Splicing Forgery Detection Technique for Digital Images: A Review

Shrutika A. Korde[1], Smita A. Nagtode[2], Dinesh Bhoyar[3]
[1]*M.Tech Student, Dept. of Electronics & Telecommunication, D.M.I.E.T.R., Sawangi (Meghe), Wardha*
[2]*Asso. Prof., Dept. of Electronics & Telecommunication, D.M.I.E.T.R., Sawangi (Meghe), Wardha*
[3]*Asso. Prof., Dept. of Electronics & Telecommunication, YCCE, Nagpur*

***Abstract*- The authenticity of digital image is finding out by using Image Forgery Detection technique. For the area of digital forensics and multimedia security it is more important. Photo-editing software, powerful computers, and a device the high resolution images are used for the manipulation. So, it is very difficult for finding the transformation in the digital image by the human eyes. The proposed method to identify splicing forgery for images which are blurred, resized and angular transformed. These images need a special kind of feature extraction namely Stationary Wavelet Transform and Singular Value Decomposition in order to perform the task. For the features extraction, we will use singular value decomposition of an image. Also, the concept of color-based segmentation will be used in this work help to achieve blur invariance. We plan to improve the overall efficiency of the system with the help of multiple feature extraction techniques.**

Index Terms- Image Splicing; Stationary Wavelet Transform; Singular Value Decomposition; Multi-Scale Local Binary Pattern

I. INTRODUCTION

Image processing is a technique of converting the image into digital image and performing some operation on it, like enhancing the image or extracting some information from the image. Image processing is one of the types of signal dispensation. In image processing, input is image such as photo, video etc and output is also image or attribute related with that image or video. Nowadays, rapidly growing area in technology is image processing.

Following three steps are involved in the image processing:

- Capturing the image using image acquisition tool
- Examine the image and manipulating the image
- Last stage is the result/output in which transformed the image [14]

Nowadays, image manipulation has become easy due to many professional software packages such as Photo editor, Adobe Photoshop, etc., so that it express as a real. Such manipulation with the real images is called image forgery.

Forgery detection technique is divided into two types: 1) active and 2) passive. In the technique of active forgery detection, some pre-processing operations are required for the images such as digital signatures or digital watermarking. In passive/blind forgery detection technique, the digital images do not require digital signatures or digital watermarking. It detects the forged regions in the image. Image tampering is the part of passive forgery detection technique.

Image tampering is a digital art which needs to understand the image properties and good visual creativity. One tampers images for various reasons either to enjoy the fun of digital works creating incredible photos or to produce false evidence [8]. Image tampering is classified into three types: copy-move, image splicing, and image retouching.

A. Copy-move:

Region duplication forgery is also called as copy-move. Copy-move is one of the types of image forgery detection technique and this is a common type. In which, some part of an original image are copied, moved it and paste to the desired location in the same image. Fig. 1 shows the example of copy-move forgery.

Fig. 1: Example of copy-move forgery

B. Image Splicing:

Image splicing is a combination of two or more different images and converted it into one image to form a dublicate image. In image splicing, cutting/copied some part from the one image and pasted it to another image. So, to detect the tampered region in the image is difficult by the human eye. Below figure i.e., fig. 2 shows the image splicing forgery.

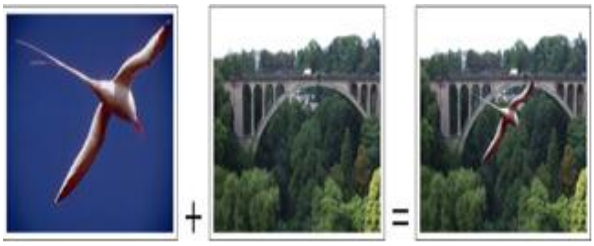

Fig. 2: Example of image splicing

C. Image retouching:

Image retouching is the process of changing the original pixel such as enhancing or reducing the features of an image. Example of image retouching is mention in the fig. 3.

Fig. 3: Example of image retouching

The proposed method to identify splicing forgery for images which are blurred, resized and angular transformed. Images are applied to pre-processing block for conversion of RGB images into YCbCr component. The images are divided into the number of blocks. These images need a special kind of feature extraction namely SWT and SVD in order to perform the task. Also, to achieve blur invariance we will use the concept of color-based segmentation.

II. RELATED WORK

Atif Shah and El-Sayed M. El-Alfy [1] detected image splicing using Multi-Scale LBP and DCT coefficient. Multi-Scale LBP was applied to the images which were divided into numbers of block, then computed DCT coefficient as well as the standard deviation. Here, the classifier Support Vector Machine with RBF kernel was predicted the forged and authentic classes of image. The results revealed 97.3% accuracy when applying multi-scale LBP.

