A Various Study of Image Forgery Detection: A Survey

Mrs. Nirupma Tiwari[1], Pawan Kushwah[2], Dr. Dinesh Goyal[3]
SRCEM

Abstract- *As we are living in the todays digital world in which all type of advancement are becoming possible and at the same time the use of images have been increasing day by day in our lives, the motivation to make manipulation of images also increases simultaneously. This type of image forgery is going on increasing day-by-day. In this paper, we are performing a review of this Image forgery technique. There are two kinds of techniques for image forensics: one is active protection, and the other is passive detection. The main types of Image forgery techniques are Image Splicing, Copy-Move forgery used mainly for making tempered photographs are studied in more detail in this paper. As the forgery of Images is growing day-by-day,it is very much necessary to develop tools for detection as which image is true and which is forgery.*

Keywords- image Forgery detection; Techniques Types image forgery.

I. INTRODUCTION

Detection of digital Image forgery is a relatively new scientific field that addresses the problem of digital images authenticity. Advances in digital technologies have made it easy to manipulate and counterfeit digital images. This problem is aggravated by the availability of vast amount of images available through the internet [1-5]. Detecting image forgery has significant implications in a variety of applications such as copyright protection, proof of ownership, legal, commercial, and security related issues. One of the most widely known image forgery methods is the copy-move approach, where part of an image is copied and then moved to a different location in the image. This may also be accompanied by a change of scale or rotation. Several methods have been used in the literature to address the copy move detection problem [1] .

Forged images can be used at various places like news report, magazines and websites to mislead persons. So, for avoiding such situations various methods are developed to examine authenticity of images. Copy-move forgery used at various places because of its difficult detection. Many researchers invented different methods for detecting copy-move forgery. Digital image forgery detection methods can be divided in two broad categories: active and passive approach. Active approach requires anterior information about the image. Active approaches demands watermark or generation of signatures at the time of image acquisition. Due to this requirement, active approaches limit their applications [2]. Passive approaches are also known as blind forgery detection methods because these methods do not require any prior information about image. Passive approaches are divided in five categories which are Pixel-based, Format-based, Camera-Based, Source Camera Identification-based, Physics-based and Geometry-based.

Pixel-based: These techniques are based on differentiating pixel values of image to identify anomalies present in input image. Such techniques are categorized into Cloning, Splicing and Resampling.

Format-based: These methods are concerned about image format. Especially, these techniques used in JPEG Format. Such kind of approaches are divided in Double JPEG, JPEG Blocking and JPEG Quantization.

Camera-based: When an image is captured from a camera it goes through various image processing procedures. These kind of techniques are based on detecting image forgery on the basis of Color Filter Array, Camera Response, Sensor imperfections and Chromatic Aberrations.

Source Camera Identification-based: These techniques are based on finding forgery in images on the basis of specification of camera used for capturing image. This technique is divided in three categories which are Lens Aberration, Sensor imperfections and CFA interpolations.

Physics-based: These methods are based on finding forgery in image byanalyzing different illuminating environment in which image was captured. These techniques divided in three categories: Light Directions (2D), Light Directions (3D) and Light Environment.

Geometry-based: These methods are based on position of objects and their measurement relative to source camera. Such

techniques are divided in two categories which are based on principal point and metric measurements.

II. FORGERY DETECTION

Forgery detection methods become much more complicated to deal with the latest forgery techniques. This back to the availability of digital editing tools, alteration, and manipulation become very easy and as a result forgery detection becomes a complex and threatening problem [3]. Image forgery detection can be manipulated in various ways with many simple operations like affine transforms such as translation, scaling, etc., compensation operations such as brightness, colors, contrast adjustments, etc., suppression operation such as noise extraction, filtering, compression, etc., .Furthermore, more complex operations are also possible such as compositing, blending, matting, cropping, photomontage leading to visually untraceable artifacts in an image. The automatic and scientific method of detecting the forged images has become a big challenging problem for researchers and the same problem is true for every multimedia contents.

