Splicing Forgery Detection Technique by using SWT and MS-LBP

Smita A. Nagtode, Shrutika A. Korde

Abstract: The authenticity of digital image find out by using the Image Forgery Detection technique. In 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 SWT in order to perform the task. MS-LBP is applied to the SWT for finding key-points and creating the database to show the forgery status as well as features of the image. Match the new keypoints with the saved databased and display the output.

Keyword: Image Splicing, Stationary Wavelet Transform, Singular Value Decomposition, *Multi-Scale Local Binary Pattern*

I. INTRODUCTION

Image processing is a technique of changing the images into digital images along with it performs some kind of action on it, like enhancing the image or extracting the data. Image processing is one of the types of signal dispensation. In image processing, input is an image such as photo, video, etc. and output is also the image or attribute related to that image or video. Nowadays, rapidly growing area in technology is image processing.

Following the three steps are involved in the image processing:

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

Nowadays, image manipulation has become easier due to various specialized software like Photo editor, Adobe Photoshop, etc., so it expresses as a real. Such manipulation with the real images is called image forgery.

Forgery detection technique is divided in 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 the passive forgery detection technique.

Image tampering is a skill 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 the type of image forgery detection technique and this is a common type. In which, some part of an real image is copied, passed it and paste in the particular place of the correlative image. Following fig. 1 illustrate the copy-move forgery.

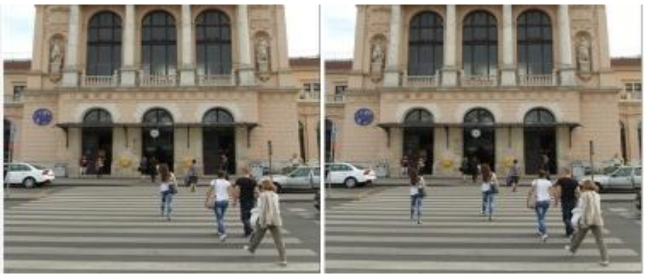


Fig. 1 Copy-move Forgery

B. Image Splicing

Image splicing is a fusion of more than one different images also converted to one image to form a duplicate image. In image splicing, cutting/copying some part of the one image and pasted it to another image. So, to detect the tampered region in the image is difficult by the human eye. Following fig. 2 shows the image splicing forgery.

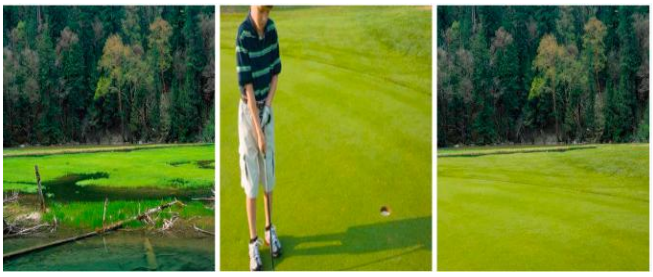


Fig. 2 Image Splicing Forgery

C. Image Retouching

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

Revised Manuscript Received on December 22, 2018.

Smita A. Nagtode, Associate Professor, D.M.I.E.T.R Wardha
Shrutika A. Korde, Associate Professor, D.M.I.E.T.R Wardha

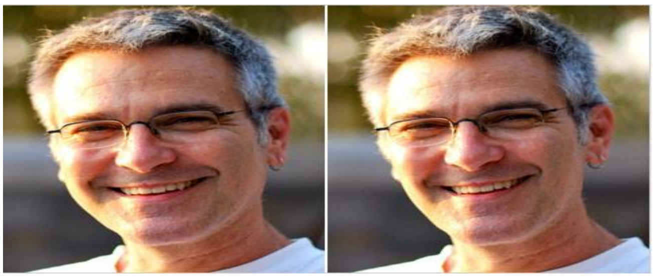


Fig. 3 Image Retouching

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 need a special kind of feature extraction namely SWT in order to perform the task. MS-LBP is applied to the SWT for finding key-points. Depending upon the key-points we can find out forgery status and the features of the image which are mentioned in the created database. Match each keypoint of the new image with the created database and display the messege i.e., image is forged or not forged.