Rahul Dixit, Ruchira Naskar, Swati Mishra [2] used SWT and SVD technique to detect copy-move foegery detection. They negotiated color-based division to implement blur invariance and to decrease the number of FPR (false positive rate), 8 connected neighborhoods were used for blurring and without blurring images. The presented method provided higher forgery DA (detection accuracy) comparing with the state-of-the-art.

XiaoBing KANG, ShengMin WEI [8] detected copy-move image forgery using SVD (singular value decomposition). For algebraic and geometric features extraction SVD (singular value decomposition) provided the method. The proposed method is effective in cases of copy-move image tampering induced with noise and robust next to retouching details.

Zahra Moghaddasi, Hamid A. Jalab, and Rafidah Md Noor [9] used the SVD-based steganalysis method with the discrete cosine transform (DCT) for the image forgery detection. The combination of SVD+SVD-DCT was given the excellent result as compared to the separate methods of SVD and SVD-DCT. The result revealed less accuracy (less than 80%).

Fahime Hikimi, Mahdi Hariri, Farhad GharehBhagi [10] detected forgery for image using LBP, wavelet transform and PCA. All extracted feature was fed into SVM classifier. The proposed method was applied to CASIA TIDA v1.0 and database of Columbia Uncompressed Image Splicing Detection Evaluation. The result showed 97.21% accuracy of CASIA TIDA v1.0 and 95.13% accuracy of Columbia database.

Sevinc Bayram, Husrev Taha Sencar, Nasir Memon [11] used transform features of Fourier Mellin, which are invariant to scaling and translation for the detection of copy-move. This method was computationally efficient and being capable forgery detection even in the image which are highly compressed.

Songpon TEERAKANOK, Tetsutaro UEHARA [3] detected copy-move forgery using Key-point selection and rotation-invariant feature descriptor

using SURF and GLCM respectively. Improving the overall accuracy of the system, proposed method needs some threshold value for further analysis.

Sondos M. Fadl, Noura A. Semary, Mohiy M. Hadhoud [12] detected copy-move forgery detection using Fast K-means and block frames features as a fast and efficient method, whether without alteration and with alternation modify in a spatial domain. The image was divided into numbers of block and then extracting the feature for every block. The result of the method was efficient to detect duplicated region under several modifications like JPEG compression, alternation and smoothing environment. The proposed method is 75% faster than other systems.

Atefeh Shahroudnejad, Mohammad Rahmati [13] proposed a method to identify tampering regions which was copy-moved under various geometrical transformations because it was based on (affine scale-invariant feature transform) which is a fully affine invariant descriptor. The method detected a large number of matched ASIFT key-points and all pixels were calculated from the duplicate region by utilizing superpixel segmentation and morphological operations. The result of the method was efficient and powerful for copy-move region detection under several transformations and post-possessing operation.

Ambili B, Prof. Nimmy George [4] developed the splicing detection technique of tampered blurred images, in this original image and spliced blur image was a different type of blurring.

Anushree U. Tembe, Supriya S. Thombre [5] studied a copy-move forgery detection technique and its classification which are a block-based method and key-point based method.

Deepika Sharma, Pawanesh Abrol [7] studied the threat of Digital Image tampering for security as well as different image tampering detection algorithms. Algorithms use various techniques for tamper detection such as Principal Component Analysis (PCA), Discrete Cosine Transform (DCT), Discrete Wavelet Transforms (DWT), and Singular Value Decomposition (SVD). Gajanan K. Birajdar, Vijay H. Mankar [6] studied different image tampering detection algorithms for Digital image forgery detection using passive techniques.

III. PROPOSED WORK

Most of the researcher has paid more attention to copy-move forgery. Some techniques are available for the detection of image splicing but accuracy is lower and not considers feature extraction.

Among the proposed approaches is image splicing recognition using multi-scale LBP with DCT but they do not consider any kind of noise or pixel level manipulation [1]. Some author detected copy-move forgery using SWT and SVD technique, in which they do not consider other forms of image region transformations, such as rotation, rescale, and reflection, in copy-move [2]. Some author detected image splicing using the combination of SVD and SVD-DCT but accuracy is lower in that case [10].