TYPES OF IMAGE FORGERY

Creation of forged image is classified into three parts as follows:

1. Copy-move forgery
2. Image forgery using splicing
3. Image retouching

Explanation of all different parts:

1. copy-move forgery:-

This is most commonly used image tempering method. In this a part of the source image is first taken out and then copied to other parts once or may be multiple times to hide or add some information. Copy-move is also known as cloning. Copied part is taken from same image. In simple word, we can say that source image and destination image is same. In Copymove forgery, Copied regions in image can be post processed, rotated flipped and scaled before pasting to other places to hide or remove any details. Example of copy-move image forgery is presented in fig-2. [4]

Fig-1 example of copy-move forgery; (left) original image with three missiles; (right) forged image with four missiles [4]
Copy-move forgery is divided into mainly two groups namely: keypoint based methods and block based method. We can say that Keypoint based methods are same as suspicious points. They are spatial locations or points in the image that define what is interesting or what is stand out in the image. Keypoint is better than block based method because no matter if there is rotation in image or distorted, keypoint always define interesting points. Whereas in block based method, image is separated into small overlapping or non-overlapping blocks. For analyzing the matching area of image, these blocks are compared with each other.

2. image forgery using splicing:

In this technique, there are more than one source images from where some part of image is taken to create a new fake (forged) image.

Fig-2: example of image forgery using splicing

As in fig-3: first image of helicopter is turned over horizontally and then add another image of „The shark" to create a new fake image. Image splicing involves composite of two or more than two images which are combined to create a forged image.

3. image retouching:

Image retouching is less harmful than other forged images. In this, image is not significantly change, but instead, enhances or reduces certain features of an image as shown in

fig-4. In this method, the professional image editors adjust colors, change background and work with hue saturation for toning and balancing. Image retouching is mostly used for fashion, beauty or advertising photos, interesting images for advertisement.

Fig-3: example of image retouching

COMMON FRAMEWORK FOR FORGERY DETECTION

Forgery detection in images is a two class problem. The main objective of passive detection technique remains to classify a given image as original or tampered. Most of the existing techniques extract features from image after that select a suitable classifier and then classify the features. General structure of image tampering detection consisting of following steps shown in Figure

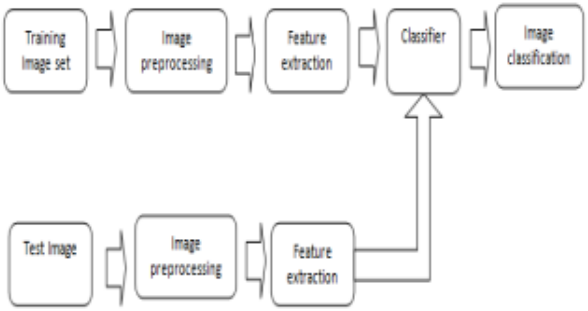

Fig.4: Framework for Image Forgery Detection

Image preprocessing is the first step. Before image could be subjected to feature extraction operation some preprocessing is done on the image under consideration such as enhancement, filtering, cropping, and DCT transformation [5], conversion from RGB to gray scale. After this comes feature extraction. Feature set for each class which differentiates it from other classes but at the same time remains invariant for a particular class are selected. After this is Classifier selections. Based on extracted feature set appropriate classifier is either selected or designed. The sole purpose of classifier is to classify an image either as original or forged. In past many of the algorithm were failed many times in the detection of forged image, because single feature extraction algorithm is not capable to contain the specific feature of the images. So to overcome the limitation of existing algorithm, meta-fusion technique classifiers can be used.

III. CLASSIFICATION OF IMAGE FORGERY TECHNIQUES

There are two kinds of techniques for image forensics: one is active protection, and the other is passive detection. Which again consist of many different methods, as shown in below figure [6]:

Active Approach

In this active approach, the digital image requires some kind of pre-processing such as watermark embedded or signatures are generated at the time of creating the image. However, in practice this would limit their application. Digital watermarking and signature are two main active protection techniques, as something are embedded into images when they are obtained. We can detect the Image is tampered, if special information cannot be extracted from that obtained image image. Watermarking is such a method of active tampering detection, as a security structure is embedded into the image, but most present imaging devices do not contain any watermarking or signature module and that are similar to the application of active protection. This structure is used for integrity evaluation in the sense that if any discrepancy is found with the structure then the image is tampered and an inverse analysis over the structure is done to locate tampered

