International Journal of Modern Computer Science (IJMCS)
Volume 7, Issue 3, June, 2019
ISSN: 2320-7868 (Online)

A Review of Novel Hybrid Image Forgery Detection Model

Samiksha Singla
Doaba group of colleges
Punjab, India
E-mail: samiksha.singla@gmail.com

Harpreet Tiwana
Doaba group of colleges
Punjab, India
E-mail: tiwana_harpreet9@yahoo.com

Abstract: The image forgery is the term given to the copying of the image content after editing the digital image data in order to remove the similarity with the original image. The image forgery cause monetary losses to the graphic designer professionals or the digital media companies. Latter organizations run their business from the graphic designing etc, which is severely hurt by the image forgery. The image forgery detection is the branch of digital image processing to detect the image forgery in the image content for the purpose of copyright protection. In this paper, we are proposing the image forgery detection model for the images using the hybrid algorithm, which uses the combination of the SURF, FREAK, SVM and GREEDY algorithms. The proposed model is designed to work in the double layered model for the forgery detection and relies upon the greedy algorithm for the final result generation. The proposed model is expected to outperform the existing image forgery detection models. The proposed model results would be employed in the form of accuracy, precision and recall. The statistical analysis would be performed over the obtained results in order to analyze the performance of the proposed model.

Keywords: Image forgery detection, SURF, FREAK, GREEDY, Forgery classification.

I. INTRODUCTION

Nowadays, we are living in a technically advanced world, where capturing pictorial information of any event in the form of digital images has become very simple. Currently, digital images play significant role in our everyday life, where they are being used as means for capturing pictorial information and are being employed in various domains such as medical diagnosis, daily newspapers, magazines, and as evidence at court or for insurance claims [8]. Because of the widespread applications of digital images, very powerful and easy-to-use image editing tools like Photoshop are available. Using these tools even a novice can alter the digital contents of a digital image without leaving any visible traces, which can be noticed by human eyes. The digital contents are often altered with illicit designs in mind by hiding or adding important information to an image. Therefore, the authenticity of digital images cannot be taken for granted; it needs verification and is an object for research. Copy-move forgery (CMF) is the most common type of image forgery; in this case one region is copied from one place and pasted to another place of the same image in order to conceal important information. Sometimes, the copied region is modified by pre-processing operations like scaling, rotation, adding noise, etc. to make it matching with the surrounding region so that the tempering is not visible. In another similar kind of forgery, a part is copied from one image and is pasted to a different image. This type of forgery is called image splicing. [10]

Authenticating digital images is a very serious issue and so far the researchers developed many methods, which can mainly be classified into (1) intrusive (active) and (2) non-intrusive (blind or passive) techniques [4]. Further, intrusive methods can be divided into two classes based on (1) embedding a watermark and (2) incorporating digital signature in an image. In each of these techniques, a piece of information is integrated into digital images as an aid for authenticating digital contents and security rights. Once the digital contents of an image are changed, the incorporated information is also modified. The authenticity of an image is validated by ensuring that the embedded information is unaltered. Though these methods are robust, their domain of application is restricted because all digital cameras are not equipped with the feature of embedding digital signature. In addition, these methods need pre-processing for creating labeled images. [4-9] These limitations and constraints of active methods motivated the research to propose non-intrusive methods for authenticating digital images. This class of methods do not take into consideration any kind of embedded information (such as watermarks or signatures) to validate the authenticity of a digital image. Instead, these methods draw their conclusions about the originality of the digital content of images using its structural changes, which take place due to tempering. [14]

The development of computer technology has enabled digital image forgery extremely easy and leaves no visual clue of being tampered. This fact is deteriorating the historical trust of image evidences. In digital investigation, there are active and passive ways to authenticate integrity of digital images. [8] Active techniques involve embedding of data during the time of recording or sending. Digital watermarks and digital signatures are widely used active image authentication techniques. However, it is not always feasible to embed a watermark or signature to an image. This limits the use of active techniques. Passive authentication techniques are based on the analysis of different image attributes to detect inconsistencies that might be caused by forgery. Different features of image can be used for forgery detection, pixel statistics of natural image, lossy

compression artifacts, the nature of image capturing devices, and the characteristics of interaction between physical object, light and camera and so on. [8, 10-14].

II. LITERATURE REVIEW

2014. Li, Jian et. al.[11] has proposed the segmentation-based Image Copy-move Forgery Detection Scheme. In this paper, the authors have proposed a scheme to detect the copy-move forgery in an image, mainly by extracting the keypoints for comparison. The main difference to the traditional methods is that the proposed scheme first segments the test image into semantically independent patches prior to keypoint extraction. As a result, the copy-move regions can be detected by matching between these patches. The matching process consists of two stages. In the first stage, they have found the suspicious pairs of patches that may contain copy-move forgery regions, and roughly estimated an affine transform matrix. In the second stage, an Expectation-Maximization-based algorithm is designed to refine the estimated matrix and to confirm the existence of copy-move forgery.

