STUDY OF VARIOUS DETECTION TECHNIQUES OF TAMPERED REGIONS IN DIGITAL IMAGE FORENSICS

S. Priyadarshini[1] and Dr. S. Miruna Joe Amali[2]

Abstract-   Availability of various image editing software both online and offline has tremendously proliferated. This has greatly increased the incidences of digital images manipulation for various intentions. Thereby, causing increased threat to the originality and authenticity of the digital images. Originality of digital images is mandatory for many applications like in military, medical etc. There are various detection techniques in the literature for the identification of tampered images. The focus of this paper is to present a review on the various techniques available to find out the manipulated regions in the digital image. Various techniques are described and focus on their comparison according to the properties like tamper detection, localization, selective or strict authentication is performed.
Keywords – Random walk, First digit features, Salient object detection, Photo Response Non-Uniformity, splicing attacks.

I. INTRODUCTION

Digital images serve as deciding factors now-a-days for many crucial applications. For instance, they extend their hands in identifying the responsibilities in a crime scene, road accidents etc. They are manipulated illegally for varied intentions with the availability of various softwares, thus leading to the accelerated misuse of those softwares. Digital images that are transmitted through less secure channels are also a source of image alteration. Digital images are often manipulated for illegal needs rather than for legal purposes. Digital watermarking was imposed to diminish the above mentioned threats. But it can't be used to prove the authenticity of an image and its pristine nature cannot be validated.

Forgeries in digital images may be done through various ways like performing copy - move forgeries, splicing attacks (to add/remove any component from the image, duplicating certain regions of the image, altering in physical inconsistencies like lighting of geometric features, objects, shadows etc.)

Various methods that are available to detect and localize the tampered regions are discussed. Section II elaborates the various methods and their pros and cons. Section III summaries the various methods and conclusion is given in section IV.

[1] *Department of Computer Science and Engineering K.L.N. College of Engineering, Sivagangai, Tamil Nadu, India*
[2] *Department of Computer Science and Engineering K.L.N. College of Engineering, Sivagangai, Tamil Nadu, India*

II. METHODS

Various research works are constantly being done to improve the identification of tampered images. Various image features like saliency, intensity frequency information, gradient etc. are regularly used by researchers to improve the identification of tampered regions. In this review the following methods are reviewed and their advantages and limitations are discussed.

The methods discussed here includes
A.   First digit features
B.   Saliency object detection: Random walk
C.   Visual saliency: Maximal Entropy Random Walk, MERW
D.   Color-Decoupled Photo Response Non-Uniformity, PRNU
E.   Bayesian Markov Random Field Approach

A.   *First digit features* –

The tampered regions in a digital image are found by the assistance of the first digit features. The information revealed is that each digit's frequency of appearance in the first significant place of quantities obtained from conventional method is logarithmic. By analyzing this, the splicing attack (grabbing any part of image and pasting onto another after enhancing or geometrically transforming) can be detected. First digit feature extraction helps to identify the number of subsequent compressions an image has suffered by analyzing the divergence of DCT first digit feature.

The experiment is carried out in UCID dataset that contains 1338 TIFF images. The algorithm follows the training on a set of $W \times W$ pixels obtained from the UCID dataset for images and the images are split in sizes that are confined to $W = 64$ pixels. The method involves the extraction of DCT coefficients from the given image. Then, the estimation of first 9 spatial frequencies in zig-zag order is done.   Finally a feature vector of size 27(3 first digit features $\times$ 9 DCT coefficients) for each block B_k will be obtained [5]. The Support Vector Machine classifier takes this feature vector of size 27, to discern a positive set and a negative set of images that respectively corresponds to the single and double compressed images. And also returns a confidence value D_k. Then, the SVM classifier compares the D_k value with the threshold of $T=0$ and concludes if a block in the image is JPEG compressed once or twice.

This method is effective in identifying tampered regions with respect to diverse quality compressions, forgery dimensions and under the presence of multiple forgeries. The major disadvantage of the method is that the search window size is smaller while the algorithm is bigger, so lagging in addressing the not-aligned splicing attack is present. Also, the method poses difficulty in properly dealing with flat and heavily compressed image regions.

B. *Saliency object detection: Random walk*–

Identifying the salient objects paves the way to locate the tampered region in an image with much lesser difficulties. Salient object is the subset of the image that is well-thought-out to be the relevant objects by the human visual system. Random walk is used to find out the salient objects. It results in pop-out graph model i.e. the localized
object pops-out from the rest of the regions in an image.

The experiment is setup on the database with 5000 images [8] and it also contains the ground truth of the salient regions. Initially, the image is broken into blocks or patches of pixels, each

block of size 8×8 considered as the vertex, v $\square$ V and they are connected by edges e $\square$ E, thus a graph is constructed. The w_{ij}, weight of the edges is estimated by the frequency of node visits by the walker.

