IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

FORGERY DETECTION USING DEEP FEATURES IN DIGITAL IMAGES

P.Thanumathi [1], Dr.K.Merriliance[2]

Department of Computer Applications, Sarah Tucker College, Thirunelveli-7.

ABSTRACT:

Due to a multi-fold growth in the diffusion of multimedia data through the open and unprotected Internet, content authentication of digital photographs has caught the attention of forensic professionals and security researchers. Attackers who are astute come up with new approaches to test state-of-the-art forensic tools for detecting forgeries in digital photographs. On benchmarked datasets, feature engineering techniques have produced accuracy of up to 97 percent. Deep learning algorithms have showed promise in a variety of picture classification tasks, but they are unable to discover hidden patterns in digital images that can be used to consistently detect image forgeries. Deep learning techniques for forgery detection have a state-of-the-art accuracy of up to 98 percent on benchmarked datasets. The proposed approach aims to improve detection accuracy even more, bringing it close to 100%. To mine patterns responsible for accurate forgery detection, this work uses a synergy of created features based on colour attributes and deep features using the image's luminance channel. The first Stream computes 648-D Markov-based features from the image's quaternion discrete cosine transform. In the second Stream, the image's Local Binary Pattern is extracted using the YCbCr colorspace's luminance channel. Local binary feature maps are also input into the pre-trained ResNet-18 model to get a 512-D feature vector named 'ResFeats' from the model's convolutional base portion's last layer. An 1160-D feature vector is created by combining handcrafted features from Stream I and ResFeats from Stream II. The method is also tested on the CASIA v1 and CASIA v2 datasets, and classification is done with a shallow neural network. On benchmark datasets, the suggested fusion-based technique has a 99.3 percent accuracy.

INTODUCTION:

The quantity of photographs transferred and shared on web-based media platforms such as WhatsApp, Instagram, Facebook, YouTube, and others has increased dramatically as a result of their widespread use.These digital images are used to disseminate information to a big audience and, as a result, build a broad public opinion. Images are vulnerable to fraudulent modifications due of the ease

with which software and editing tools are available on the Internet. Images like these are shared on social media and even used in courtrooms, literature, research and medicine, the military, and other places. The act of modifying photos to exhibit misleading information is referred to as image forging and is divided into two categories: active and passive techniques. Active approaches [5] rely on prior knowledge about the image being considered. It contains a digital watermark or digital signatures encoded in the image, which are extracted at the receiver end and compared to the original watermark/signature.

Passive approaches, on the other hand, are used when no prior knowledge is available. The intrinsic changes in images due to underlying alterations are determined using the pixels of an image. To identify between counterfeit and legitimate photos, several inherent properties from highly discriminable images must be retrieved.

The strategy proposed in this research is groundbreaking in four ways:

1. This is the first method for identifying picture modifications that combines high-level, in-depth features with manually generated image attributes. On the CASIA v1 and CASIA v2 datasets, combining deep high-level features and manually generated picture features boosted detection accuracy compared to standard state-of-the-art detection approaches.

2. In the case of handmade feature extraction, three channels of RGB colour space are employed, and the luma channel of YCbCr colour space is used in the case of deep features to identify forgeries in photos. Forgeries in digital photographs have been effectively identified using complimentary information in two different colorspaces.

3. Instead of sending RGB images directly, we input the pre-trained ResNet-50 model Scale and Orientation invariant local binary pattern maps of the image. LBP's rich textural description capacity aids the deep neural network in producing a more meaningful and low-dimensional representation.

4. For classification, a fused feature vector is utilised to train a shallow neural network.

LITERATURE SURVEY:

In this work, we have presented a new method for detecting copy-move forgeries in digital photos that is much more resistant to lossy compression, scaling, and rotation. We also propose using counting bloom filters as an alternative to lexicographic sorting, which is a common component of most proposed copy-move forgery detection techniques, to reduce the computational complexity of finding duplicated picture regions.The proposed characteristics can recognise duplicated regions in photos quite accurately, even when the copied region has been subjected to severe image alterations, according to our results. Furthermore, using counting bloom filters improves time efficiency while reducing robustness slightly.

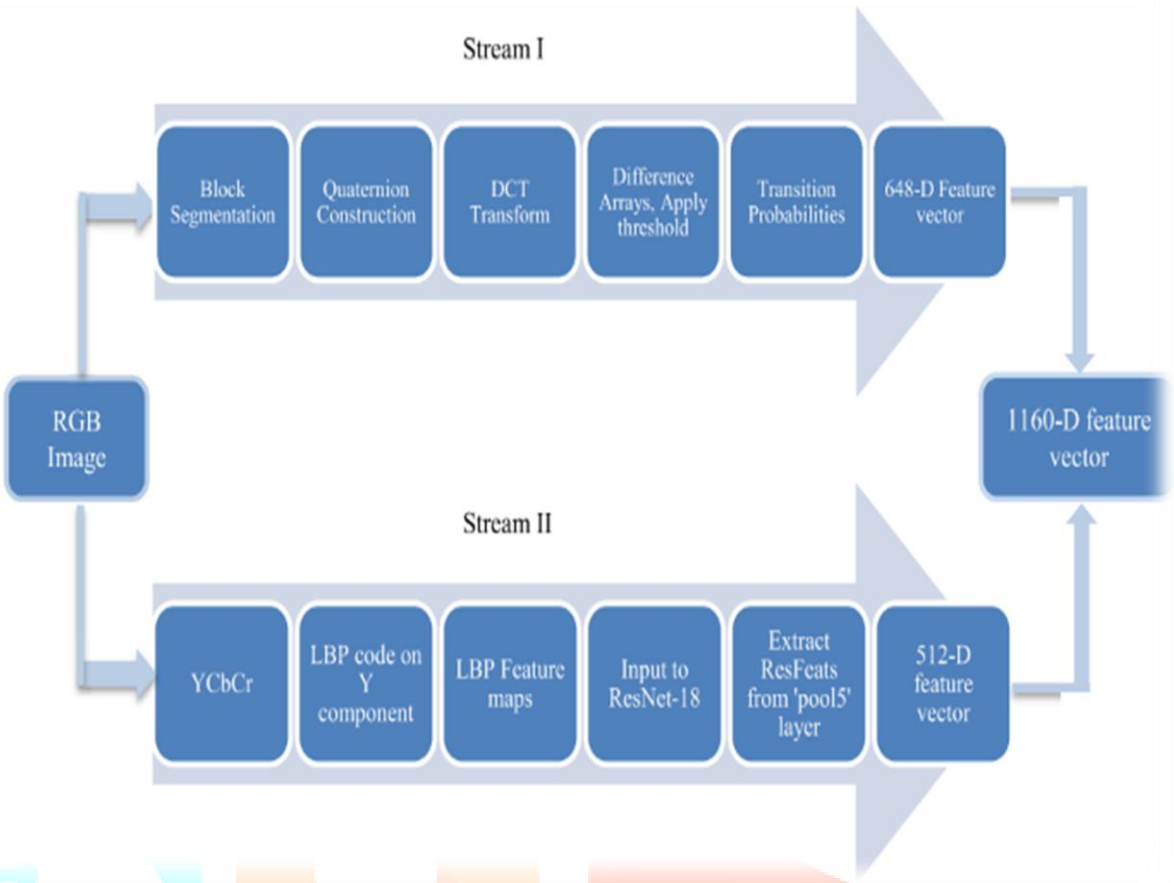
In this work, we have investigated numerous passive block-based copy move forgery detection algorithms in this work. Without any prior knowledge, a passive technique aims to detect forgeries in digital photographs. There's also a comparison of different techniques.

In this work we can compare and assess their suggested tampering detection algorithms using the database, which is open to the public.CASI-A Image Tampering Detection Evaluation Database is the name of the database. In this work, we present the database's aim, design criteria, organisation, and self-evaluation.

We have presented a modified model that uses batch normalisation instead of local Response normalisation, a maxout activation function instead of a rectified linear unit, and a softmax activation function in the last layer to operate as a classifier to optimise the AlexNet model.As a result, the AlexNet suggested model can perform feature extraction as well as forgery detection without the need for additional manipulations. We investigate and differentiate the effects of many key AlexNet design decisions through a series of experiments. On the CASIA v2.0, CASIA v1.0, DVMM, and NIST Nimble Challenge 2017 datasets, the proposed networks model is used. We also partition datasets into training and test data samples using k-fold cross-validation. The obtained experimental findings show that the suggested model is capable of recognising various types of forgeries with high accuracy. The suggested model can detect image forgeries with 98.176 percent accuracy, according to quantitative performance analysis.

PROPOSED METHODOLOGY:

The suggested method mines features using two streams, which are then combined to yield the most discriminable features. Handcrafted and in-depth features can represent various types of information from input photos, improving detection accuracy. The block diagram of two separate streams utilised for feature representations is shown in Figure. The following information is provided:



A. STREAM I: HANDCRAFTED FEATURE ENGINEERING:

According to the research, most Markov model-based techniques treat the image as a 1-D signal. Traditional techniques depict simply the state circumstances between nearby states and specified directions (vertical, horizontal). State dependencies on minor and major diagonals are also taken into account in this technique to better portray the image. Algorithm 1 provides the pseudocode for obtaining handcrafted features.The image has been divided into 8 x 8 blocks. Separately extracted and processed are the three colour components. The feature vector on the quaternion discrete cosine transformation of an RGB image is also formulated using intra-block and inter-block differences in vertical, horizontal, and diagonal directions.

STREAM II: EXTRACTING OFF-THE-SHELF FEATURES 'RESFEATS' FROM RESNET

Mahmood et al. coined the name ResFeats to describe a method for improving underwater picture classification accuracy by combining low- and high-level features derived from different residual blocks of the network. Similarly, we may use ResNet-18 architecture to extract rich textural features by feeding the model local binary pattern codes.The stages for extracting ResFeats are detailed below, and Algorithm 2 contains the pseudocode for this Stream:

1) RGB TO YCbCr

Because the R, G, and B colour channels of the image were considered in Stream I, we wish to employ the image's achromatic features in Stream II because we used chromatic components in Stream I.

For further processing, the luminance component of the YCbCr colour system is used. The YCbCr colour space uses the human eye's features to characterise colour as intensity.

Algorithm 1 Extract_deep_features

Input: IRGB: RGB image

Output: Vector of 512-dimensional deep features, Df Preprocessing;

IRGB → IYCbCr

IYCbCr → Y_channel

Apply Scale Orientation invariant Local Binary patterns;

SO_LBP = LBP(Y_channel)

Feature_maps = Multi_Dimensional_Scaling(SO_LBP)

Load the pre-trained Resnet18 model;

Net = Load(resnet18) Df = Extract_features(Net,preprocessed_images,layer, 'pool5')

Return Df

The advantage of YCbCr color space is that it can separate luminance from chrominance more efficiently than RGB color space. Luminance in the image is light intensity, or the amount of light ranges from black to white. The point of a luminance channel is to capture all of the available (visible) wavelengths at the same time and enable you to concentrate combining your noise reduction (through stacking), sharpness, and detail efforts into a single layer Equation 1 shows how to obtain a YCbCr representation from RGB colorspace.

C. CLASSIFICATION OF FUSED FEATURES USING A SHALLOW NEURAL NETWORK

Using Algorithm 2, 648-D handcrafted features and 512-D ResFeats are combined to generate a 1160-D feature vector of pictures called Ff. The feature vector dataset is normalised with the z-score approach to avoid outliers. A shallow neural network (SNN) with two feed-forward layers and a sigmoid function on the hidden layer and a softmax function on the output layer is used to categorise the normalised 1160-D feature vectors. The network's structure is depicted in Figure 3. For weight and bias value updates, the network is trained using the scaled conjugate gradient method.

Algorithm 2 Fused_features

Input: Hf , Df

Output: Fused features, Ff

Concatenate Hf and Df

Ff → [Hf, Df]

Return Ff

Experimental Result:

Functional Documentation plays a vital role in describing the various functionalities of the project. Basically, it considers the various forms designed for the project and explains various functions associated with the form. As a matter of fact, each form is an integrated part of the project and has its own, intended functionality. In this section, we explain the functional documentation of the project. It considers various blocks of the modules and the associated forms.

Algorithm 3 Extract_handcrafted_features

Input: IRGB: RGB image

Output: Vector of 648-dimensional handcrafted features, Hf

Begin

Repeat

Load image_file()

Segment the image_file using 8 × 8 blocks

Construct a Quaternion from color channels of the image

Apply Forward DCT transform

Until Making_8 × 8_2D matrix;

Block_Rearrangement();

Compute_2D_FFT();

FDCT_coefficients();

Compute quantisation and dequantisation

Compute DFT coefficients to further compute 2D IFFT

End Until_finished_image_file

For block_list

Calculate QV, QH, QD, and Q-D

Calculate RV, RH, RD, and R-D

Calculate transitional probabilities

Return Hf of size (2T + 1) × (2T + 1) × 8 for T = 4

Output:

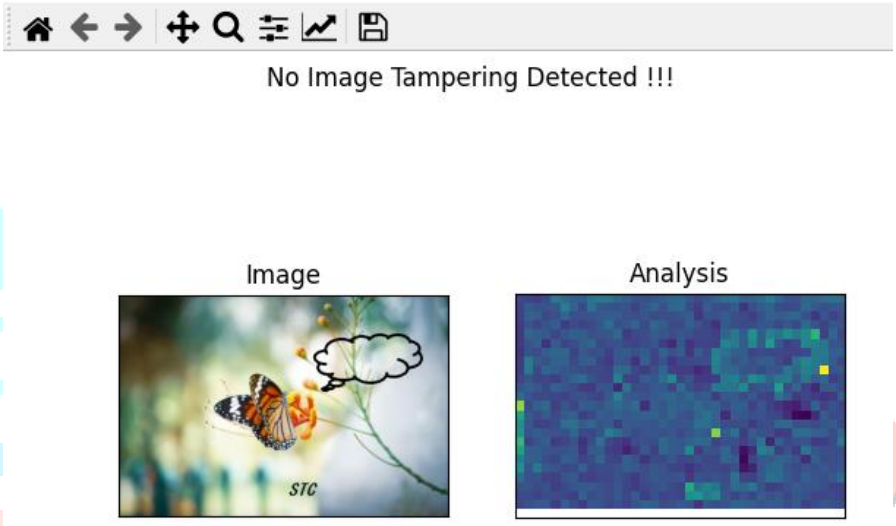


Fig 1: No Image Tampering Detected

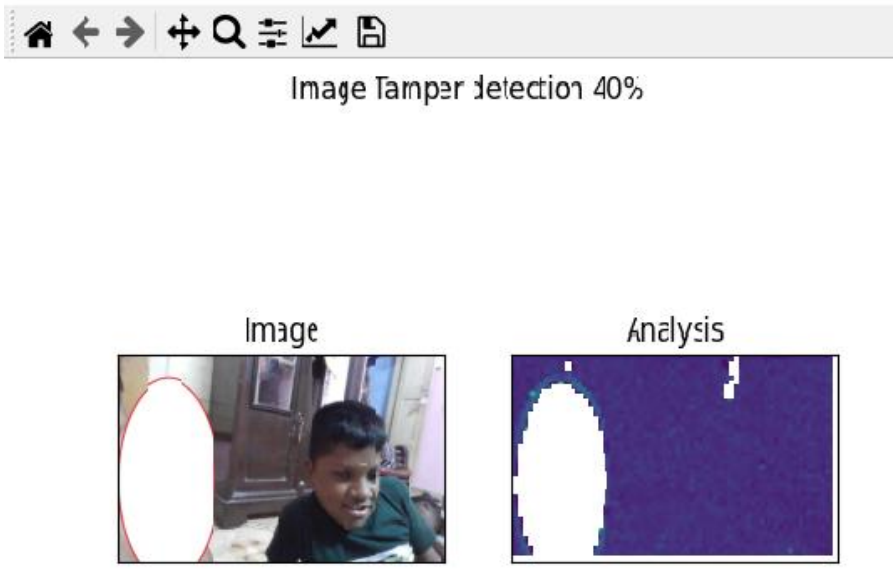


Fig 2: 40% of Image Tampering has been Detected

CONCLUSION:

