International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 6, Nov-Dec-2021, ISSN (Online): 2395-566X

A Review Article Enhancement of Image Forgery and Improvement of Image Parameters Using DWT Algorithm

Rajni Soni, Asst. Prof. Hemant Amhia
Department of Electrical engineering (Control System),
Jabalpur Engineering College
Jabalpur,MP,India

Abstract- This paper presents a new system for integration of a grid-connected photovoltaic (PV) system together with a self-supported dynamic voltage restorer (DVR).Power quality (PQ) is gaining a great deal of importance as more sensitive loads are introduced into the utility grid. The degradation of product quality, damage of equipment and temporary shutdowns are the general issues associated with PQ problems in industries. Any mal-operation or damage of the industrial sensitive loads results in monetary losses disproportionately higher than the severity of the PQ issues. The evolution of power electronics technology replaced the traditional power quality mitigation methods with the introduction of Custom Power System devices (CUPS). The major power electronic controller based CUPS are DSTATCOM, DVR and UPQC. DVR is a pertinent solution for the economic losses caused by the PQ issues in the industries. Among the CUPS, DVR is the most cost-effective one. In the published literature, only a few papers correspond to the review of DVR technology. In this paper, a systematic review of published literature is conducted and a description is given on the design, standards and challenges in the DVR technology. In addition to the energy variability of renewable energy sources, random voltage sags, swells and disruptions are already a major issue in power systems. Recent advances in power electronic devices have provided a platform for new solutions to the voltage support problem in power systems.

Keywords- Wind, Solar, MPPT, DVR, SVM, DC to DC converter.

I. INTRODUCTION

We are living in an era where we are open to abundant digital imagery. We use to have blind trust on integrity and authenticity of this imagery but today's technology has depleted this trust. From the esteemed magazines to the media industry, courtrooms, fashion outlets, scientific journals, political campaigns, and the photographic jest that land in our e-mail inboxes and social media platforms. Forged photographs are appearing with a growing frequency. Without any doubt image authenticity now is a big matter of concern.

There are two main categories of image forgery detection to verify the legitimacy of the manipulated image. The first one is Active method and another is Passive method for forgery detection and they are further explained in the literature. Watermarking and Steganography are two main categories under the active methods where the authentic information is inserted into the digital image. The prior stored information is used to enlighten whenever there is a need to test the authenticity of the image. If we talk about passive techniques the most popular method to forge an image is a copy-move forgery. It is done by copying apart from the image and paste it into the same image.

There are many other faster techniques like double JPEG compression, Noise Inconsistency etc. 0 After undergoing through photo-editing software, both original and manipulated image is compressed twice due to the lossy nature of the JPEG (since most images are stored in JPEG). This double compression creates specific artefacts not present in a single compression.

II. GENERALIZED SCHEMA FOR IMAGE FORGERY IDENTIFICATION

Forgery identification in pictures is two step issues. The principle target of blind forgery detection technique stays to categorize a given picture as real or altered. We will depict a widely used schema of image forgery identification procedure that comprises of the following steps:

1. Image Preprocessing:
Image preprocessing is the initial pace. Some preprocessing is performed on the picture under deliberation like image filtering, image enrichment, trimming, change in DCT coefficients, RGB to grayscale transformation before handling the image to feature extraction procedures. Algorithms examined at this

juncture might possibly include this step depending upon the calculation.

2. Feature Extraction:
Selection of features for every class separates the image-set from different classes however in the meantime stays constant intended for a specific class chosen. The attractive element of the chosen set of features is to have a tiny measurement so that computational complexity can be diminished and have an extensive distinction with other classes [42].

3. Selection of Classifier:
Depending upon the feature-set that is extracted in above step, suitable classifier is either chosen or composed. The large training sets will yield the improved performance of classifier.

4. Classification:
The only motive behind classification is to determine if the image is original or not. Neural systems [4], LDA[6] and SVM[4] are classifiers used for this purpose.

5. Post processing:
Some forgeries will possibly require post processing that includes manipulations like localization of copy locales.

III. LITERATURE REVIEW

Anuja Dixit, Adaptive clustering-based approach for forgery detection in images containing similar appearing but authentic objects: Copy-move forgery is one of the well-known image forgery technique which exploits regions of the same image to create forged image by replicating or hiding authentic content of the original image. Original images can also contain similar looking but authentic objects. Approximate nearest neighbor search is performed using Random Binary Search Tree (RBST) method. For keypoint clustering,

Adaptive Density Peak Clustering (ADPC) technique is employed. Outlier removal is performed using Random Sample Consensus (RANSAC) technique. Further, forged regions are localized using correlation map generation. Experimental results display that the proposed approach can effectively distinguish between forged and original images containing similar appearing but authentic objects. It is also able to detect forged images sustaining different post-processing attacks. For COVERAGE dataset, proposed technique achieves high F-Measure = 86.901% and low False Positive Rate (FPR) = 15.241% in comparison to state-of-the-art techniques [1].