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 blocks, 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 forgery detection. They negotiated color-based division to implement blur invariance and to decrease the number of the FPR (false positive rate), 8 connected neighborhoods were used for blurring and without blurring the 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 by noise and robust next to retouching details.

Fahime Hikimi, Mahdi Hariri, Farhad GharehBhagi [10] detected forgery for an 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 to 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 frame 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 the 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 were copy-moved under various geometrical transformations. 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-processing 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.

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, in copy-move [2]. Some author detected image splicing using the combination of SVD and SVD-DCT but accuracy is lower in that case [9].

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.

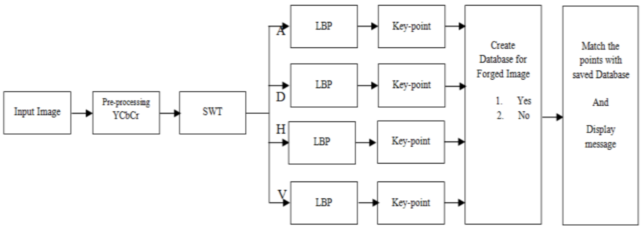


Fig. 4 Proposed model architecture

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Fig. 5 shows the input images first one is the real image and another one is the forged image.

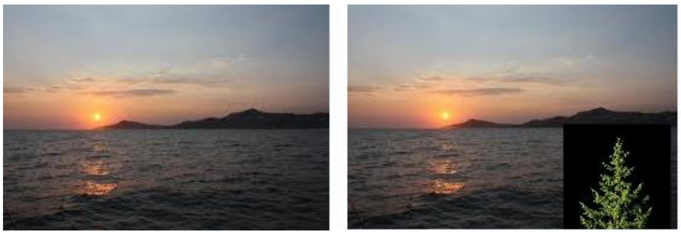


Fig. 5 Input Images (a) Original Image (b) Forged Image

A. Pre-processing Unit

Images are applied to the pre-processing block, in which convert the RGB images into YCbCr color space. YCbCr contains luminance (Y), and the Chrominance (Cb and Cr), where Cb is the Chrominance-blue and Cr is the Chrominance-red color value as a column. The transformation formula is as follows:

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} + \begin{bmatrix} 65.485 & 128.553 & 24.966 \\ -37.797 & -74.203 & 112.0 \\ 112.0 & -93.786 & -18.214 \end{bmatrix} \cdot \begin{bmatrix} R \\ G \\ B \end{bmatrix}$$

Pixels are represented in RGB format, i.e., 8 bits per sample, where a black color represented by 0 and white color represented by 255 respectively, the YCbCr components can be obtained by using the above equations.

B. SWT (Stationary Wavelet Transform)

The 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 A (approximation), D (diagonal), H (horizontal), and V (vertical).

C. MS-LBP (Multi-Scale Local Binary Pattern)

MS-LBP is applied to each subband (i.e. A (approximation), D (diagonal), H (horizontal), and V (vertical)) to identify the key-points in the image. Depending upon the key-points we can find out the forgery status of the image.

Key-points of real image and forged image are shown in the fig. 6 and fig. 7. Image is split into four subband (i.e. A (approximation), D (diagonal), H (horizontal), and V (vertical)). Each subband has its individual key-point.

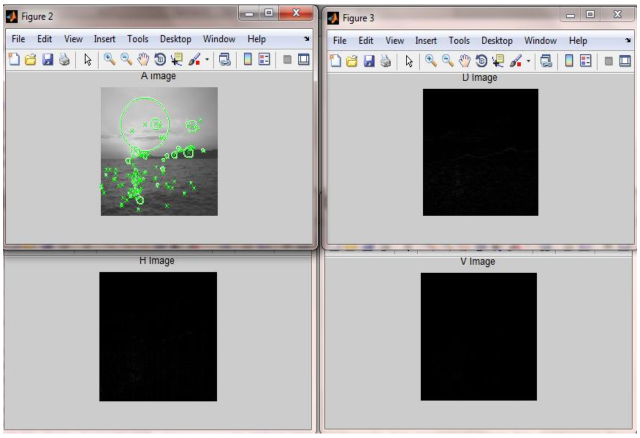


Figure 2
File Edit View Insert Tools Desktop Window Help
A image
Figure 3
File Edit View Insert Tools Desktop Window Help
D image
H image
V image