Automatic way is used to identify the region to which the seed node belongs [14]. The region might be either salient region or background region. A node is characterized to be most salient node, when it is possible for it to pop out globally when compared to other related nodes. A node is said to be most salient node when it maximizes other salient nodes.

The main benefit of the method is listed below,

- High accuracy of the graph with respect to salient object detection due to distance weighted pop-out affinity graph.

- Improved performance due to priorities of correct labeled nodes over its counter based on soft labeling.

- Improved labeling with equal number of background nodes along with multiple salient nodes.

The difficulty of the method is that the accuracy of automatic labeling method depends on the accuracy of the graphs with respect to the representation of salient objects. So, if the accuracy of the latter fails, then the whole method may not work out.

C. Visual saliency: Maximal Entropy Random Walk, MERW–

This method is used to detect the salient objects in the input image. MERW, is not only restricted in localizing the tampered region, it is also adopted for other issues in image segmentation, saliency detection, and link prediction. The way from which the MERW [9] discerns from the generic random walk method is that the former knows the complete details about the full graph structure, whereas the latter is aware only of the local knowledge.

The input image is first over-segmented into superpixels [6] and they're taken as the primary units for the subsequent   procedures. The random walker moves randomly from one node to another, and the saliency estimation can be obtained by predicting the probability of querying the walker on the nodes at stationary distribution. MERW also helps in finding the accurate salient regions based on the uniqueness and visual organization.

The experimental setup is on Uncompressed Color Image Dataset, UCID dataset and it is tested on a dataset of 1000 response maps. This method outperforms the threshold-based method and Markovian prior method in terms of low false positive rates.

MERW is best used, as it has the awareness of global knowledge in decision making and localization properly. The lagging of this method is that many regional features like orientation, symmetry, size, existence of human face identification are not done in this method. Despite this, the method outperforms all the other methods.

Color-Decoupled Photo Response Non-Uniformity, CD-PRNU–

Digital image that is being given as the input for forgery detection may contain artificial channels with interpolation noise. This noise can be understood only when the type of color filter array, CFA, used by the manufacturer of the image acquisition device reveals it. But, for this method [2], CFA information isn't required as this method follows the process of subdividing the image into four sub-images, then the corresponding noise residuals are found out, and consolidated into W, the noise residual of the input image.

The experiments are carried out on source camera identification and integrity of image contents. The cameras used include, Canon IXUS 850is, Canon PowerShot A400, Canon IXY Digital 500, FujiFilm A602, Olympus FE210, Olympus C730.

The main strength of this method lies in the following

- For this method, CFA pattern used by the manufacturer need not be known. As, the decomposition of I_c into four sub images $I_{c,IJ}$ reveals that four sub-images either contains only physical or only artificial colors.

- Decoupling of physical / artificial components before extracting the noise residuals eliminates the artificial components from contaminating the physical components.

This method lags behind due to the reasons like,

- Multiple pixels are used in wavelet transform used in noise residual extraction. [Both physical and artificial components].

- So, the interpolation noise gets diffused from the artificial components into the physical components during the application of wavelet transform in noise residual extraction process.

E. Bayesian Markov Random Field Approach–

Sensor pattern noise is used to find the image forgeries. Markov random fields are used to model the spatial dependences of the source that're strong [4]. The problem formulation takes the lead from the prior knowledge on the image, as this process is based on Bayesian approach. The MRF is used on the decision variables, thus accounting for the spatial dependencies.

The experiment is conducted on 200 images for estimation of the PRNU pattern and on 20 images for designing the predictor.

The proposed method provides a significant and consistent performance gain over the original, in terms of object level detection ability. It faces difficulty due to the following reasons,

- Image level segmentation increases resolution, yet the segmentation is very challenging and unreliable process.

- Spatial resolution is low, that the smaller forgeries detection is difficult.

III. SUMMARY

Each method paves a different path to arrive at the target i.e. to find the tampered region and locate it. In such scenario, all the aforementioned methods act smart and however find the tampered region effectively. The status and virtues are reflected in the chart (Table 1). Though, all the above said methods are effective in their own way, MERW method is effective and the overall performance is also higher.