2014. Hashmi, Mohammad Farukh [8] has worked on the copy-move image forgery detection based on speeded up robust feature transform and Wavelet Transforms. In this paper, the authors have proposed d a series of algorithms which are combination of speeded-up robust feature transforms and Wavelet Transforms. In doing so authors have first discussed the Speeded-Up Robust Feature (SURF), SURF in combination with Discrete Wavelet Transform (DWT), SURF in combination with Dyadic Wavelet Transform (DyWT). These algorithms are different from the previously proposed algorithm in the manner that they are applied on the entire image to extract features rather than dividing the image into the blocks. From the results obtained they are able to conclude the proposed algorithms are better than their counterparts both in terms of computational complexity and invariance to scale and rotation and also for the combination of attacks.

2014 Ayalneh, Dessalegn et. al. [4] has proposed the JPEG copy paste forgery detection using BAG optimized for complex images.

Image forgery detection is one of important activities of digital forensics. Forging an image has become very easy and visually confusing with the real one. Different features of an image can be used in passive forgery detection. Most of lossy compression methods demonstrate some distinct characteristics. JPEG images have a traceable zero valued DCT coefficients in the high frequency regions due to quantization. This appears as a square grid all over the image, known as Block Artifact Grid (BAG). In this paper the BAG based copy-paste forgery detection method is improved by changing the input DCT coefficients for Local Effect computation. The proposed method has shown a better performance especially for complex images.

2014. Hussain, Muhammad [9] has performed a performance evaluation survey on WLD and LBP descriptors for non-intrusive image forgery detection. The authors have investigated the detection of copy-move and splicing, the two harmful types of image forgery, using textural properties of images. Tampering distorts the texture micro-patterns in an image and texture descriptors can be employed to detect tampering. They did comparative study to examine the effect of two state-of-the-art best texture descriptors: Multiscale Local Binary Pattern (Multi-LBP) and Multiscale Weber Law Descriptor (Multi-WLD). Multiscale texture descriptors extracted from the chrominance components of an image are passed to Support Vector Machine (SVM) to identify it as authentic or forged.

2014. Jaberi, Maryam et. al. [10] has worked with accurate and robust localization of duplicated region in copy–move image forgery. In this paper, the authors have adopted keypoint-based features for copy-move image forgery detection; however, our emphasis is on accurate and robust localization of duplicated regions. In this context, we are interested in estimating the transformation (e.g., affine) between the copied and pasted regions more accurately as well as extracting these regions as robustly by reducing the number of false positives and negatives. To address these issues, they have proposed using a more powerful set of keypoint based features, called MIFT, which share the properties of SIFT features but also are invariant to mirror reflection transformations. Moreover, they have also proposed refining the affine transformation using an iterative scheme which improves the estimation of the affine transformation parameters by incrementally finding additional keypoint matches. To reduce false positives and negatives when extracting the copied and pasted regions, they propose using “dense” MIFT features, instead of standard pixel correlation, along with hystereresis thresholding and morphological operations.

2014. Muhammad, Ghulam [14] have developed an image forgery detection technique using steerable pyramid transform and local binary pattern. In this paper, a novel image forgery detection method is proposed based on the steerable pyramid transform (SPT) and local binary pattern (LBP). First, given a color image, the authors transform it in the YCbCr color space and apply the SPT transform on chrominance channels Cb and Cr, yielding a number of multi-scale and multi-oriented subbands. Then, they describe the texture in each SPT sub band using LBP histograms.

III. PROPOSED METHODOLOGY

To mitigate the problems of the existing system, we propose the use of FREAK descriptor along with speeded-up robust features (SURF) and dyadic wavelet transform (DyWT).SVM can be use d to classify the descriptors. The DyWT will be used to decompose the image into multiple coefficients. Feature descriptor vectors will be generated on the basis of SURF and FREAK. These descriptor vectors will be analyzed on the final stage and compare with the feature descriptor vectors obtained from the target image. Then the decision will be taken after applying GREEDY algorithm on the results obtained in previous step that will returns the forged regions in case any forged (matching region or similar region) regions are found in the scanned image. The performance of the proposed algorithm will be measured on the basis of Precision, Recall, False positive rate, true positive, true negative, false positive and false negatives.

Figure1. Proposed Methodology

IV. PARAMETERS USED

There are some parameters given which is useful in our implementation:

TP = True Positive

TN = True Negative

FN = False Negative

FP = False Positive

Recall: Recall is the probability that a test will indicate 'test' among those with the matching sample.

Recall: TP/(TP+FN) × 100

Precision: Precision is the fraction of the documents retrieved that are relevant to the user's information need. In binary classification, precision is analogous to positive predictive value. Precision takes all retrieved documents into account. It can also be evaluated at a given cut-off rank, considering only the topmost results returned by the system. This measure is called precision at n or P@n.

PPV or Precision: TP/(TP+FP)

Accuracy: The percentage of the result success out of the whole results is called accuracy or success rate.