Fig. 6 Keypoints of Original Image

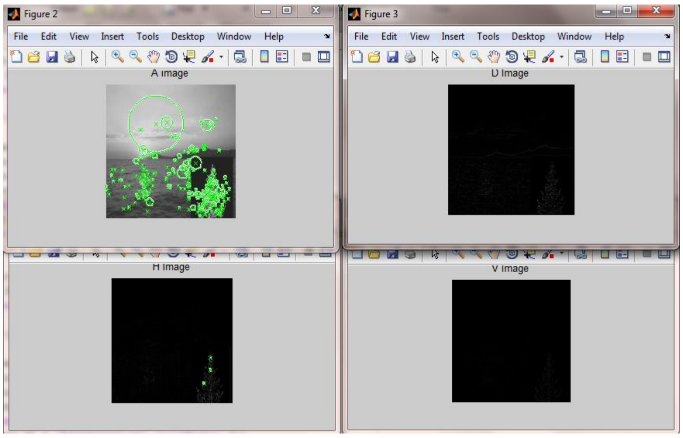
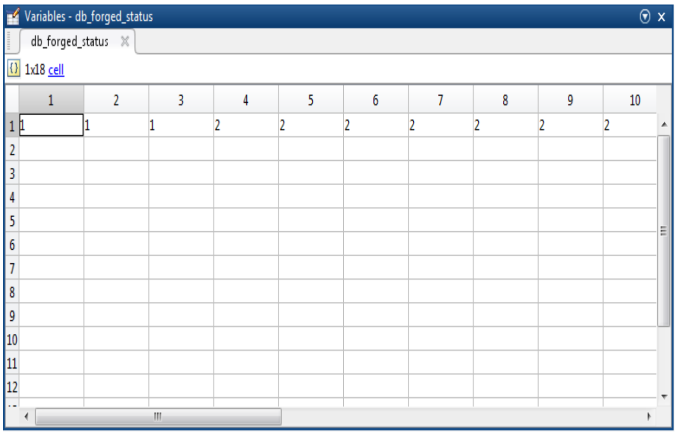


Figure 2
File Edit View Insert Tools Desktop Window Help
A image
Figure 3
File Edit View Insert Tools Desktop Window Help
D image
H image
V image

Fig. 7 Keypoints of Forged Image

Subsequently, we are creating a database for forgery status and the features of the image which are divided into subband i.e., A (approximation), D (diagonal), H (horizontal), and V (vertical). Forgery status of original image and forged image are shown in the database of fig. 8.

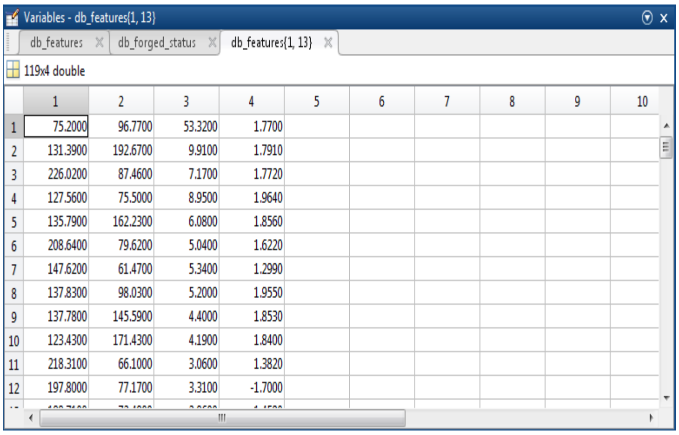


1x18 cell

	1	2	3	4	5	6	7	8	9	10
1	1	1	1	2	2	2	2	2	2	2
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										

Fig. 8 Forgery Status of Images

In forgery status of images, 1 is denoted as spliced image and 2 is denoted as non-spliced image. Features of original image and forged image are shown in the database of fig. 9 and fig. 10.