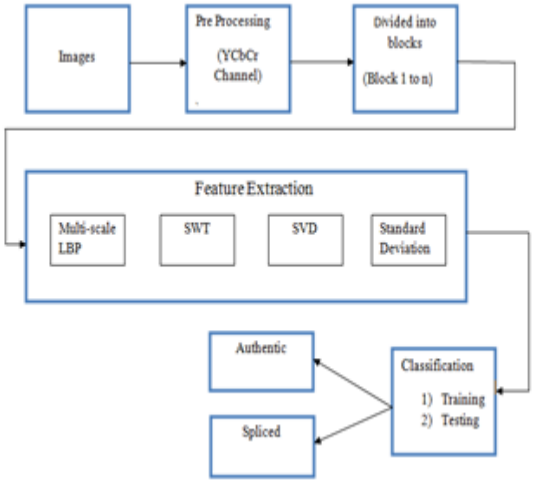

Fig. 4: Proposed model architecture

In our work, we will identify splicing forgery for images based on MS-LBP with SWT-SVD for blurred images along with resizing and angular shift. Images are applied to the pre-processing block, in which RGB images are converted into YCbCr components. The images are divided into the number of blocks. These images need a special kind of feature extraction namely SWT and SVD in order to perform the task. SWT is applied to the input YCbCr images to obtain four subbands, viz approximation, vertical, horizontal, and diagonal. Then MS-LBP is applied to each subband to find out the key points in the image. For the features extraction, we will use singular value decomposition (SVD) of an image. Also, the concept of color-based segmentation will be used in this work help to achieve blur invariance. With the help of multiple feature extraction techniques, we will improve the overall efficiency of the system.

IV. CONCLUSION

The authenticity of digital image find out by using the Image Forgery Detection technique. So it must to dig out the image is duplicate or real. We decided the propose image splicing forgery detection method for digital images, based on MS-LBP with SWT-SVD for blurred images along with resizing and angular shift, So that this work will give depth analysis for the image under test.

REFERANCES

[1] Atif Shah and El-Sayed M. El-Alfy, (2018), "Image Splicing Forgery Detection Using DCT Coefficients with Multi-Scale LBP", IEEE, 978-1-5386-4680-9/18/$31.00.

[2] Rahul Dixit, Ruchira Naskar, Swati Mishra, (2017), "Blur-invariant copy-move forgery detection technique with improved detection accuracy utilizing SWT-SVD", IET Journals, Institute of engineering and technology 2017, ISSN 1751-9659, 2017, Vol. 11 Iss. 5, pp. 301-309.

[3] Songpon TEERAKANOK, Tetsutaro UEHARA, (2018), "Copy-move Forgery Detection using GLCM-based Rotation-invariant Feature: A Preliminary Research", 42nd IEEE International Conference on Computer Software & Applications,.0730-3157/18/$31.00 ©2018 IEEE.

[4] Ambili B, Prof. Nimmy George, (2017), "A Robust Technique for Splicing Detection in Tampered Blurred Images", International Conference on Trends in Electronics and Informatics (ICEI 2017), 978-1-5090-4257-9/17/$31.00 ©2017, IEEE.

[5] Anushree U. Tembe, Supriya S. Thombre, (2017), "Survey of Copy-Paste Forgery Detection in Digital Image Forensic", International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2017), 978-1-5090-5960-7/17/$31.00 ©2017, IEEE.

[6] Gajanan K. Birajdar, Vijay H. Mankar, (2013), "Digital image forgery detection using passive techniques: A Survey", Digital Investigation, vol. 10, no. 3.

[7] Deepika Sharma, Pawanesh Abrol "Digital Image Tampering-A Threat To Security Management" International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, issues 10, ISSN (Online): 2278-1021 IJARCCE, 2013.

[8] XiaoBing KANG, ShengMin WEI, (2008), "Identifying Tampered Region Using Singular Value Decomposition in Digital Image Forensics", International Conference on Computer Science and Software Engineering, © 2008, IEEE.

[9] Zahra Moghaddasi, Hamid A. Jalab, and Rafidah Md Noor, (2014), "SVD-based Image Splicing Detection", International Conference on Information Technology and Multimedia (ICIMU), November 18 – 20, 2014, Putrajaya, Malaysia.

[10] Fahime Hikimi, Mahdi Hariri, Farhad GharehBhagi, (2015), "Image Splicing Forgery Detection Using Local Binary Pattern And Discrete Wavelet Transform", 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI).

[11] Sevinc Bayram, Husrev Taha Sencar, Nasir Memon, (2009), "An Efficient And Robust Method For Detecting Copy-Move Forgery", 978-1-4244-2354-5/09/$25.00 ©2009, IEEE.

[12] Sondos M. Fadl, Noura A. Semary, Mohiy M. Hadhoud, (2014), "Copy-Rotate-Move Forgery Detection Based On Spatial Domain", 978-1-4799-6594-6/14/$31.00 ©2014, IEEE.

[13] Atefeh Shahroudnejad, Mohammad Rahmati, (2016), "Copy-Move Forgery Detection In Digital Images Using Affine-SIFT", 978-1-5090-5820-4/16/$31.00 ©2016, IEEE

[14] Introduction to image processing website [online]https://sisu.ut.ee/imageprocessing/book/1

[15] https://ai2-s2public.s3.amazonaws.com /figures /2017-0808/6c96317aa8883d3223 a4c7f49231a 5e88f 7a8f14 /5-Figure10-1.png

[16] https://ars.els-cdn.com/content/image/1-s2.0-S0923596515001393-gr6.jpg

[17] https://aescripts.com/media/blog/post/digital-beauty-retouch---age-reduction-vfx.jpg