Image Region Duplication Identification: A review

S. V. Deshpande, S. K. Jagtap

Abstract— This paper studies reviews of image Region duplication identification. Currently, digital images being the main source of information have gain high importance. Also with the popularity of low cost, high resolution digital cameras & sophisticated editing software, digital image tampering has become relatively easy. This makes authenticity of digital images untrustful. So it is very necessary and challenging to find effective methods to detect digital image forgeries. One of the specific types of forgery, where a part of the image is copied and pasted on another part of the same image and post processing is done, without leaving obvious visual clues, is called region duplication forgery. To detect the region duplication attacks, block based and key-point based methods are integrated together. The host image is divided into non-overlapping and irregular blocks adaptively using over-segmentation algorithm. The feature points are then extracted from each block as block features. The block features are matched with one another to locate the labelled feature points, which approximately indicate the suspected forgery regions. Then forgery region extraction algorithm is used to detect more accurate forgery regions. Finally morphological operation is applied to generate the detected forgery regions. As compared to previous methods this forgery detection method achieves much better detection results.

Index Terms— Image forensics, image tampering, region duplication forgery detection, adaptive over-segmentation, block feature extraction, feature matching, forgery region extraction.

1 Introduction

In past few decades, with increase in number of internet user digital images have become the main source of information. These images play an essential role in courtrooms, where they are used as evidence. Every day newspapers and magazines depend on digital images. Physicians make critical decisions based on digital images. But anyone with little knowledge in software like Adobe Photoshop can create forged images, without leaving any perception clues of event, though the statistics of image has been altered. These tampered images can be used to miscarry justice by wippping off important element or person from evidence image, destroy someone's reputation by replacing his face in photo with someone else face, mislead the public opinion, destroy the truth of news reports. So the authenticity ie trustworthiness of image is significant in many social areas and has become the largest growth profession of 21st century.
Region duplication is one of the specific types of forgery, where a part of the image is copied and pasted on another part of the same image and post processing is done, with the intent of hiding undesired objects or replicating objects. Practically this type of forgery involves intermediate operations and such as rotation, reflection, scaling or combination of two or more operations to provide a type of spatial synchronization and homogeneity between the copied region and its neighbors. Post-processing operations are used to remove any detectable traces of the region duplication operation, such as sharp edges. Post-processing operations could be additive noise, JPEG compression or blurring.
The existing key point based and block based algorithms divide the host image into over-lapping rectangular blocks of fixed size. Then these blocks are matched for detecting the forgery. So the detected regions are always the regular sized blocks. They can not represent the forgery regions accurately so the recall rate is low. To address these problems region duplication forgery detection using adaptive over segmentation and feature point matching method is proposed.

- *S.V.Deshpande is currently pursuing masters degree program in Electronics & Telecommunication Engineering in Smt. Kashibai Navale College of Engineering Pune, India, PH-9422144010, E-mail: sunetradeshpande5@gmail.com.*
- *Prof. (Dr.) S. K. Jagtap, Head, Electronics & Telecommunication Engineering, Smt. Kashibai Navale College of Engineering, Pune , India, PH-9404995702, E-mail: skjagtap.skncoe@sinhgad.edu.*

2 Literature Review

Fridrich et al [1] proposed the first method for copy-move forgery detection where it is suggested that there is correlation between copied image segment and the pasted one which can used as the basis for detection of this type of forgery. The detection algorithm allow for an approximate match of small image segments. The forged segments are considered to be connected component rather than a collection of very small patches or individual pixels. The DCT coefficients are exploited as feature that is robust against JPEG compression. The B×B block is slide along the image from the upper left corner to the down to the lower right corner by one pixel. For each position of this block, DCT transform is calculated. The quantized coefficients are stored in the matrix A as one row with B×B columns and (M– B+1)

(N–B+1) rows. The rows of matrix A are sorted lexicographically. If two consecutive rows of matrix A are found matched, the positions of the matching blocks is stored in a separate list. For each matching pair of blocks, the normalized shift vector counter C, which is initially set to zero is incremented by one: C (s1, s2) = C (s1, s2) + 1. Then the normalized shift vectors, whose occurrence C(s(r)) exceeds user defined threshold T for all r = 1, …, K are found. At the end the matching blocks that have contributed to the specific shift vector are colored with same color. The advantage of exploiting DCT as a feature descriptor is the simplicity, relative reduction in the feature vector size and robustness to post-processing operations, like additive noise and JPEG compression. The method cannot resist the geometric operations and cannot detect small duplicated regions.

Hu et al [2] grouped the DCT coefficients as feature vector and distance between every pair of vector is sorted to reduce the false positive rate. The algorithm is simple and robust to noise.

Myna et al [3] proposed the forgery detection algorithm that applies DWT to the input image to get reduced dimensional representation. The image blocks are then mapped to the log-polar co-ordinates. The log polar transform is achieved by mapping the Cartesian space co-ordinates into radius r and angle θ relative to the origin of the coordinate system. Then matched blocks are then identified by performing exhaustive search, using phase correlation as the similarity criteria. The matching is done only once at the lowest resolution of wavelet transform. Only the matched blocks are considered for comparison to the next level. This reduces the forgery detection time. The log polar transform is invariant to intermediate operations like scaling and translation but it is not robust against post-processing operations and depends on several thresholds, which mean that they require many images and a substantial number of experiments to set the thresholds for the best performance.

Langille and Gong [4] proposed a method based on searching the blocks with similar intensity patterns. The input image is first segmented into blocks. The algorithm sorts the blocks based on pixel information using a kd-tree based sorting technique. Sorting ensures that reasonably similar blocks are located in close proximity. So instead of exhaustive search, the search within a variable-sized neighbourhood is required. The found matches are encoded as a color image. Then a refining operation,
consisting of a series of colour-based morphological operations, is applied to remove isolated mismatches and fill in missing matches in the detection results. The method has advantage of reducing the computational complexity, computation time and reduced vector size but it is not robust against geometric operations.

Huang et al [5] proposed the first method that do not divide the image into blocks but extract distinctive features called as SIFT (Scale Invariant Feature Transform) from whole image. These features are invariant to changes in noise, illumination, distortion and viewpoint and robust to image scale and rotation. SIFT descriptors are then matched between each other to detect any possible forgery in images. The advantage of this method is its robustness and sensitivity to post image processing operations such as additive noise and lossy JPEG compression, but it cannot detect the small size tampered region efficiently.

Bo et al [10] suggested the Speeded Up Robust Feature (SURF) descriptor that detects the key-points which are invariant to rotation and scaling.

3 PROPOSED METHODOLOGY

Image forgery detection using adaptive over-segmentation and feature point matching combines both block-based and keypoint based forgery detection methods.

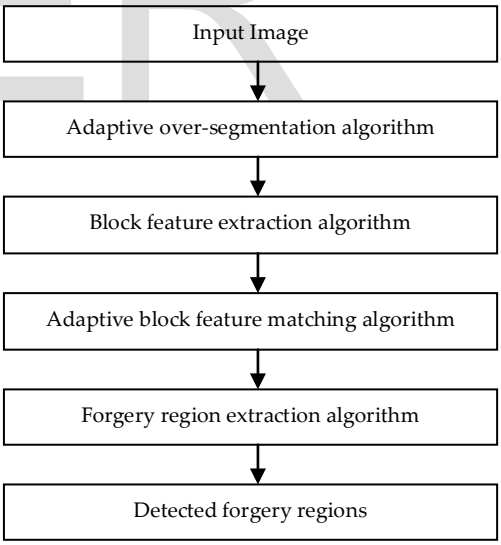

Fig. 1: Flow Diagram of image region duplication detection system.

3.1 Adaptive Over-Segmentation Algorithm

This algorithm divides the image into non-overlapping regions of irregular shape using SLIC (Simple linear Iterative Clustering) algorithm. The slic adopts k-means clustering approach to generate the superpixels. It is difficult to decide the initial size of the superpixel which is important to obtain

the good forgery detection results. Practically it is difficult to decide the initial size of the superpixel. The adaptive over-segmentation method is proposed that can determine the initial size of the superpixel adaptively based on the texture of the host image. When the texture of host image is smooth the size of superpixelis is selected to be large which insures that superpixels get close to the edges and contains sufficient feature points that can be used for forgery detection. The Larger size of superpixels reduces number of blocks and computational complexity. On the other hand if texture of the host image has more details we can set the initial size of the superpixel to be relatively smaller which ensures good forgery detection results.

The host image first undergoes four level Discrete Wavelet Transform using 'Haar' wavelet. Then the two parameters, E_{LF} low-frequency energy and E_{HF} high frequency energy, are calculated as follows.

$$E_{LF}=\sum|CA_4| \quad (1)$$

$$E_{HF}=\sum(\sum|CD_i|+\sum|CH_i|+\sum|CV_i|), i=1,2,\dots,4 \quad (2)$$

where CA_4 indicates the approximation coefficients at the 4th level of DWT; CD_i , CH_i and CV_i indicate the detailed coefficients at the i^{th} level of DWT, i = 1, 2, ..., 4.

Then P_{LF} , the percentage of the low-frequency distribution is calculated as

$$P_{LF}=\frac{E_{LF}}{E_{LF}+E_{HF}}.100\% \quad (3)$$

Depending upon P_{LF}, the initial size of the superpixel *is* determined

$$S=\begin{cases}\sqrt{0.02\times M\times N} & P_{LF}>50\% \\ \sqrt{0.01\times M\times N} & P_{LF}\leq 50\%\end{cases} \quad (4)$$

where S indicates the initial size of the superpixels

$M\times N$; indicates the size of the host image; P_{LF} shows the percentage of the low-frequency distribution.

3.2 Block Feature Extraction Algorithm

The block features are extracted from the image blocks (IB) using SIFT feature point extraction method.

The scale-space of input image I(x,y) is found as

L(x,y,σ)=G(x,y,σ)*I(x,y)

Here * indicates the convolution operation in x and y directions, σ indicates factor of scale space and Gaussian function

$$G(x,y,\sigma)=\frac{1}{2\pi\sigma^2}e^{\frac{x^2+y^2}{\sigma^2}} \quad (5)$$

To detect the keypoints in SIFT that are invariant to scale and orientation, the scale space extrema in the difference of Gaussion function convolved with image, D(x,y,σ) is used. This can be found from difference of two nearby scales separated by a constant factor k.

$$D(x,y,\sigma)=[G(x,y,k\sigma)-G(x,y,\sigma)*I(x,y) \quad (6)$$
$$=L(x,y,k\sigma)-L(x,y,\sigma)$$

The convolved images are grouped by octave. Each octave doubles the value of σ. Then value of k is selected so as to obtain fix no. of blurred images per octave. Each pixel in DoG images is compared with its eight neighbours at the same scale and nine corresponding neighbours in each of the neighbouring scales. Maximum or minimum pixel value among all compared pixels is selected as keypoint.

At the end of first step too many keypoints are obtained. Keypoints with low contrast are sensitive to noise or poorly localized along an edge. So these keypoints are rejected. Each keypoint is then assigned with one or more orientations which is calculated from an orientation histogram of local gradients, from closest smoothed image L(x,y,σ). The gradient magnitude m(x,y) and orientation θ(x,y) for each image sample L(x,y) at keypoint scale σ is calculated using pixel differences.

$$m(x,y)=\sqrt{L_1^2+L_2^2} \quad (7)$$

$$\theta(x,y)=\arctan(L_2/L_1) \quad (8)$$

$$L_1=L(x+1,y,\sigma)-L(x-1,y,\sigma). \quad (9)$$

$$L_2=L(x,y+1,\sigma)-L(x,y-1,\sigma). \quad (10)$$

From the gradient orientation of sample points within region around keypoint, an orientation histogram with 36 bins with each bin covering 10^0 is formed. Maximum orientation is assigned to this keypoint. Thus additional keypoints are created with orientation within 80% of maximum orientation.