TABLE I. STATUS AND VIRTUES OF THE METHODS DISCUSSED

Category	Measurements	CPU/Running time (in seconds)	Localization Capability
First digit feature	False Positive Rate, FPR: 0,Total Positive Rate TPR: 100	NA	Yes
Salient object detection: Random walk	F-measures varies between 0.66 and 0.69	0.90	Yes
MERW	F-measure, $\tau = 0.035$	Average running time 0.71	Yes

CD-PRNU	FP < TP where FP is False Positive and TP is True Positive.	Identification rate 0.9400	Yes
Bayesian-MRF approach	Receiver Operating Characteristics, ROC, ω = 0.2	Mean CPU time 7.10	Yes

Its average running time is also limited within 0.71 seconds. Though methods that use PRNU based approaches detect the tampered regions, they must be followed by other complicated processes whereas; MERW is simpler in that context.

IV.CONCLUSION

This paper has overviewed some of the effective techniques that are used to detect the tampered regions yet there is a long way to go. A future way of working may be like developing methods to increase the accuracy in authenticating images, recovering back to original and better localization techniques.

REFERENCES

[1] Bartolini. F., Tefas, A., Barni, M., Pitas. I, "Image authentication techniques for surveillance applications", *Proceedings of the IEEE*, vol. 89, no. 10, pp. 1403–1418, 2001.

[2] Chang-TsunLi, Yue Li,"Color-Decoupled Photo Response Non-Uniformity For Digital Image Forensics", *IEEE Transactions on circuits and systems for video technology*, vol. 22, no. 2, pp. 260-271, 2012.

[3] Chen. M., Fridrich, J., Goljan, M., Lukas, J, "Determining image origin and integrity using sensor noise", *IEEE Transactions Information Forensics Security*, vol. 3, no. 1, pp. 74-90, 2008.

[4] Giovanni Chierchia, Giovanni Poggi, Carlo Sansone Luisa Verdoliva, "A Bayesian-MRF Approach For PRNU-Based Image Forgery Detection", *IEEE Transactions on information forensics and security*, vol. 9, no. 4, pp. 554-567, 2014.

[5] Irene Amerini, Rudy Becarelli, Roberto Caldelli,Andrea Del Mastio, "Splicing Forgeries Localization Through The Use Of First Digit Features", *IEEE International Workshop on Information Forensics and Security (WIFS)*, pp. 143-148, 2014.

[6] Jin-Gang Yu,Ji Zhao, Jinwen Tian, and Yihua Tan, "Maximal Entropy Random Walk For Region-Based Visual Saliency", *IEEE Transactions on cybernetics*, vol. 44, no. 9, pp. 1661-1672, 2014.

[7] Ju. W, D. Xiang, B. Zhang, L. Wang, I. Kopriva, and X. Chen, "Random walk and graph cut for co-segmentation of lung tumor on pet-ct images", *IEEE Transactions Image Processing*, vol. 24, no. 12, pp. 5854-5867, 2015.

[8] Liu. T, J. Sun, N. Zheng, "Learning to detect a salient object", *in Proceeding IEEE Conference Computer Visual Pattern Recognition*, pp. 1-8, 2007.

[9] Pawel Korus and Jiwu Huang, "Improved Tampering Localization in Digital Image Forensics Based on Maximal Entropy Random Walk", *IEEE Signal Processing Letters*, vol. 23, no. 1, pp. 169-173, 2016.

[10] Saeed Sarreshtedari and Mohammad Ali Akhaee, "A Source Channel Coding Approach To Digital Image Protection And Self-Recovery", *IEEE Transactions on image processing*, vol. 24, no.7, pp. 2266-2277, 2015.

[11] Seung-JinRyu, Matthias Kirchner, Min-Jeong Lee, and Heung-Kyu Lee, "Rotation invariant localization of duplicated image regions based on Zernike moments", *IEEE Transactions on information forensics and security*, vol. 8, no. 8, pp. 1355-1370, 2013.

[12] Tiago José de Carvalho, Christian Riess, Elli Angelopoulou, HélioPedrini and Anderson de Rezende Rocha, "Exposing Digital Image Forgeries By Illumination Color Classification", *IEEE Transactions on information forensics and security*, vol. 8, no. 7, pp. 1182 – 1194, 2013.

[13] Valentina Conotter, James F. O'Brien, and Hany Farid, "Exposing Digital Forgeries In Ballistic Motion", *IEEE Transactions on information forensics and security*, vol. 7, no. 1, pp. 283-296, 2012.

[14] Viswanath Gopalakrishnan, Yiqun Hu, and DeepuRajan,"Random Walks on Graphs for Salient Object Detection in Images", *IEEE Transactions On Image Processing*, vol. 19, no. 12, pp. 3232 – 3242, 2010.

[15] Wei Fan, Kai Wang, François Cayre, and Zhang Xiong, "Median Filtered Image Quality Enhancement And Anti-Forensics Via Variational Deconvolution", *IEEE Transactions on information forensics and security*, vol. 10, no. 5, pp. 1076-1091, 2015.