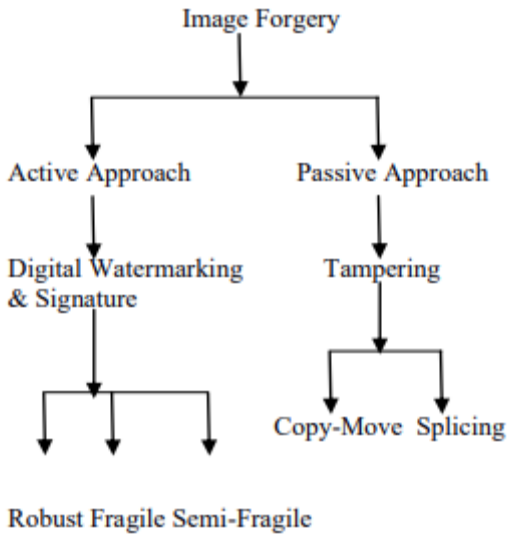

Fig. 5. Classification of Image forgery approaches

Regions of the image. In recent times, various schemes are proposed for providing security to the image, which is analogous to the concept of watermarking like,

message authentication code, image hash, image checksum and image shielding as a counterpart to it.

Passive Approach

Passive image forensics is usually a great challenge in image processing techniques. There is not a particular method that can treat all these cases, but many methods each can detect a special forgery in its own way. The stream of passive tampering detection deals with analyzing the raw image based on various statistics and semantics of image content to localize tampering of image. Neither construct is embedded in the image and nor associated with it for security, as like active approaches and hence this method is also known as raw image analysis. The localization of tampering is solely based on image feature statistics. Hence, algorithms and methods of detection and localization of image based on passive tampering vary depending upon the type of security construct used. Nevertheless, passive tampering detection typically aims for localization of tampering on raw image.

IV. DIGITAL IMAGE FORGERY TECHNIQUES

Digital image forgeries can be classified into five categories: Copy-move, Image Retouching, Image Splicing, Morphing and Enhancing.

Copy-Move:

In this technique, a part of image is copied. Copied part is pasted at some other location on the same image to hide objects of image or to bring additional objects in the image which alters message conveyed by the image.

Image Retouching:

This technique is used for commercial and aesthetic uses. Retouching is done for enhancing features of an image. This forgery technique can also be used for degrading features of an image.

Image Splicing:

In this forgery, components of different images are used for producing a single composite image. Objects of several images are juxtaposed on a single image.

Morphing:

In this kind of forgery, similar type of objects present in two images are used for turning original object into different object. Such forgery technique is performed to change faces present in image.

Enhancing:

In this kind of image manipulation, several enhancement operations (like color changes in image, blurring the background of image etc.) are performed over the image to make objects more visible.[7]

4.1 Copy-Move Forgery Detection

As region duplication is performed in copy-move forgery so at least two similar region will be present in tampered image. Copied segment will have similar properties like noise components, dynamic range and color palette maintaining compatibility to rest of the image. Copy-Move forgery detection can be divided into two categories: Block-based [7] and Key point based methods. In block-based methods, input image is divided in fixed size overlapping or non-overlapping blocks. Generally, Square blocks are used but some researchers also used circular blocks. Features are extracted from each block using several methods such as intensity-based, moment-based, dimensionality reduction-based, frequency-based etc. Similar feature vectors are configured to find similar regions of image. In key point based methods, key points are scanned and features are extracted corresponding to these key points. Similar feature vectors are identified to find altered region present in image. In this category, image is not divided in fixed size blocks.

4.2 General Steps for Copy-Move Forgery Detection

In copy-move image forgery, strong correlation between copied and pasted parts exist which is exploited for finding tampering present in image. The workflow used for finding forgery is shown in Figure (1). The steps [7] followed for forgery detection are as follows:

Preprocessing:

The purpose of preprocessing is enhancement in image data. Color conversion is performed if there is requirement to convert color image in gray scale image. Different preprocessing functions are applied like resizing input image, dimension reduction, filtering image with low-pass filter. In both block-based and key point based techniques, preprocessing can be applied.

Feature Extraction:

In this step, feature vectors are extracted. If block based method is used then image is divided in overlapping or non-overlapping blocks of fixed size. These blocks can be square or circular. Features are extracted corresponding to each block of image. In case of key point based methods, feature corresponding to key points are extracted.