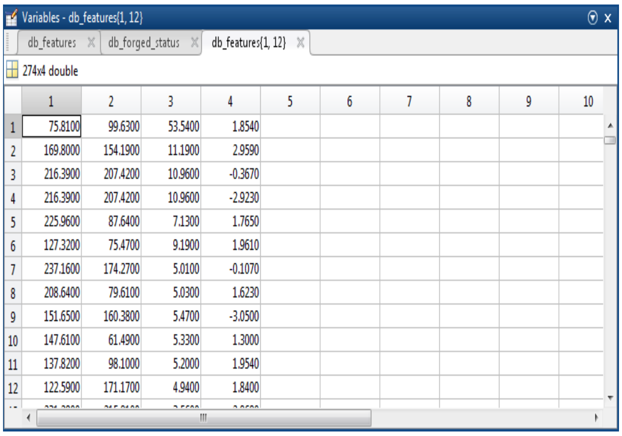


119x4 double

	1	2	3	4	5	6	7	8	9	10
1	75.2000	96.7700	53.3200	1.7700						
2	131.3900	192.6700	9.9100	1.7910						
3	226.0200	87.4600	7.1700	1.7720						
4	127.5600	75.5000	8.9500	1.9640						
5	135.7900	162.2300	6.0800	1.8560						
6	208.6400	79.6200	5.0400	1.6220						
7	147.6200	61.4700	5.3400	1.2990						
8	137.8300	98.0300	5.2000	1.9550						
9	137.7800	145.5900	4.4000	1.8530						
10	123.4300	171.4300	4.1900	1.8400						
11	218.3100	66.1000	3.0600	1.3820						
12	197.8000	77.1700	3.3100	-1.7000						

Fig. 9 Features of Original Image

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication



	1	2	3	4	5	6	7	8	9	10
1	75.8100	99.6300	53.5400	1.8540						
2	169.8000	154.1900	11.1900	2.9590						
3	216.3900	207.4200	10.9600	-0.3670						
4	216.3900	207.4200	10.9600	-2.9230						
5	225.9600	87.6400	7.1300	1.7650						
6	127.3200	75.4700	9.1900	1.9610						
7	237.1600	174.2700	5.0100	-0.1070						
8	208.6400	79.6100	5.0300	1.6230						
9	151.6500	160.3800	5.4700	-3.0500						
10	147.6100	61.4900	5.3300	1.3000						
11	137.8200	98.1000	5.2000	1.9540						
12	122.5900	171.1700	4.9400	1.8400						

Fig. 10 Features of Forged Image

When uploading the new image in the system, match each keypoint of the new image with the saved database. If forged count is greater than non-forged count then display the massege i.e., image is classified as FORGED otherwise it is display as a image is classified as NOT FORGED. Output of the original image and forged image are shown in the fig. 11 and fig. 12.

