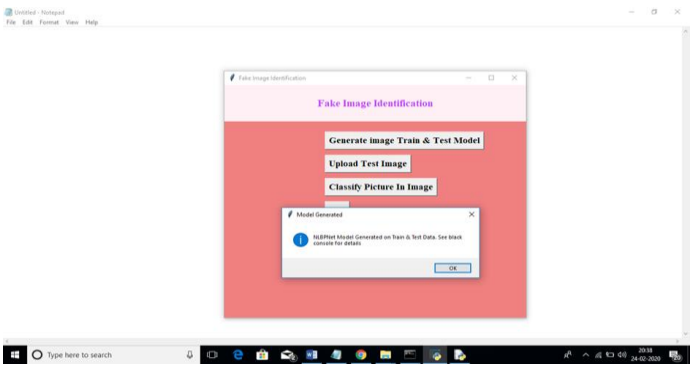

Fig 4: generate train and test image

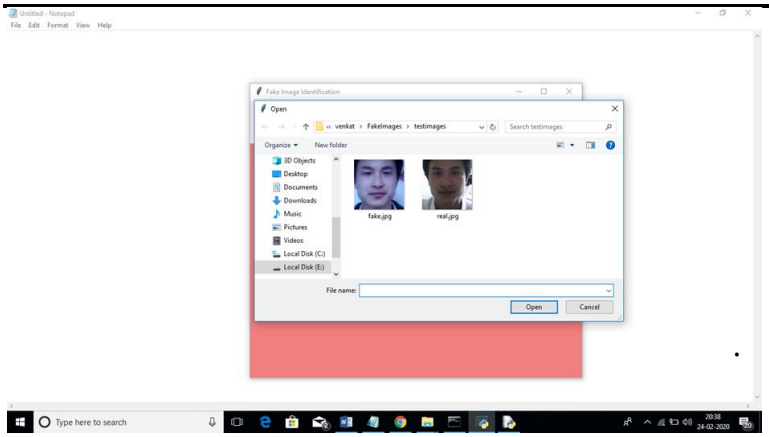

Fig 5: In above screen upload an image

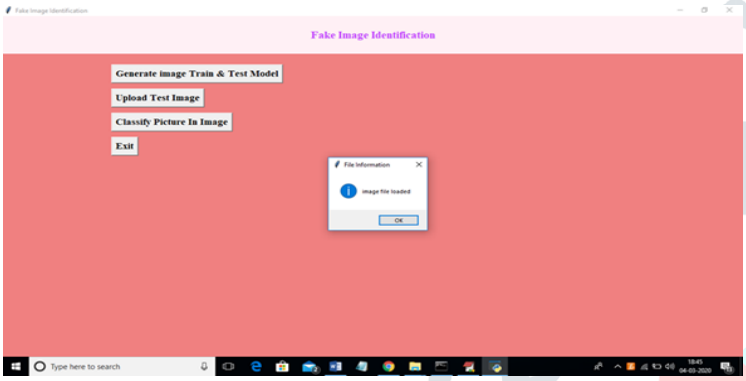

Fig 6 : image loaded

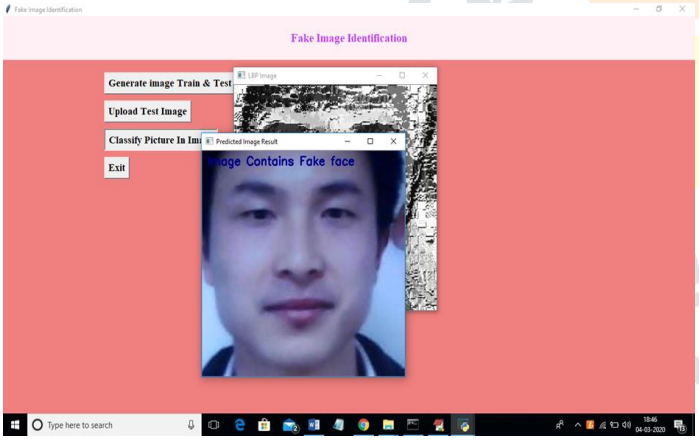

Fig 7: image classified by LBPNET

5 Conclusion

In this paper, we present a unique paired learning-based common fake feature network to accurately detect fake face/general images produced by cutting-edge GANs. By combining the cross-layer feature representations into the final fully connected layers, the proposed CFFN can be utilised to train middle- and high-level and discriminative fake features. The performance of false picture detection can be further enhanced using the suggested paired learning. The proposed fake image detector should be able to recognise the false image produced by a fresh GAN with the help of the proposed pairwise learning. Our test findings showed that the suggested strategy works better in terms of precision and recall rate than other cutting-edge schemes.

References

[1] Hsu, C.; Lee, C.; Zhuang, Y. Learning to detect fake face images in the Wild. 2018 International Symposium 264 on Computer, Consumer and Control (IS3C), 2018, pp. 388–391. doi:10.1109/IS3C.2018.00104.

[2] H.T. Chang, C.C. Hsu, C.Y.a.D.S. Image authentication with tampering localization based on watermark 266 embedding in wavelet domain. Optical Engineering 2009, 48, 057002.

[3] Hsu, C.C.; Hung, T.Y.; Lin, C.W.; Hsu, C.T. Video forgery detection using correlation of noise residue. Proc. of the IEEE Workshop on Multimedia Signal Processing. IEEE, 2008, pp. 170–174.

[4] Ravi, K., 2018. Detecting fake images with machine learning. *Harkuch J*.

[5] Yang, Y., Zheng, L., Zhang, J., Cui, Q., Li, Z. and Yu, P.S., 2018. TI-CNN: Convolutional neural networks for fake news detection. *arXiv preprint arXiv:1806.00749*.

[6] Raturi, R., 2018. Machine learning implementation for identifying fake accounts in social network. *International Journal of Pure and Applied Mathematics*, *118*(20), pp.4785-4797.

[7] Bunk, J., Bappy, J.H., Mohammed, T.M., Nataraj, L., Flenner, A., Manjunath, B.S., Chandrasekaran, S., Roy-Chowdhury, A.K. and Peterson, L., 2017, July. Detection and localization of image forgeries using resampling features and deep learning. In *2017 IEEE conference on computer vision and pattern recognition workshops (CVPRW)* (pp. 1881-1889). IEEE.

[8] Aphiwongsophon, S. and Chongstitvatana, P., 2018, July. Detecting fake news with machine learning method. In *2018 15th international conference on electrical engineering/electronics, computer, telecommunications and information technology (ECTI-CON)* (pp. 528-531). IEEE.

[9] Villan, M.A., Kuruvilla, A., Paul, J. and Elias, E.P., 2017. Fake Image Detection Using Machine Learning. *IRACST-International Journal of Computer Science and Information Technology & Security (IJCSITS)*.

[10] Kim, D.H. and Lee, H.Y., 2017. Image manipulation detection using convolutional neural network. *International Journal of Applied Engineering Research*, *12*(21), pp.11640-11646.