Anuja Dixit, A fast technique to detect copy-move image forgery with reflection and non-affine transformation attacks: Copy-move forgery is one of the most frequently utilized image tampering technique which uses the segment of the same image to produce manipulated image by duplicating or concealing image regions. To remove suspicious traces of forgery, various attacks are applied over the tampered image which makes forgery detection process too complicated. We propose a forgery detection technique in which Center Surround Extrema (CenSurE) detector is applied for keypoint detection from images.

To compute keypoint descriptors, Local Image Permutation Interval Descriptor (LIPID) is used. Keypoint matching is performed using k-Nearest Neighbor (k-NN) technique with utilization of k-d tree and Best-Bin-First (BBF) search method. Grouping over keypoints is performed using Fuzzy C-Means (FCM) clustering. We apply Random Sample Consensus (RANSAC) algorithm to remove outliers obtained during forgery detection process [2].

Rachna Mehta, Markov features based DTCWS algorithm for online image forgery detection using ensemble classifier in the pandemic: The unexpected blast of the COVID has been found everywhere in the world, and everyone has been shocked unusually. In this critical situation, the number of online activities increases, whether related to online education, research, business meetings, virtual conferences, or virtual court. Under this pandemic situation, digital images are the only source of information that can be generally shared and visualized in virtual conferences and social media, and it's challenging to share the document for forgery detection.

Today, it's straight forward to forge these images using image-editing software, and it's essential to detect image forgery for such images. In this paper, an efficient novel Discrete-Time Cosine Wavelet and Spatial (DTCWS) Markov feature-based algorithm has been designed for the detection of such forgery, especially for this pandemic situation. For this work, high-dimensional Markov features have been extracted in the DTCWS domain, and the dimensionality of these Markov features has been reduced with Principal Component Analysis (PCA).

Furthermore, the co-occurrence matrix has increased the correlation among coefficients. For classification, an optimized ensemble classifier is used for evaluating the results instead of using a support vector machine classifier. Due to the time constraint in online activities, the proposed algorithm shows the best accuracy of 99.9% without taking too much time and fewer complexes compared to the current work [3].

H.Kasban, An efficient approach for forgery detection in digital images using Hilbert–Huangtransform: Image manipulation plays important role in fake news spreading and it may cause ethical, economic, or political problems for people and sometimes for countries. Image integrity verification becomes a very important research issue due to increasing the forged images on the Internet and social media.

The objective of this paper is presenting an accurate approach for digital image forgery detection has enough capability to sense any small image tampering and robustness against image manipulation attacks. The first step in the proposed approach is converting the RGB image into YCbCr space, then, the Hilbert–Huang Transform (HHT) features extracted from the chrominance-red component Cr, then, three different classifiers; Support Vector Machines (SVM), K-Nearest Neighbors (KNN), and Artificial Neuron Networks (ANN) have been tested and compared for image classification into authentic or forged. The results are verified using Structural-Similarity (SSIM) to calculate the forgery detection accuracy.

The proposed approach has been tested with seven different manipulation images datasets; CASIA-V1, CASIA-V2, MICC-F2000, MICC-F600, MICC-F220, CoMoFoD and additional dataset collected from different Internet websites and social media. Furthermore, the proposed approach has been tested against post-processing attacks such as; image compression, adding Gaussian noises or adjusting the contrast of the image. The results show that, SVM classifier has achieved the highest accuracy compared to ANN and KNN classifiers. The proposed approach has been compared with other published approaches, and the comparison proved its superiority over the previously published approaches [4].

Kunj Bihari Meena, A copy-move image forgery detection technique based on tetrolet transform: Copy-move forgery is a common type of forgery in digital images. In copy-move forgery, one part of the image is replicated within the same image, generally at different location. For revival of trustworthiness of images, there is a need to develop an efficient and robust technique to detect such forgeries. This paper proposes a new copy-move image forgery detection technique based on Tetrolet transform. In this technique, initially the input image is divided into overlapping blocks, then four low-pass coefficients and twelve high-pass coefficients are extracted from each block by applying Tetrolet transform.

Feature vectors are then sorted lexicographically, and similar blocks are identified by matching the extracted Tetrolet features. Experimental results show that the proposed technique can detect and locate the duplicated regions in the images very accurately, even when the copied regions have undergone some post-processing operations blurring, color reduction, adjustment of brightness and contrast, rotation, scaling, JPEG compression. In addition, it is also observed that the proposed technique is able to detect very small duplicated regions and multiple forgery cases, even when image is smooth [5].

S. Uma, Soccer game optimization based forgery detection of digital images: Copy move tampering (CMT) is commonly applied for forging digital images employing user-friendly image processing tools. Interest-point (IP) based forgery detection methods are very popular as they involve a comparatively lower computational burden than those of block-based methods. The IPs in existing methods may not spread over the entire region of the image and concentrate on regions with high gradients.

If the tampering region contains low gradients, then that region has very sparse or no IPs, thereby making the algorithm to fail in detecting the forgery. This paper attempts to spread a minimum number of IPs over all regions of the image and evaluate scale-invariant features transform (SIFT) descriptors, and employ soccer game optimization (SGO), a metaheuristic algorithm inspired from the intelligent behaviour of soccer game players, for transforming the feature space into cluster space. The paper studies the performance of the suggested method on 500 digital images and presents the results [6].

Boubacar Diallo, Robust forgery detection for compressed images using CNN supervision: Images available on online sharing platforms have a high probability of being modified, with additional global transformations such as compression, resizing or filtering covering the possible alteration. Such manipulations impose many constraints on forgery detection algorithms. This article presents a framework improving robustness for image forgery detection. The most important step of our framework is to take into account the image quality corresponding to the chosen application. Therefore, we relied on a camera identification model based on convolutional neural networks. Lossy compression such as JPEG being considered as the most common type of intentional or inadvertent concealment of image forgery, that leads us to experiment our proposal on this manipulation.

Thus, our trained CNN is fed with a mixture of different qualities of compressed and uncompressed images. Experimental results showed the importance of this step to improve the effectiveness of our approach against recent literature approaches. To better interpret our trained CNN, we proposed an in-depth supervision by first a visualization of the layer and an experimental analysis of the influence of the learned features. This analysis led us to a more robust and accurate framework. Finally, we applied this improved system on an image forgery detection application and showed some promising results [7].

M. Geetha, A novel approach for image forgery detection using improved crow search algorithm: In recent days, the image data plays a important role in every field. In this digital world generation of image data is becoming popular. A novel method has been proposed for a forgery detection technique in image using enhanced improved crow search algorithm.

Preprocessing is done at the initial stage to convert RGB to LAB space conversion, Proceeded with feature selection and alalysis using Ada boost algorithm and cascade architecture. Next step is to extract the features like Haralick feature, Skewness and inverse difference movement. In Continuation with feature extraction, feature selection is performed using proposed algorithm followed by enhanced convolution neural network classification. Finally the comparison of the proposed classification algorithm and sensitivity analysis is done [8].

P.Niu C. Wang, Fast and effective Keypoint-based image copy-move forgery detection using complex-valued moment invariants: Copy-move forgery is one of the most common image tampering schemes, with the potential use for misleading the opinion of the general public. Keypoint-based detection methods exhibit remarkable performance in terms of computational cost and robustness. However, these methods are difficult to effectively deal with the cases when 1) forgery only involves small or smooth regions, 2) multiple clones are conducted or 3) duplicated regions undergo geometric transformations or signal corruptions. To overcome such limitations, we propose a fast and accurate copy-move forgery detection algorithm, based on complex-valued invariant features.

First, dense and uniform keypoints are extracted from the whole image, even in small and smooth regions. Then, these keypoints are represented by robust and discriminative moment invariants, where a novel fast algorithm is designed especially for the computation of dense keypoint features.

Next, an effective magnitude-phase hierarchical matching strategy is proposed for fast matching a massive number of keypoints while maintaining the accuracy. Finally, a reliable post-processing algorithm is developed, which can simultaneously reduce false negative rate and false positive rate. Extensive experimental results demonstrate the superior performance of our proposed scheme compared with existing state-of-the-art algorithms, with average pixel-level F-measure of 94.54% and average CPU-time of 36.25 s on four publicly available datasets [9].

VenuK.N. Enhanced block based copy paste image forgery detection, Materials Today: With the easy availability of wide variety of image editing software, digital images can be easily edited and manipulated. The need of the hour is to expose such image forgeries and manipulations. Copy move attack is one such forgery method where a portion of the image is copied from one place and pasted into a different region on the same image and made to appear like an original part of the image. In Adobe photoshop imaging software, a part of the image is copied and pasted onto the same image by using Rectangle Marquee tool, such duplicated portion of the image can be detected with block-based copy paste forgery detection method. The Polygonal Lasso Tool available in Adobe photoshop can also be used for copy paste operation. This tool creates selection with straight edges making it easy to select objects with different shapes. Because of its straight edges and corners created in copy paste region we are not able to determine the complete region with block-based copy paste detection method (Fridrich et al., 2003).