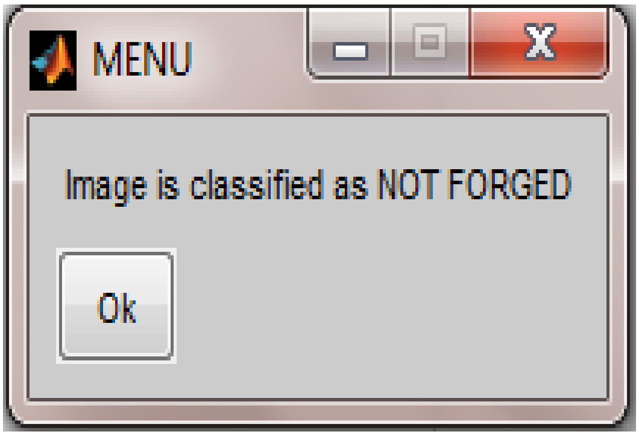


Image is classified as NOT FORGED

Fig. 11 Output of Original Image

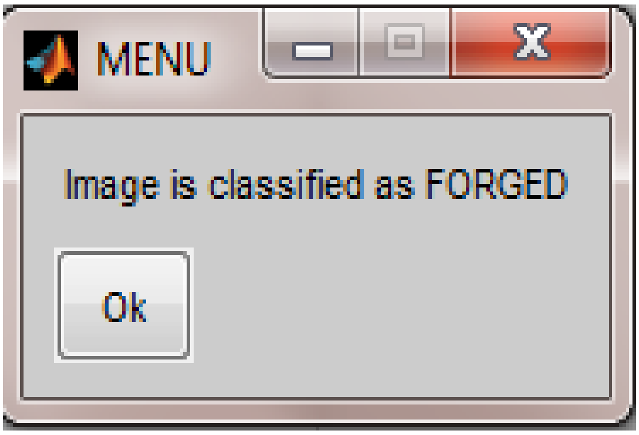


Image is classified as FORGED

Fig. 12 Output of Forged Image

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. The proposed model of this paper is based on Multi-Scale Local Binary Pattern (MS-LBP) with SWT coefficient for the detection image splicing. Images are applied to pre-processing block for conversion of RGB images into YCbCr component. The images need a special kind of feature extraction namely SWT in order to perform the task. MS-LBP is applied to the SWT for finding key-points. By utilizing the key-points from the image, we can depict the features and forgery status. Compairing the features of the saved databased with the new image feature and obtain the output in the form of messege. For further work we are going to extract the features of an image, so that this work will give depth analysis of the image under test.

REFERENCES

1. Atif Shah and El-Sayed M. El-Alfy, “Image Splicing Forgery Detection Using DCT Coefficients with Multi-Scale LBP”, 978-1-5386-4680-9/18/$31.00 ©2018 IEEE.
2. Rahul Dixit, Ruchira Naskar, Swati Mishra, “Blur-invariant copy-move forgery detection technique with improved detection accuracy utilizing SWT-SVD”, IET Journals, ISSN 1751-9659, 2017, Vol. 11 Iss. 5, pp. 301-309, © Institute of engineering and technology 2017.
3. Songpon TEERAKANOK, Tetsutaro UEHARA, “Copy-move Forgery Detection using GLCM-based Rotation-invariant Feature: A Preliminary Research”, 2018 42nd IEEE International Conference on Computer Software & Applications,.0730-3157/18/$31.00 ©2018 IEEE.
4. Ambili B, Prof. Nimmy George, “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, “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 “Digital image forgery detection using passive techniques: A Survey”, Digital Investigation, vol. 10, no. 3, 2013.
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, “Identifying Tampered Region Using Singular Value Decomposition in Digital Image Forensics”, 2008 International Conference on Computer Science and Software Engineering, © 2008 IEEE.
9. Zahra Moghaddasi, Hamid A. Jalab, and Rafidah Md Noor, “SVD-based Image Splicing Detection”, 2014 International Conference on Information Technology and Multimedia (ICIMU), November 18 – 20, 2014, Putrajaya, Malaysia.
10. Fahime Hikimi, Mahdi Hariri, Farhad GharehBhagi, “Image Splicing Forgery Detection Using Local Binary Pattern And Discrete Wavelet Transform”, 2015 2nd International Conference on Knowledge-Based Engineering and Innovation(KBEI).
11. Sevinc Bayram, Husrev Taha Sencar, Nasir Memon, “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, “Copy-Rotate-Move Forgery Detection Based On Spatial Domain”, 978-1-4799-6594-6/14/$31.00 ©2014 IEEE.
13. Atefeh Shahroudnejad, Mohammad Rahmati, “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://ars.els-cdn.com/content/image/1-s2.0-S0379073817302967-gr1.jpg
16. https://ars.els-cdn.com/content/image/1-s2.0-S0925231216312747-gr1.jpg
17. https://static01.nyt.com/images/2009/08/25/technology/personaltech/rikliquify.480.jpg.

AUTHORS PROFILE

Smita Nagtode received her B.E.(Electronics) degree in 1998, M.E.(Electronics) degree from SGGS College of Engineering & Technology, Nanded in 2001 and PhD in 2016 from Nagpur university. Presently she is working as Associate Professor in department of Electronics and telecommunication engeneering, D.M.I.E.T.R., Wardha. Her field of research is speech recognisition and image processing.

Shrutika A. Korde received her B.E.(Electronics) degree in 2016 from B.D.C.O.E., Wardha. She is currently pursuing her M.E.(Electronics and Communication) degree from D.M.I.E.T.R., Wardha.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication