Image Tampering Detection Using Learning with Neural Network

Vivek Nema[1], Prachi Parwar[2]
[1]Dept of Computer Science and Engineering
[2] Asst.Prof. Dept of Computer Science and Engineering
[1, 2] Takshshila Institute of Engineering And Technology, Jabalpur

Abstract- *- In multimedia forensics, several attempts have been made to find out whether an image is ancient or has been manipulated over the past decade with high enough accuracy based on specially designed features and its classifiers . Editing an actual image via software or Android application is one of the easiest things one can do today before sharing a doctored image on social networking sites. Although most people do it for fun, it is susceptible if a person hides an object or changes someone's face within the image. Before questioning the intent behind editing tasks, we first need to identify which and which part of the image has been manipulated. It therefore invokes automated tools to identify intrinsic differences between authentic images and manipulated images. However, the important task of localizing manipulated regions in a simulated image still poses more challenges than manipulation detection and relatively few algorithms attempt to deal with it. Keeping this in mind, a technique that uses dual domain-based asserted network networks taking into account different types of inputs is proposed in this thesis. In the proposed framework, models are designed and trained, respectively. A transfer policy is applied to the training process of F-CNN, with well-trained parameters. Extensive experiments show that the proposed post-processing operations optimize the final manipulation probability map, and our framework in conjunction with F-CNN and parameters better explains state-of-the-art techniques with precise accuracy and detection.*

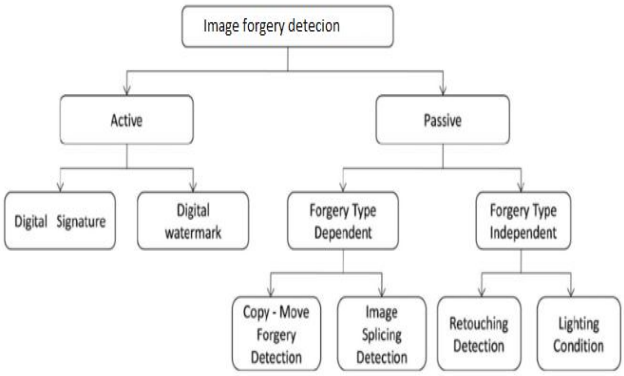
Keywords- Image tampering detection; image forgery detection; image forensics; image copy-move detection; image splicing detection, CNN.

I. INTRODUCTION

fast growing technological advancements in the new era, the development of every sector has been imaginative, security being one of them, it has also become easy to dissolve. Not only legal documents can be stolen and easily forged, criminal evidence such as photographs and security footage can be produced in the courts. One might think that this is enough for an institution to check the ID at the front gate, but they do not know how big a job it is to hold the perpetrator's hand on a fake ID. Posing as someone else in a public setting is also a hassle-free task for amateur criminals. As previously mentioned, photo editing tools that are easily accessible at the top are also very compatible. A person can learn basic photo editing tips within a few hours, even if they have never seen image editing software before. Now there is nothing advanced about photo editing, while forgery has become even more difficult to detect. Image forgeries can be classified into many types such as copy-move forgery, splicing and image Retouching etc. Research has been going on in this field for years now and many effective methods have been proposed to detect such forgeries. Xuedong Zhao et al. proposed a method for color channel design to find the most inequitable channel, which they called the optimal chroma-like channel, for feature extraction [1]. Another process to detect counterfeited documents, mainly tampered with using a photocopier, is through superimposition [2]. However, such techniques have now become obsolete since forgery these days is digital, clean and indistinguishable to the human eye. Therefore, machines are a more viable option now. Most of the techniques used to detect those manipulations employ machine learning and pattern recognition [3]. Region duplication can be detected by calculating the scale invariant feature transform (SIFT) key-points and then finding all the pixels within the duplicated region [4]. Digital documents that have been rotated, scaled or resized can also be detected easily using image processing tools [5].