Smart attackers create forgeries in digital photos so that state-of-the-art forensics technologies are unable to reliably track abnormality features. Deep learning approaches, on the other hand, are well known for providing the knowledge needed to generate high-level features suited for categorization issues. Furthermore, handcrafted features derived from photos that have been carefully constructed function admirably with relatively high accuracies.In the case of forgery detection, however, attackers have an advantage over state-of-the-art deep learning systems and manually built features, according to research. Therefore, this paper proposes a novel feature fusion-based approach that exploits RGB color space and luminance channels to trap forgeries in digital images. On the other hand, high-level deep image features based on luminance components and textural characteristics have performed up to the mark for false negative cases of manually engineered features. Moreover, LBP-based pre-processing of raw images has immensely improved the classification of scaled and rotated images in benchmarked datasets. As a result, combining the two types of image features improves detection accuracy significantly when compared to employing a single method or other modern methods. The proposed method for offline forensic analysis of digital photographs appears to be promising. The fundamental obstacle for real-time analysis is the high dimensionality of fused features. In the future, the authors will look into new techniques to reduce the feature complexity of the suggested fusion-based strategy .This work concluded that the ResNet-50 obtained 99.3%

REFERENCES

[1] S. Bayram, H. Taha Sencar and N. Memon, "An efficient and robust method for detecting copy-move forgery," *2009 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2009, pp. 1053-1056, doi: 10.1109/ICASSP.2009.4959768.

[2] T. Mahmood *et al.*, "A survey on block based copy move image forgery detection techniques," *2015 International Conference on Emerging Technologies (ICET)*, 2015, pp. 1-6, doi: 10.1109/ICET.2015.7389169.

[3] G. Muzaffer and G. Ulutas, "A new deep learning-based method to detection of copy-move forgery in digital images," *2019 Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT)*, 2019, pp. 1-4, doi: 10.1109/EBBT.2019.8741657.

[4] X. Zhao, S. Wang, S. Li and J. Li, "Passive Image-Splicing Detection by a 2-D Noncausal Markov Model," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 25, no. 2, pp. 185-199, Feb. 2015, doi: 10.1109/TCSVT.2014.2347513.

[5] Nguyen, D.T.; Pham, T.D.; Baek, N.R.; Park, K.R. Combining Deep and Handcrafted Image Features for Presentation Attack Detection in Face Recognition Systems Using Visible-Light Camera Sensors. *Sensors* **2018**, *18*, 699. https://doi.org/10.3390/s18030699

[6] Ullah, J. Ahmad, K. Muhammad, M. Sajjad and S. W. Baik, "Action Recognition inVideo Sequences using Deep Bi-Directional LSTM With CNN Features,"

in *IEEE Access*, vol. 6,pp1155-1166, 2018, doi: 10.1109/ACCESS.2017.2778011.

[7] M. Hussain, S. Q. Saleh, H. Aboalsamh, G. Muhammad and G. Bebis, "Comparison between WLD and LBP descriptors for non-intrusive image forgery detection," 2014 IEEE International Symposium on Innovations in Intelligent Systems and Applications (INISTA) Proceedings, 2014, pp.197-204, doi: 10.1109/INISTA.2014.6873618.

[8] J. Dong, W. Wang and T. Tan, "CASIA Image Tampering Detection Evaluation Database," 2013 IEEE China Summit and International Conference On Signal and Information Processing, 2013, pp. 422-426, doi: 10.1109/ChinaSIP.2013.6625374.

[9] Samir, S.; Emary, E.; El-Sayed, K.; Onsi, H. Optimization of a Pre-Trained AlexNet Model for Detecting and Localizing Image Forgeries. *Information* **2020**, *11*, 275. https://doi.org/10.3390/info11050275