Accuracy: (TP+TN)/(TP+TN+FP+FN) * 100

V. CONCLUSION

The proposed model has been designed using the combination of the different feature descriptor algorithms. The feature extraction is performed using the FREAK and SURF models, which are further, analyzed using the support vector machine (SVM) classifier in order to find the similarity between the two images. The classifier decides the forgery in the images on the basis of the volume of similar pixels. In the case of opposite results, the greedy is utilized to produce the results by running in the biased mode. The expected outcome is the supposed to be obtained in the form of statistical parameters of precision, recall, accuracy, etc. The proposed model is expected to overcome the problems of the existing models and will perform better than the existing models.

REFERENCES

[1] Al-Qershi, Osamah M., and Bee EeKhoo. "Passive detection of copymove forgery in digital images: State-of-the-art." Forensic Science International, vol. 231, no. 1, pp. 284-295, 2013.

[2] Amerini, Irene, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo, and Giuseppe Serra. "A sift-based forensic method for copy–move attack detection and transformation recovery." IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 1099-1110, 2011.

[3] Anand, Vijay, Mohammad Farukh Hashmi, and Avinash G. Keskar. "A Copy Move Forgery Detection to Overcome Sustained Attacks Using Dyadic Wavelet Transform and SIFT Methods." In Proceedings of the 6th Asian Conference on Intelligent Information and Database Systems (ACIIDS 2014), Springer International Publishing, pp. 530-542, 2014.

[4] Ayalneh, Dessalegn Atnafu, Hyoung Joong Kim, and Yong Soo Choi. "JPEG copy paste forgery detection using BAG optimized for complex images." InAdvanced Communication Technology (ICACT), 2014 16th International Conference on, pp. 181-185. IEEE, 2014.

[5] Bo, Xu, Wang Junwen, Liu Guangjie, and Dai Yuewei. "Image copymove forgery detection based on SURF." In Proceedings of

IEEE International Conference on Multimedia Information Networking and Security (MINES-2010), pp. 889-892, 2010.

[6] E. Ardizzone, A. Bruno, and G. Mazzola, "Detecting multiple copies in tampered images." In Proceedings of the 17th IEEE International Conference on Image Processing (ICIP -10), pp.2117–2120, September 2010.

[7] Hashmi, Mohammad Farukh, Aaditya R. Hambarde, and Avinash G. Keskar. "Copy Move Forgery Detection using DWT and SIFT Features." In Proceedings of 13th IEEE International Conference on Intelligent Systems Design and Applications (ISDA-2013), pp.188-193, December 2013.

[8] Hashmi, Mohammad Farukh, Vijay Anand, and Avinash G. Keskar. "A copy-move image forgery detection based on speeded up robust feature transform and Wavelet Transforms." In Computer and Communication Technology (ICCCT), 2014 International Conference on, pp. 147-152. IEEE, 2014.

[9] Hussain, Muhammad, Sahar Q. Saleh, Hatim Aboalsamh, Ghulam Muhammad, and George Bebis. "Comparison between WLD and LBP descriptors for non-intrusive image forgery detection." In Innovations in Intelligent Systems and Applications (INISTA) Proceedings, 2014 IEEE International Symposium on, pp. 197-204. IEEE, 2014.

[10] Jaberi, Maryam, George Bebis, Muhammad Hussain, and Ghulam Muhammad. "Accurate and robust localization of duplicated region in copy–move image forgery." Machine vision and applications 25, no. 2 (2014): 451-475.

[11] Li, Jian, Xiaolong Li, Bin Yang, and Xingming Sun. "Segmentation-based Image Copy-move Forgery Detection Scheme.", Information Forensics and Security, IEEE Journals, 2014.

[12] Li, Leida, Shushang Li, Hancheng Zhu, Shu-Chuan Chu, John F. Roddick, and Jeng-Shyang Pan. "An Efficient Scheme for Detecting Copy-move Forged Images by Local Binary Patterns", Journal of Information Hiding and Multimedia Signal Processing, vol. 4, no. 1, pp. 46-56, January 2013.

[13] Mishra, Parul, Nishchol Mishra, Sanjeev Sharma, and Ravindra Patel. "Region Duplication Forgery Detection Technique Based on SURF and HAC." The Scientific World Journal, vol. 2013, Article ID 267691, pages 8, 2013.

[14] Muhammad, Ghulam, Munner H. Al-Hammadi, Muhammad Hussain, and George Bebis. "Image forgery detection using steerable pyramid transform and local binary pattern." Machine Vision and Applications 25, no. 4 (2014): 985-995.

[15] Shivakumar, B. L., and S. Santhosh Baboo. "Detection of Region Duplication Forgery in Digital Images Using SURF." International Journal of Computer Science Issues (IJCSI), vol. 8, no. 4, pp.199-205, 2011.

[16] Zhang, Chenyang, Xiaojie Guo, and Xiaochun Cao. "Duplication localization and segmentation." In Proceedings of Advances in Multimedia Information Processing(PCM 2010), pp. 578-589, Springer Berlin Heidelberg, 2010.