Matching:

After feature extraction, matching between feature vectors is performed for finding similar regions present in an image. In block based methods, lexicographical or radix sorting is used for arranging similar features in proximity to each other. Best-Bin-First searching procedure is used for identifying approximate nearest neighbor which helps in feature matching for key point based methods.

Filtering:

Filtering procedures are used for reducing number of false matches. Morphological operations are applied to remove isolated regions.

V. LITERATURE SURVEY

Ahmed Ghoneim, et al. (2018) With the invention of new communication technologies, new features and facilities are provided in a smart healthcare framework. The features and facilities aim to provide a seamless, easy-to-use, accurate, and real-time healthcare service to clients. As health is a sensitive issue, it should be taken care of with utmost security and caution. This article proposes a new medical image forgery detection system for the healthcare framework to verify that images related to healthcare are not changed or altered. The system works on a noise map of an image, applies a multi-resolution regression filter on the noise map, and feeds the output to support-vector-machine-based and extreme-learning-based classifiers. The noise map is created in an edge computing resource, while the filtering and classification are done in a core cloud computing resource. In this way, the system works seamlessly and in real time. The bandwidth requirement of the proposed system is also reasonable.[8]

GonapalliRamu, et al. (2017) Cloning (copy-move forgery) is a malicious tampering attack with digital images where a part of image is copied and pasted within the image to conceal the important details of image without any obvious traces of manipulation. This type of tampering attacks leaves a big question of authenticity of images to the forensics. Many techniques are proposed in the past few years after powerful software's are developed to manipulate the image. The proposed scheme is involved with both the block based and feature point extraction based techniques to extract the forged regions more accurately. The proposed algorithm mainly involves in matching the tentacles of same features extracted from each block by computing the dot product between the unit vectors. Random Sample Consensus (RANSAC) algorithm is used to extract the matched regions. The experimental result of the algorithm which is proposed indicates that, it can extract more accurate results compared with existing forgery detection methods.[9]

Kang Hyeon RHEE (2017) For a design of the Gaussian filtering (GF) detection (GFD) in the tampered digital images, this paper presents three kinds of the new feature vector which are extracted from the edge ratios and the parameters of Hough peaks. In the proposed algorithm, the formed 10-dim. feature vector is trained in SVM (Support Vector Machine) for the GFD.[10]

Ying Zhang, et al. (2017) This work introduces an approach to localize the tampered region among the images from social media platforms. We propose a joint model to integrate the predictions from a set of features, each of which represents the inherent relation among the pixels within a certain distance to detect the forgery. Within a fixed distance, the feature is adapted from a few basic statistics through a stacked Autoencoder to a proper version in a noise-resistant manner, so that it will be more robust to detect the tampering when the forgery gone through some common social media platform operations. The classifier is trained using a standalone dataset from a benchmarking but is pre-processed properly to simulate its possible imperfections when spreading over the Internet. The approach was tested on images from Facebook, with results showing an encouraging improvement from the prior arts.[11]

Junjie Zhang, et al.(2017) Active detection technology was widely used in the traditional tampering detection. Firstly, those mainstream technologies of active detection were introduced. Then, some necessary improvements for the tampering detection algorithm were proposed in this paper, for example, the steganography information was cross-embedded to enhance the safety of the images, and the chaos function was simplified to enhance the execution efficiency and detection precision of the algorithm. Experimental results showed that the proposed algorithm can improve the efficiency of image tamper detection.[12]

Paulo Max G. I. Reis (2017) et al present that Audio authentication is an essential project in multimedia forensics stressful strong techniques to hit upon and identify tampered audio recordings. In this text, a brand new method to detect adulterations in audio recordings is proposed by exploiting odd versions inside the Electrical Network Frequency (ENF) signal in the end embedded in a questioned audio recording.

These unusual versions are due to abrupt segment discontinuities because of insertions and suppressions of audio snippets during the tampering task. First, we recommend an ESPRIT-Hilbert ENF estimator alongside an outlier detector based at the sample kurtosis of the anticipated ENF. Next, we use the computed kurtosis as entering for a Support Vector Machine (SVM) classifier to suggest the presence of tampering. The proposed scheme, wherein unique as SPHINS, drastically outperforms associated previous tampering detection methods within the performed assessments. We validate our effects the use of the Carioca 1 corpus with a hundred unedited authorized audio recordings of phone calls.[13]

Sayyed Mohammad Hosseini (2016) et al present that In this paper a new method for detection of camera tampering is proposed. Some examples for camera tampering are: shaking the camera, movement of the camera, occlusion, and rotation of the camera. The tampering may be intentional or unintentional. In the proposed algorithm, in addition to detection of the exact nature of tampering, the exact amount of tampering also can be detected (i.e. the amount and direction of movement). This will help operator in diction making for management in surveillance system. The proposed algorithm detect the shaking using current and previous frames, as well as by constructing a total background based on all frames and building a temporary background based on last 10 frames. The proposed method employs the SURF feature detector to find interest points in both of two backgrounds and compare and match them using MSAC algorithm. The transformation matrix can be obtained to detect the camera movement; camera image zoom and camera rotate. Finally, using the method sobel edge detection the camera occlusion and defocus can be detected. The method also detect the sudden shut downs in camera or images loss. Another feature of the algorithm is providing the information concerning the camera tampering.[14]

MusaedAlhussein (2016) et. al. present that this paper proposed a brand new IT detection technique based totally on neighborhood texture descriptor and extreme learning machine (ELM). The IT includes both splicing and CMF. First, the picture turned into decomposed into three coloration channels (one luminance and two Chroma), and each channel was divided into non-overlapping blocks. Local textures in the shape of local binary pattern (LBP) had been extracted from each block. The histograms of the patterns of all of the blocks had been concatenated to form a feature vector. The characteristic vector became then fed to an ELM for category. The ELM is a powerful and fast classification approach. The experiments were performed using two publicly available databases. The experimental results showed that the proposed method achieved high detection accuracy in both the databases.[15]

M.V. Bhatkar (2016) et. al. present that this paper presents a unmarried segment virtual power meter primarily based on a microcontroller. This virtual meter does now not have any rotating elements, and the electricity consumption can be without difficulty study from a digital show additionally at far flung region it's far easily possible to check energy intake and TD with the aid of the usage of GSM generation. When deliver wills cut-off, the meter will restart with the stored value. Today power robbery is a global hassle that contributes heavily to sales losses. Consumers have been determined manipulating their electric powered meters; try and cause them to stop, or maybe bypassing the meter, successfully the usage of energy without buying it. This strength meter can come across tampering in a strength meter by means of the use of microcontroller and provide there information at remote location.[16]

Chi-Man Pun (2016) et. Al. present that TD strategies based on picture hashing were widely studied with non-stop improvements. However, most existing fashions can't generate object-level tampering localization consequences because the forensic hashes connected to the image lack contour records. In this paper, we gift a singular TD version that may generate an accurate, item-level tampering localization quit end result. First, an adaptive image segmentation technique is proposed to phase the picture into closed regions based on strong edges. Then, the color and function features of the closed areas are extracted as a forensic hash. Furthermore, a geometrical invariant tampering localization version named Image Alignment based Multi-Region Matching (IAMRM) is proposed to establish the location correspondence among the obtained and forensic images by exploiting their intrinsic shape statistics. The model estimates the parameters of geometric ameliorations thru a robust image alignment approach primarily based on triangle similarity; additionally, it fits multiple regions concurrently throughx utilizing manifold rating based on one-of-a-kind graph systems and functions. Experimental consequences display that the proposed IAMRM is a promising method for object-stage TD compared with ultra-modern strategies.[17].

VI. CONCLUSION

While going through the various papers on digital image forgery, which describes method for detection of copy move image forgery in digital image, it has been seen that a lot of work has been completed for copy move forgery detection. Thus further research effort is still needed to develop an appropriate algorithm that can detect the copy move. From the

literature survey, we observed that the big problem with the copy move forgery in digital image is the detection of duplicated region processed by some common post processing operations such as compression, noise addition, rotation, scaling, flipping etc. The other concern is the time complexity of detection technique of copy move forgery in digital image. The problem of detecting if an image has been forged is investigated; in particular, attention has been paid to the case in which an area of an image is copied and then pasted onto another zone to create duplication or to cancel something that was awkward. In the future work I will use DWT and SIFT technique with optical flow to detect the forgery from the video frames and some parameters are calculated to check the performance of the work.