In this paper we investigate the method to detect the complete pasted region in an image using Adobe's Polygonal Lasso Tool. The proposed method detects the pasted image region by block matching. It also detects additional pixels around the boundaries of the pasted region, additional pixels that are not part of the interested region are excluded by using the morphological open operation. This proposed method has been experimentally verified, and it detects more pixels in the pasted region as compared to the traditional block-based [10].

Yilan Wang, Robust and accurate detection of image copy-move forgery using PCET-SVD and histogram of block similarity measures: Many block-based detection methods for image copy-move forgery have been reported. However, their performance degrades significantly under different geometric attacks such as rotation and scaling. In this paper, we propose a novel robust and accurate detection scheme for image copy-move forgery.

It mainly consists of three steps: firstly, a suspicious image is divided into overlapping circular blocks, and polar complex exponential transform (PCET) is employed to extract geometric invariant feature of each block. Next, singular value decomposition (SVD) is applied to the coefficient matrix composed of extracted geometric invariant moments for dimension reduction. Meanwhile, the histogram of block similarity measures is adopted to estimate the optimal similarity threshold. Finally, the calculated similarity threshold is used for block matching process and consequently more accurate tampered areas are obtained [11].

Diaa M.Uliyan, Investigation of image forgery based on multiscale retinex under illumination variations: The number of forged images is currently expanding vastly over the Internet. Therefore, image authenticity represents a globally challenging issue that must be addressed. Emerging tools for image editing have been developed to manipulate and enhance digital images; however, forgers can exploit these tools to achieve their destructive purposes. Forgers often use a common method of image forgery called region duplication forgery. In this method, the copied region in the fake image can appear identical to the original region of the image. This paper aims to target this issue by developing an algorithm that can detect

suspected images through localizing small duplicated regions. These regions can be described by multiscale features, which are invariant with illumination variations. The proposed method begins with segmenting suspected images using an adaptive statistical region merging.

The goal of the segmentation method is to discover small regions. The method then targets the small regions based on color correction to represent their illumination features. Experiments are also conducted to validate the proposed method on two image datasets, Media Integration and Communication Center (MICC) and Image Data Manipulation, yielding positive results. A comparative study of the most recent methods is carried out [12].

Bin Xiao, Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering: This paper proposes a splicing forgery detection method with two parts: a coarse-to-refined convolutional neural network (C2RNet) and diluted adaptive clustering. The proposed C2RNet cascades a coarse convolutional neural network (C-CNN) and a refined CNN (R-CNN) and extracts the differences in the image properties between un-tampered and tampered regions from image patches with different scales. Further, to decrease the computational complexity, an image-level CNN is introduced to replace patch-level CNN in C2RNet.

The proposed detection method learns the differences of various image properties to guarantee a stable detection performance, and the image-level CNN tremendously decreases its computational time. After the suspicious forgery regions are located by the proposed C2RNet, the final detected forgery regions are generated by applying the proposed adaptive clustering approach. The experiment results demonstrate that the proposed detection method achieves relatively promising results compared with state-of-the-art splicing forgery detection methods, even under various attack conditions [13].

D.Vaishnavi, Application of local invariant symmetry features to detect and localize image copy move forgeries: Today whatever is seen in digital images could be unrealistic due to the advent of sophisticated systems and image editing software's. It is easy to edit digital images without leaving the traces of manipulation, therefore tampering is hard to discern visually. Among the types of digital image forgeries, realizing the copy move forgery is very challenging.

Hence, this paper proposes a novel scheme to detect copy-move forgery by means of symmetry based local features. The proposed scheme can also detect the multiple copy move forgeries and localize the detected regions. The experiments are carried out by using the various datasets, and comparative study also made with the existing methods [14].

Shilpa Dua, Image forgery detection based on statistical features of block DCT coefficients: Majority of the existing detection algorithms are able to deal with either type of forgery (splicing or copy-move). However, if we require a unified approach, we need to combine two previous works for each one of the alterations. In order to solve this problem, the authors present a new algorithm for the detection of splicing and copy-move forgery in the same instance. In this paper, a forgery detection technique is proposed which exploits the artifacts originated due to manipulations performed on JPEG encoded images.

In JPEG compression technique, an image is divided into non-overlapping blocks of size 8x8 pixels and discrete cosine transform (DCT) coefficients are evaluated for each block independently. When a JPEG compressed image is tampered, there is a change in the statistical properties of AC components of block DCT coefficients. To capture this change, we propose to use standard deviation and count of non-zero DCT coefficients corresponding to each of the AC frequency components independently.