II. CLASSIFICATION OF IMAGE FORGERY

With creativity and understanding of the properties of image only, tampering of images becomes successful. Tampered images are used not only to create incredible photos for fun, but also in various other walks of life like providing security to valid documents with watermarks or digital signatures. No matter what the cause of the act is, Forager should use a single or a combination of series of image processing operations. “To detect image tampering, knowledge of tampering functions is required. Image forgery techniques are classified into two: active and passive approaches "[16]. Below image shows the major classification of image forgery.



III. RELATED WORK

With the development of imaging and computer graphics technologies, transmission of the massive video data volume [17], [18] and video data security have both become challenges. Editing or tampering with digital videos (images) has become easier, even With the help of multimedia editing software, for an inexperienced forger. The potential increase in multimedia tampering can severely affect the security of our society. Therefore, multimedia information security [19]–[22] and multimedia forensics [23]–[26] have become important topics.

Unlike the active multimedia forensic approaches, e.g. , digital watermarking [27] and signatures [28], passive techniques for video (image) forensics are more challenging. As no additional information is embedded into the original video (image) in advance. Although there may be no tampering in the digital forge, it can leave no visible clues, they can alter the underlying data . In recognition of this fact, a variety of tampering detection techniques have been proposed in recent years, such as recompression detection [29], copy move detection, and splicing detection. Because JPEG is the most popular image format, passive JPEG image tampering detection has attracted much research interest. Since the blocking artifacts introduced by JPEG compression will change considerably if tampering operations exist, Ye et al. [30]

The symmetric property of artifacts is measured by blocking a blocking artifact matrix (BACM) as evidence of tampering in a suspect JPEG image. Farid [31] proposed to detect tampered regions for a double compressed JPEG image by recompressing the image at different quality levels and looking for the presence of so-called ghosts. Wang et al. [32] observed that the quantization noise of high frequency DCT coefficients in a tampered region is stronger than an unchanged region, and they subsequently utilized this feature to locate tampered regions.

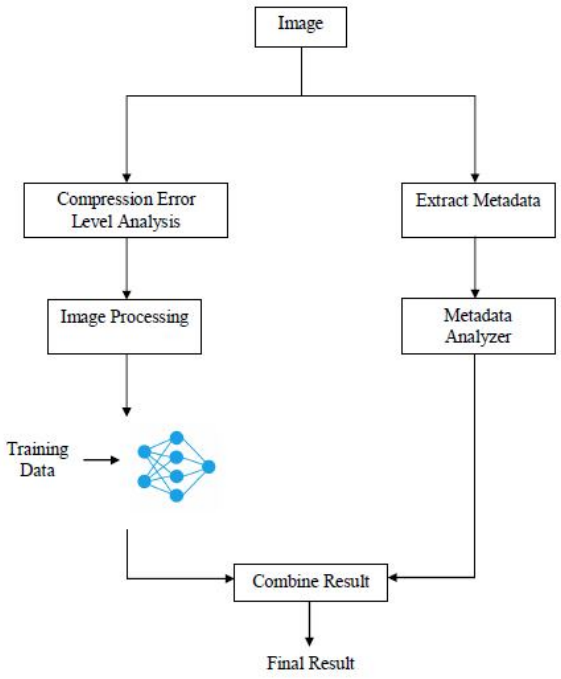
In recent years, deep neural networks, such as the deep belief network, deep auto encoder and convolutional neural network (CNN), have shown to be capable of extracting complex statistical dependencies from high dimensional sensory inputs and efficiently learning their hierarchical representations; this capability allows these methods to generalize well across a wide variety of computer vision (CV) tasks, including image classification, speech recognition, and image restoration [33]. However, with the development of graphics processing units (GPUs) and the availability of large-scale training datasets, it is reasonable that the forgery might take these powerful manipulation methods, based on deep learning to cover JPEG artifacts, may be the cause of the failure of traditional forensic methods. Therefore, it is necessary to study the forensics of debocking. Motion JPEG (MJPEG) is one of the powerful video formats, in This each video frame or interlaced region of a digital video sequence is compressed separately as a JPEG image. In this paper, we propose a novel image deblocking detection approach that can detect deblocking and automatically learn feature representations based on a deep learning framework. We train a supervised CNN to learn the hierarchical features of deblocking operations with labeled patches from the training dataset. The first convolutional layer of the CNN serves as the preprocessing module to efficiently obtain the tampering artifacts. Instead of a random strategy, the kernel weights of the first layer are initialized with 23 high-pass filters used in the calculation of residual maps, which helps to obtain the tampering artifacts. We then extract the features on the basis of a patch by applying a patch-sized sliding window to scan the whole image. The generated image representation is then condensed by regional pooling to obtain the discriminative feature.

IV. PROPOSED ALGORITHM

The proposed work aims to identify tampering on images. The proposed system will find that the input image is digitally altered by some software or that it is real. Existing systems use specific methods such as splicing, color, etc. to detect tampering on images. The proposed system will develop image manipulation using learning with a neural network approach. There are various software for image conversion. They do it very efficiently so no user will see it with human eyes. Even with a neural network, it is not possible to determine whether an image is manipulated without identifying a common factor in almost all of the manipulated images. Therefore, the proposed system will use the error level analyzed image instead of the raw pixel to

identify the intersection. Each image has its metadata attached. Image metadata includes information related to the image such as size, type, properties, make, etc. For example, if an image is edited with Adobe Photoshop, the metadata will also include the version of Adobe Photoshop used. Image metadata can be changed by programming or software. In some cases, the metadata is useful to identify the image or not. First, the proposed system examines image metadata.

Secondly, the proposed system converts the image to the error level analysis format and will be resized to produce an M pixel x N pixel image. These MXN pixels with RGB values are then given in the input layer of the multilayer perceptron network. The output layer consists of two neurons - one for the manipulator image and one for the real image. Based on the value of these neuron outputs along with the metadata analyzer output, we determine whether the image has been tampered with and how likely it is to manipulate the given image. image is tampered or not and how much chance is there for the given image to be tampered.



Current forensic techniques require an expert to analyze the credibility of an image. We implemented a system that can determine whether an image is fake or not with the help of machine learning and thereby making it available for the common public. System contains following phases

A)Metadata Analysis: Most image files do not contain just one picture. They also contain information (metadata) about the image. Metadata provides information about the lineage of a photograph; Including camera type, color space data and application notes. Different image formats include different types of metadata. Some formats, such as BMP, PPM, and PBM, contain little information beyond image dimensions and color space. In contrast, JPEGs from a camera typically contain different types of information, including the camera's make and model, focal and aperture information, and timestamps. Metadata-extractor is capable of extracting metadata information of various types of large image. Once an image is selected for processing, it is tuned into 2 separate stages. The first stage is metadata analysis. After extracting the metadata, the metadata text is fed into the metadata analysis module. Metadata Analyzer is basically an algorithm search tag. If keywords like Photoshop, Gimp, Adobe etc. are found in the text and then the chances of tampering are increased. Two different variables are created which are called fecundity and reality. Each variable represents the weight of being a real or fake image. Once the tag is taken, it is analyzed and the corresponding variable is incremented by a fixed predefined weighting. The following table represents the keywords and the corresponding weight increase. After the entire tag has been processed, the final values of the fakeness and reality variables are fed into the production phase.

B) Error level analysis: JPEG is a lossy format, but the amount of error initiated by each re-save is not a line. Any modification to the image will change the image such that the static field (no additional errors) becomes unstable. Additional areas of the photo show slightly more volatility as Photoshop merges information from multiple layers, effectively modifying multiple pixels. Error level analysis (ELA) works by deliberately calculating the image at a known error rate, such as 95%, and then distinguishing between images. If there is indeed no change, the cell has reached its local minima for error at that quality level. However, if a large amount of change occurs, the pixels are not in their local minima and are effectively "original". The same image is then converted to a 90% quality image. The difference between these two is revealed, although the difference is method. The resulting image is the ELA image required for the input image. This image is saved as a buffered image and sent to the neural network for further processing.

C) Machine learning: implemented using the Neurof library for Java. We have accelerated a multilayer perceptron network with diffusion education rules. A multilayer perceptual neural network is used with one input layer, 3 hidden layers and 1 output layer. Once the image is selected for evaluation, it is changed from an error level analysis representation to a compression and error level analysis step. 100%, 90% of images are used to create an ELA image. Once the ELA is calculated, the image is preprocessed to convert to mxn px width and height. After preprocessing, the image is sorted into

an array. The array consists of N integer values that represent mXn pixels. Since each pixel has red, green, and blue components, MXN pixels will have n values.

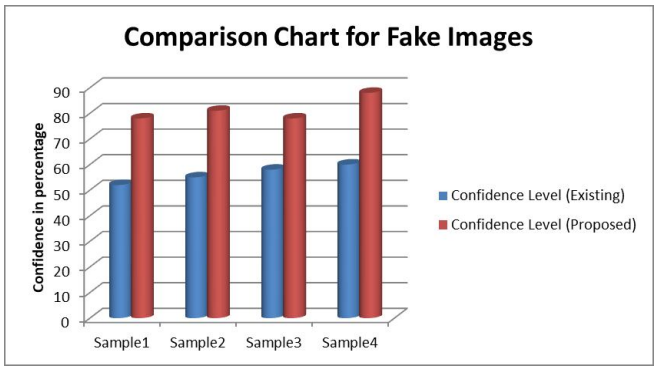
During training, the array is given as an input to the multilayer perceptron network and output neurons are also set. multilayer perceptron neural network is a fully connected neural network. There are 2 output neurons. The first is for the neuron representing the intersection and the second for the real image. If the given image is manipulated, the simulated neuron is set to one and the real one is set to zero. The fake set to zero and the real set to one. We have used the sigmoid activation function.

V. SIMULATION RESULTS

Performance is evaluated on the basis of confidence level for fake and real images. For samples that are fake, result summary is shown in table below:

Sample	Confidence Level (Existing) In percentage	Confidence Level (Proposed) In percentage
Sample1	52	78
Sample2	55	81
Sample3	58	78
Sample4	60	88

Chart is shown below:



VI. CONCLUSION AND FUTURE WORK

In the present time, with the advancement in the field of science and technology, the introduction of various advance images editing tools are also surging up. These advanced image editing tools have multitudinous features. We can use these advanced image editing tools in our further extension of the project to implement the required results more easily and instantly. While these tools are mostly used in the creative design related areas, criminals also can easily get access to them and as a result, can exploit them to create fake identities to hide themselves in public, or to commit a crime. Research has been going on for the past few decades to come up with a fool-proof method to detect these forged documents which do not look any different to the human eye. Most of the forgery detection methods rely on feature extraction and texture analysis of the scanned document, and the detection program is created through pattern recognition and machine learning. Our purpose was to propose one such method with good efficiency and accuracy. We will continue to refine the methodology so that there are lesser loop-holes in the analysis and will hopefully come up with a better method in future..

REFERENCES

[1] Zhao, X., Li, S., Wang, S., Li, J., & Yang, K. (2012) , Optimal chroma-like channel design for passive colour image splicing detection, EURASIP Journal on Advances in Signal Processing, 2012(1), 240.

[2] Joshi MC, Kumar A, Thakur S. Examination of digitally manipulated-machine generated document, a case study elucidating the issue of such unwanted progenies of modern technology. Prob Forensic Science 2011; 56:162–73.

[3] Qureshi, Muhammad Ali, and Mohamed Deriche, A bibliography of pixel-based blind image forgery detection techniques, Signal Processing: Image Communication 39 (2015): 46-74.

[4] Xunyu Pan, Siwei Lyu, "Region Duplication Detection Using Image Feature Matching", Information Forensics and Security IEEE Transactions on, vol. 5, pp. 857-867, 2010, ISSN 1556-6013.

[5] Anil Dada Warbhe, Rajiv V. Dharaskar, Vilas M. Thakare, "Digital image forensics: An affine transform robust copy-paste tampering detection", Intelligent Systems and Control (ISCO) 2016 10th International Conference on, pp. 1-5, 2016.

[6] Mohsen Zandi, Ahmad Mahmoudi- Aznaveh, Alireza Talebpour, "Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector", Information Forensics and Security IEEE Transactions on, vol. 11, pp. 2499-2512, 2016, ISSN 1556-6013.

[7] Xia, Z., Lv, R., Zhu, Y., Ji, P., Sun, H., & Shi, Y. Q. (2017), Fingerprint liveness detection using gradient-based texture features. Signal, Image and Video Processing, 11(2), 381-388.

[8] Lin, Hwei-Jen & Wang, Chun-Wei & Kao, Yang-Ta. (2009) Fast copy-move forgery detection WSEAS Transactions on Signal Processing. 5. 188-197.

[9] Ansari, Mohd Dilshad & Prakash Ghrera, Satya. (2018). Copymove image forgery detection using direct fuzzy transform and ring projection. International Journal of

Signal and Imaging Systems Engineering. 11. 44. 10.1504/IJSISE.2018.10011742.

[10] Badal Soni, Pradip K. Das, Dalton Meitei Thounaojam. (2018) CMFD: a detailed review of block based and key feature based techniques in image copy-move forgery detection. IET Image Processing 12:2, pages 167-178.

[11] Jawadul H. Bappy, Amit K. Roy-Chowdhury, Jason Bunk, Lakshmanan Nataraj, B.S. Manjunath. Exploiting Spatial Structure for Localizing Manipulated Image Regions. (2017) IEEE International Conference on Computer Vision (ICCV), pages 4980- 4989.

[12] Hajihashemi, Vahid & Gharabagh, Abdorreza. (2018). A Fast, Block Based, Copy-Move Forgery Detection Approach Using Image Gradient and Modified K-Means. 298-307. 10.1007/978-3-319-68385-0_25.

[13] Mahmood, Toqeer & Nawaz Tabassam & Mehmood, Zahid &Khan, Zakir & Shah, Mohsin & Ashraf, Rehan. (2016). Forensic analysis of copy-move forgery in digital images using the stationary wavelets.578-58310.1109/INTECH.2016.7845040.

[14] Kushol, Rafsanjany & Salekin, Md Sirajus & Hasanul Kabir, Md & Alam Khan, Ashraful. (2016). Copy-Move Forgery Detection Using Colour Space and Moment Invariants-Based Features.1-6.10.1109/DICTA.2016.7797027.

[15] Agarwal, Vanita & Mane, Vanita. (2016). Reflective SIFT for improving the detection of copy-move image forgery.84-88.10.1109/ICRCICN.2016.7813636.

[16] Nishtha Parashar and Nirupama Tiwari, A Survey of Digital Image Tampering Techniques, International Journal of Signal Processing, 2015, Vol.8, No.10, Pp.91-96.

[17] Z. Pan, J. Lei, Y. Zhang, and F. L. Wang, ‘‘Adaptive fractional-pixel motion estimation skipped algorithm for efficient HEVC motion estimation,’’ ACM Trans. Multimedia Comput. Commun. Appl., vol. 14, no. 1, pp. 1–19, 2018.

[18] Z. Pan, X. Yi, and L. Chen, ‘‘Motion and disparity vectors early determination for texture video in 3D-HEVC,’’ Multimedia Tools Appl., pp. 1–18, Nov. 2018. doi: 10.1007/s11042-018-6830-7.