REFERENCES

[1] Bayumy A.B. Youssef1 and Essam H. Atta, "Image Forgery Detection using FREAK Binary Descriptor and Level Set Segmentation". International Journal of Scientific & Engineering Research, Volume 7, Issue 2, February-2016 1 ISSN 2229-5518

[2] Shivani Thakur1Ramanpreet Kaur2Dr. Raman Chadha3 Jasmeet Kaur4," A Review Paper on Image Forgery Detection In Image Processing", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 18, Issue 4, Ver. I (Jul.-Aug. 2016), PP 86-89

[3] ManpreetKaur1 ,Mandeep Kaur, "A Review Paper on Forgery Part Detection using Different Methods". International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified Vol. 5, Issue 8, August 2016

[4] Sawinder Singh Mangat¹Harpreet Kaur, "A Review of Literature On copy-move forgery detection techniques". IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol.6, No1, Jan-Feb 2016

[5] Asif Hassan1 ,Dr. V.K. Sharma, "Passive Forgery Detection and Analysis-A Survey". International Journal of Recent Trends in Engineering & Research (IJRTER) Volume 03, Issue 01; January - 2017 [ISSN: 2455-1457]

[6] Snigdha K. Mankar, Prof. Dr. Ajay A. Gurjar, "Image Forgery Types and Their Detection: A Review". Mankar et al., International Journal of Advanced Research in Computer Science and Software Engineering 5 (4), April-2015, pp. 174-178

[7] Anuja Dixit1 and R. K. Gupta, "Copy-Move Image Forgery Detection using Frequency-based Techniques: A Review". International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.9, No.3 (2016), pp.71-88 http://dx.doi.org/10.14257/ijsip.2016.9.3.07.

[8] Ahmed Ghoneim, Ghulam Muhammad, Syed Umar Amin, and Brij Gupta, "Medical Image Forgery Detection for Smart Healthcare". IEEE Communications Magazine • April 2018 0163-6804/18/$25.00 © 2018 IEEE

[9] GonapalliRamu, S.B.G. ThilakBabu, "Image forgery detection for high resolution images using SIFT and RANSAC algorithm". Proceedings of the 2nd International Conference on Communication and Electronics Systems (ICCES 2017) IEEE Xplore Compliant - Part Number:CFP17AWO-ART, ISBN:978-1-5090-5013-0, 978-1-5090-5013-0/17/$31.00 ©2017 IEEE

[10] Kang Hyeon RHEE, "Forgery Image Detection of Gaussian Filtering by Support Vector Machine Using Edge Characteristics". 978-1-5090-4749-9/17/$31.00 ©2017 IEEE

[11] Ying Zhang, Vrizlynn L. L. Thing, A Multi-Scale Noise-Resistant Feature Adaptation Approach For Image Tampering Localization over Facebook". 2017 IEEE 2nd International Conference on Signal and Image Processing, 978-1-5386-0969-9/17/$31.00 ©2017 IEEE

[12] Junjie Zhang, Jun Tan , Yun Cheng, "Research on digital image tampering detecting algorithm of remote healthcare platform". 2017 4th International Conference on Information Science and Control Engineering, 978-1-5386-3013-6/17 $31.00 © 2017 IEEE

[13] Paulo Max G. I. Reis, Joao Paulo C. L. da Costa, ˜ Senior Member, IEEE, Ricardo K. Miranda, Student Member, IEEE and Giovanni Del Galdo, Member, IEEE," ESPRIT-Hilbert based audio tampering detection with SVM classifier for forensic analysis via electrical network frequency", IEEE TRANSACTIONS ON INFOMATION FORENSICS AND SECURITY, 2017.

[14] Sayyed Mohammad Hosseini and Amir HosseinTaherinia," Anomaly and tampering detection of cameras by providing details", 6th International Conference on Computer and Knowledge Engineering (ICCKE 2016), October 20-212016, Ferdowsi University of Mash had

[15] MusaedAlhussein," Image Tampering Detection Based on Local Texture Descriptor and Extreme Learning Machine", 2016 UKSim-AMSS 18th International Conference on Computer Modelling and Simulation

[16] M.V. Bhatkar and S.A.Thete," Remote Location Tampering Detection of Domestic Load", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016