ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 9, September 2019

Image Tampering Detection Using Learning with Neural Network

Vivek Kumar Nema [1], Prachi Parwar [2]

P.G. Student, Department of CSE, Takshshila Institute of Engineering & Technology, Jabalpur, MP, India[1]

Assistant Professor, Department of CSE, Takshshila Institute of Engineering & Technology, Jabalpur, MP, India[2]

ABSTRACT: In multimedia forensics, many efforts have been made to detect whether an image is pristine or manipulated with high enough accuracies based on specially designed features and classifiers in the past decade. Editing a real-world photo through computer software or mobile applications is one of the easiest things one can do today before sharing the doctored image on one's social networking sites. Although most people do it for fun, it is suspectable if one concealed an object or changed someone's face within the image. Before questioning the intention behind the editing operations, we need to first identify how and which part of the image has been manipulated. It therefore demands automatic tools for identifying the intrinsic difference between authentic images and tampered images. However, the important task for localizing the tampering regions in a fake image still faces more challenges compared with the manipulation detection and relatively a few algorithms attempt to tackle it. With this in mind, a technique that utilizes the dual-domain-based convolutional neural networks taking different kinds of input into consideration is proposed in this thesis. In the proposed framework, the model are designed and trained, respectively. With the well-trained parameters, a transfer policy is applied to the training process of the F-CNN. The extensive experiments show that the proposed post-processing operations optimize the final tamper probability map, and our framework with the combination of F-CNN and parameter learning significantly outperforms the state-of-art techniques with the best accuracy and detection.

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

I. INTRODUCTION

With the rapid technological advancement has strengthened the growth of every field imaginable, security being one of them, it has also become easy to breach it. Not only can legal documents be stolen and forged, criminal evidence- such as photographs and security footage can be easily tampered with. One may feel it is enough for an institution to check ID's at the front gate but they do not realize how menial of a task it is for a criminal to get their hands on fake ID's. Posing as someone else in a public setting is a trouble free task even for amateur criminals. As mentioned before, photo editing tools which on top being easily accessible are also extremely friendly. One can learn basic photo editing tips in a few hours, even if they have never seen an image editing software before. There is nothing too advanced about photo editing anymore, whereas forgery has become even more difficult to detect.

Image forgeries may be classified into many types such as copy-move forgery, splicing and many more. 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 colour 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)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 9, September 2019

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].

Research has been done so far to detect duplicated regions in a document tampered using copy-move forgery with the help of block-based and traditional key-point based methods [6]. Since all the databases in a security system are digital, people mostly rely on the image features that can be extracted easily. For instance, gradient based texture features, with the help of a machine, can easily be calculated and compared [7]. Another devised scheme is to divide the image into overlapping blocks, thinking of them as vectors and find the manipulated region through radix sorting [8]. Image forgery detection can also be done using only image processing and without any embedded security information. This method makes use of Fuzzy Transform (F-Transform) and Ring Projection Transform (RPT) to detect forgeries. These transforms convert the data to a single dimension significantly reducing the computational capacity [9]. Various studies have also been done weighing down the pros and cons of the prevalent copy-move forgery detection (CMFD) techniques [10]. Image processing algorithms such as DWT (Discrete Wavelet Transform) and SVD (Singular Value Decomposition) are one of the many feature extraction methods that are used today to detect forged images [11]. Another approach to detected tampered images is to make use block based methods, but by using the non-overlapping texture blocks as a base for the smooth blocks, thus reducing the computational capacity [12]. Copy-move forgery (CMF) can also be detected using algorithm based on Stationary Wavelet Transform (SWT), which is able to accurately detect the duplicated blocks [13]. CMF can also be detected easily if the feature vector generated is based on colour perception and object representation [14]. Reflective SIFT based algorithms are also proficient in detecting duplicated blocks in copy-move forgeries[15].

1.1 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 whatever the cause of act might be, the forger should use a single or a combination of series of image processing operations. To detect image tampering, the knowledge of tampering operations is essential. Image forgery techniques are classified in to two: Active and passive approaches [16]. Figure1.1 shows the major classification of image forgery.