[19] Y. Zhang, C. Qin, W. Zhang, F. Liu, and X. Luo, ‘‘On the fault-tolerant performance for a class of robust image steganography,’’ Signal Process., vol. 146, pp. 99–111, May 2018.

[20] Y. Ma, X. Luo, X. Li, Z. Bao, and Y. Zhang, ‘‘Selection of rich model steganalysis features based on decision rough set α-positive region reduction,’’ IEEE Trans. Circuits Syst. Video Technol., vol. 29, no. 2, pp. 336–350, Feb. 2019.

[21] J. Chen, W. Lu, Y. Fang, X. Liu, Y. Yeung, and Y. Xue, ‘‘Binary image steganalysis based on local texture pattern,’’ J. Vis. Commun. Image Represent, vol. 55, pp. 149–156, Aug. 2018.

[22] F. Zhang, W. Lu, H. Liu, and F. Xue, ‘‘Natural image deblurring based on L0-regularization and kernel shape optimization,’’ Multimedia Tools Appl., vol. 77, no. 20, pp. 26239–26257, 2018.

[23] X. Liu, W. Lu, Q. Zhang, J. Huang, and Y.-Q. Shi, ‘‘Downscaling factor estimation on pre-jpeg compressed images,’’ IEEE Trans. Circuits Syst. Video Technol., to be published. doi: 10.1109/TCSVT.2019.2893353.

[24] X. Liu, W. Lu, T. Huang, H. Liu, Y. Xue, and Y. Yeung, ‘‘Scaling factor estimation on jpeg compressed images by cyclostationarity analysis,’’ Multimedia Tools Appl., pp. 1–18, Jul. 2018. doi: 10.1007/s11042-018- 6411-9.

[25] J. Li, W. Lu, J. Weng, Y. Mao, and G. Li, ‘‘Double JPEG compression detection based on block statistics,’’ Multimedia Tools Appl., vol. 77, no. 24, pp. 31895–31910, 2018.

[26] C. Lin, W. Lu, W. Sun, J. Zeng, T. Xu, and J. H. Lai, ‘‘Region duplication detection based on image segmentation and keypoint contexts,’’ Multimedia Tools Appl., vol. 77, no. 11, pp. 14241–14258, 2018.

[27] C. Vyas and M. Lunagaria, ‘‘A review on methods for image authentication and visual cryptography in digital image watermarking,’’ in Proc. IEEE Int. Conf. Comput. Intell. Comput. Res., Coimbatore, India, Dec. 2014, pp. 1–6.

[28] F. Xue, Z. Ye, W. Lu, H. Liu, and B. Li, ‘‘MSE period based estimation of first quantization step in double compressed JPEG images,’’ Signal Process. Image Commun., vol. 57, pp. 76–83, Sep. 2017.

[29] S. Ye, Q. Sun, and E.-C. Chang, ‘‘Detecting digital image forgeries by measuring inconsistencies of blocking artifact,’’ in Proc. IEEE Int. Conf. Multimedia Expo, Jul. 2007, pp. 12–15.

[30] H. Farid, ‘‘Exposing digital forgeries from JPEG ghosts,’’ IEEE Trans. Inf.Forensics Security, vol. 4, no. 1, pp. 154–160, Mar. 2009.

[31] W. Wang, J. Dong, and T. Tan, ‘‘Tampered region localization of digital color images based on JPEG compression noise,’’ in Proc. Int. Conf. Digit. Watermarking. Berlin, Germany: Springer, 2011, pp. 120–133.

[32] Y. Tai, J. Yang, X. Liu, and C. Xu, ‘‘MemNet: A persistent memory network for image restoration,’’ in Proc. IEEE Int. Conf. Comput. Vis. (ICCV), Oct. 2017, pp. 4549–4557.

[33] Alin C Popescu and Hany Farid, Exposing digital forgeries by detecting traces of resampling. IEEE Transactions on signal processing, 53(2):758–767, 2005