The images are cropped by removing a few rows and columns from the top left corner and suggested features are evaluated for test image and its cropped version. The extracted feature vector is used with the support vector machine (SVM) for the classification of authentic and forged images. Experiments are conducted on a standard dataset of pre- and post-processed forged images CASIA vl.O and v2.0 to consolidate the theoretical concept of the proposed technique. Also, the comparative analysis is performed to showcase better detection rates compared with the state-of-the-art methods [15].

IV. CONCLUSION

Forgery detection using passive forgery detection techniques is one of the most growing fields of research. We have presented some of the passive techniques and also compare them in terms of accuracy of their results.

The prime drawback of the existing methods is Automation that is the answers can be interpreted with the intervention of human only. Second drawback is that if we talk about copy-move forgery, then the use of these methods is computationally expensive.

Thirdly as these techniques are applied to images only, we can extend the research on audios and videos. Fourthly at present there is no technique which can identify between the malicious forgery and just the retouching like artistic manipulation. The most challenging tasks is to develop a unified algorithm having capacity to detect any type of forgery.

REFERENCE

[1] AnujaDixit, Adaptive clustering-based approach for forgery detection in images containing similar appearing but authentic objects, Applied Soft Computing, Volume 113, Part A, December 2021, 107893, https://doi.org/10.1016/j.asoc.2021.107893.
[2] AnujaDixit, A fast technique to detect copy-move image forgery with reflection and non-affine transformation attacks, Expert Systems with Applications, Volume 182, 15 November 2021, 115282, https://doi.org/10.1016/j.eswa.2021.115282.
[3] RachnaMehta, Markov features based DTCWS algorithm for online image forgery detection using ensemble classifier in the pandemic, Expert Systems with Applications, Volume 185, 15 December 2021, 115630, https://doi.org/10.1016/j.eswa.2021.115630
[4] H.Kasban, An efficient approach for forgery detection in digital images using Hilbert–Huang transform, Applied Soft Computing Volume 97, Part A, December 2020, 106728, https://doi.org/10.1016/j.asoc.2020.106728.
[5] Kunj BihariMeena, A copy-move image forgery detection technique based on tetrolet transform, Journal of Information Security and Applications, Volume 52, June 2020, 102481, https://doi.org/10.1016/ j.jisa.2020.102481.
[6] S.Uma, Soccer game optimization based forgery detection of digital images, Forensic Imaging, Volume 25, June 2021, 200453, https://doi.org/10.1016/j.fri.2021.200453.
[7] BoubacarDiallo, Robust forgery detection for compressed images using CNN supervision, Forensic Science International: Reports Volume 2, December 2020, 100112, https://doi.org/10.1016/j.f sir.2020.100112.
[8] M.Geetha, A novel approach for image forgery detection using improved crow search algorithm, Materials Today: Proceedings Available online 19 February 2021 In Press, Corrected Proof, https://doi.org/10.1016/j.matpr.2020.12.1135.
[9] P.NiuC.Wang, Fast and effective Keypoint-based image copy-move forgery detection using complex-valued moment invariants, Journal of Visual Communication and Image Representation Volume 77, May 2021, 103068, https://doi.org/10.1016/j.jvcir.2021.103068.
[10] VenuK.N. Enhanced block based copy paste image forgery detection, Materials Today: Proceedings Available online 19 February 2021 In Press, Corrected Proof, https://doi.org/10.1016/j.m atpr.2021.01.189.
[11] YilanWang, Robust and accurate detection of image copy-move forgery using PCET-SVD and histogram of block similarity measures, Journal of Information Security and Applications Volume 54, October 2020, 102536, https://doi.org/10.1016/j.jisa.2020.102536.
[12] Diaa M.Uliyan, Investigation of image forgery based on multiscale retinex under illumination variations, Forensic Imaging Volume 22, September 2020, 200385, https://doi.org/10.1016/j.fri.2020.200385.
[13] BinXiao, Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering, Information Sciences Volume 511, February 2020, Pages 172-191, https://doi.org/10.1016/j.ins.2019.09.038.
[14] D.Vaishnavi, Application of local invariant symmetry features to detect and localize image copy move forgeries, Journal of Information Security and Applications Volume 44, February 2019, Pages 23-31, https://doi.org/10.1016/j.jisa.2018.11.001.
[15] ShilpaDua, Image forgery detection based on statistical features of block DCT coefficients, Procedia Computer Science Volume 171, 2020, Pages 369-378, https://doi.org/10.1016/j.pr ocs.2020.04 .038.