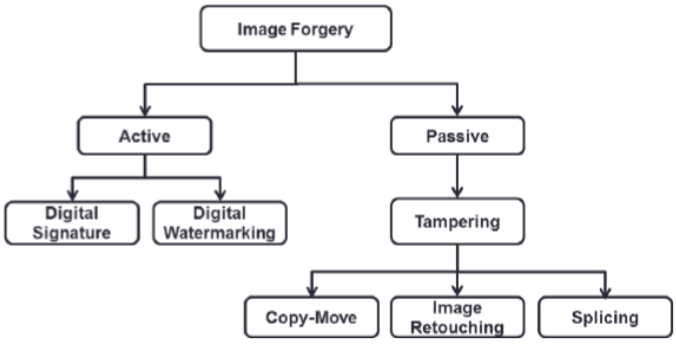

Fig 1.1: Classification of Image Forgery

II. 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 for an inexperienced forger, with the aid of multimedia editing software. A potential rise in multimedia tampering can seriously affect the security of our society. Therefore, multimedia information security [19]–[22] and multimedia forensics [23]–[26] have become important topics. In contrast to the active multimedia forensic approaches, e.g., digital watermarking [27] and signatures [28], passive techniques for video (image) forensics are more

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 9, September 2019

challenging. As no additional information is embedded into the original video (image) in advance. Although digital forges may leave no visual clues regarding what might have been tampered with, they may alter the underlying statistics. 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] measured the symmetrical property of the blocking artifacts by computing a blocking artifact characteristics matrix (BACM) in a suspicious JPEG image as evidence of tampering.

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 the JPEG artifacts, which might cause the fail of traditional forensics methods. Hence, it is necessary to study the forensics of deblocking. Motion JPEG (MJPEG) is one of the most popular video formats, in which each video frame or interlaced field 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.

Image forgery detection is a massive field in forensic and signal processing. Basic classification and localization solutions for image forgery have produced a huge number of papers since 2010. Most work in literature revolves around patch classification and using the classifiers to localize where image forgery took place. Recent works are focused on localization using different datasets..

III. PROPOSED ALGORITHM

The objective of the proposed work is to identify tampering on images. Proposed system will find that an input image is digitally altered by any software or it is real. Existing system uses specific methods like splicing, colouring etc. for detection of tampering on images. Proposed system will develop image tampering using learning with neural network approach.

There are various software for alteration in image. They do it very efficiently so any user will not judge it by human eye. Even with a neural network, it is not possible to determine whether an image is tampered or not without identifying a common factor across almost all tampered images. So, proposed system will uses error level analyzed image rather than raw pixels for identification of tampering.
Every image has its metadata associated with it. Image metadata contains image related information like size, type, attributes, make etc. For example, if an image is edited with Adobe Photoshop, the metadata will contain even the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 9, September 2019

version of the Adobe Photoshop used. Image metadata can be altered by programming or software. In some cases metadata is useful for identifying image is tampered or not. Firstly, proposed system checks the image metadata.
Secondly, proposed system converts the image into error level analyzed format and will be resized to make image of m pixels X n pixels image. Then these mXn pixels with RGB values are given in to the input layer of Multilayer perceptron network. Output layer contain two neurons - One for tampered image and one for real image. Depending upon the value of these neuron outputs along with metadata analyzer output, we determine whether the image is tampered or not and how much chance is there for the given image to be tampered.

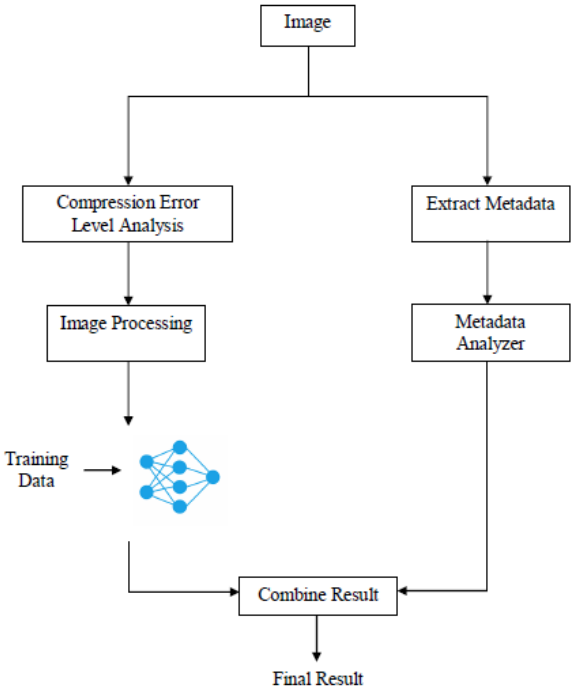

Figure. 3.1: Proposed Architecture.

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 just contain a picture. They also contain information (metadata) about the picture. Metadata provides information about a picture's pedigree; including the type of camera used, color space information, and application notes. Different picture formats include different types of metadata. Some formats, like BMP, PPM, and PBM contain very little information beyond the image dimensions and color space. In contrast, a JPEG from a camera usually contains a wide variety of information, including the camera's make and model, focal and aperture information, and timestamps. Metadata-extractor is able to extract metadata information of large no of different image types. Once an image is selected for processing, it is tunneled into 2 separate stages. First stage is metadata analysis. After extracting metadata, the metadata text is fed into metadata analysis module. Metadata analyzer is basically a tag searching algorithm. If keywords like Photoshop, Gimp, Adobe etc. is found in the text and then the possibility of being tampered is increased. Two separate variables are maintained which are called fakeness and realness. Each variable represents the weight of being real or fake image. Once a tag is taken, it is analyzed and corresponding variable is incremented by a certain predefined weight. The following table represents keywords and corresponding weight increments. After processing the entire tags, final values of fakeness and realness variable is fed into the output stage.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 9, September 2019

B) Error Level Analysis: JPEG is a lossy format, but the amount of error introduced by each re-save is not line. Any modification to the picture will alter the image such that stable areas (no additional error) become unstable. Additional areas of the picture show slightly more volatility because Photoshop merged information from multiple layers, effectively modifying many of the pixels. Error level analysis (ELA) works by intentionally resaving the image at a known error rate, such as 95%, and then computing the difference between the images. If there is virtually no change, then the cell has reached its local minima for error at that quality level. However, if there is a large amount of change, then the pixels are not at their local minima and are effectively "original". The system first saves an image at 100% quality. Then the same image is converted into 90% quality image. The difference between these two is found out though difference method. The resulting image is the required ELA image of the input image. This image is saved as a buffered image and sent to the neural network for further processing.

C) Machine learning: is implemented using Neuroph library for java. We have implemented a multilayer perceptron network with momentum back propagation learning rule. A multilayer perceptron neural network is used having one input layer, 3 hidden layers and 1 output layer. Once the image is selected for evaluation, it is converted to Error Level Analyzed representation from Compression and Error Level Analysis stage. 100%, 90% images are used for the construction of ELA image Once ELA is calculated, the image is preprocessed to convert into mxn px width and height. After preprocessing, the image is serialized in to an array. The array contains N integer values representing mXn pixels. Since each pixel has red, green and blue components, mXn pixels will have N values.
During training, the array is given as input to the multilayer perceptron network and output neurons also set. The MLP is a fully connected neural network. There are 2 output neurons. First neuron is for representing tampered and the second one for real image. If the given image is tampered one, then the fake neuron is set to one and real is set to zero. Else fake is set to zero and real set to one. We have used sigmoid activation function.

IV. 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

Table 1: Confidence Level Comparisons for Fake images.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 9, September 2019

Chart is shown below:

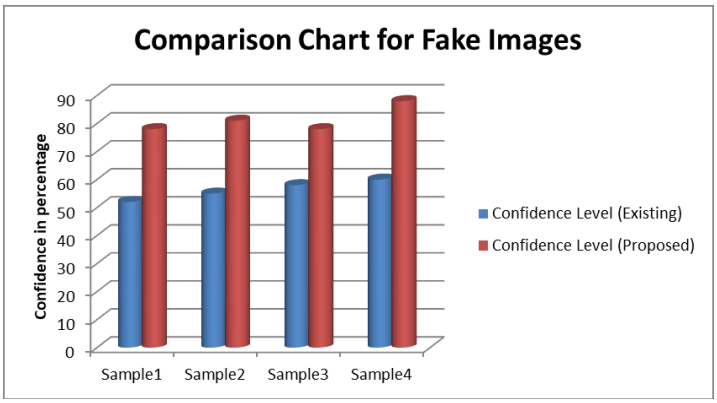

Figure 4.1:Comparison Chart

V. 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 9, September 2019

[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