Feature descriptor as a set of orientation histogram on 4X4 pixel neighbourhoods is computed. Orientation histogram contains 8 bins each and each descriptor contains 4X4 array of 16 histograms around the keypoint. This gives SIFT feature vector with (4X4X8)=128 elements.

Once the keypoints from an unknown input image are extracted, they are matched with each other to detect the region duplication forgery.

3.3 Block Feature Matching Algorithm

In this algorithm first number of feature points which are matching between two blocks, called as correlation coefficients (CC), are calculated. The feature points $f_a(x_a,y_a)$ and feature point $f_b(x_b,y_b)$ are said to be matched only if

$$d(f_a,f_b).TR_P\leq d(f_a,f_i) \quad (11)$$

where $d(f_a,f_b)$means the Euclidian distance between the feature points, f_a and f_b .

$$d(f_a,f_b)=\sqrt{(x_a-x_b)^2+(y_a-y_b)^2} \quad (12)$$

$$d(f_a,f_i)=\sqrt{(x_a-x_i)^2+(y_a-y_i)^2}, i=1,2\dots n; i\neq a, i\neq b \quad (13)$$

$d(f_a,f_i)$ is the Euclidian distances between the keypoints f_a and all of the other keypoints in the corresponding block, i is the i^{th} feature points and n is the number of feature points in the corresponding block. TR_P is set to 2 to provide a good trade-off between the matching accuracy and miss

probability. From CC, the correlation coefficient map is generated. The correlation coefficients are sorted in ascending order as CC_S= {CC1, CC2, CC3...CCt} Where t ≤ N(N-1)/2 and N is number of blocks. Then the first derivative $\nabla(CC_S)$ and the second derivative $\nabla^2(CC\_S)$ of CC_S, and mean value of the first derivative vector $\overline{\nabla(CC\_S)}$ are calculated. The minimum correlation coefficient for which the second derivative is larger than the mean value of the corresponding first derivative vector as defined in (8) is selected. This selected Correlation coefficient value is used as the block matching threshold TR_B.

$$\nabla^2(CC_S) > \overline{\nabla(CC\_S)} \quad (14)$$

If the correlation coefficient of the block pair is larger than TR_B, the corresponding block pair will be determined as the matched blocks.

3.4 Forgery Region Extraction Algorithm

After extracting the labelled feature points (LFP) , which are the locations of the forgery regions, SLIC algorithm with initial size of superpixels S, is applied to replace the LFP with small superpixels to obtain suspected forgery regions (SR). To improve the *precision* and *recall* results, the local color feature of the superpixels are measured. If their color feature is similar to that of the suspected regions, then the neighbor superpixels are merged into the corresponding suspected regions, which generate the merged regions (MR). Finally, a close morphological operation is applied
to the merged regions to generate the detected region duplication forgery regions.

4 CONCLUSION

Image region duplication identification using adaptive over-segmentation and keypoint matching method gives novel approach to determine the initial size of the superpixels adaptively depending upon the texture of host image. It is robust to various attacks such as scaling, rotation, JPEG compression. The forgery region extraction algorithm helps to reduce the possibility of the forgery region being undetected. The future work can be focus on applying the proposed method on other type of forgery such as splicing or on other type of media like audio, video.

REFERENCES

[1] J. Fridrich, D. Soukal, and J. Lukáš, "Detection of Copy-Move Forgery in Digital Images," Proceedings of DFRWS 2003. Cleveland, OH, USA, 2003

[2] J. Hu, H. Zhang, Q. Gao, and H. Huang, "An improved lexicographical sort algorithm of copy-move forgery detection," in Proceedings - 2nd International Conference on Networking and Distributed Computing, ICNDC 2011, 2011, pp. 23–27.

[3] A. N. Myna, M. G. Venkateshmurthy, and C. G. Patil, "Detection of Region Duplication Forgery in Digital Images Using Wavelets and Log-Polar Mapping," in Conference on Computational Intelligence and Multimedia Applications, 2007. International Conference on, 2007, vol. 3, pp. 371–377.

[4] A. Langille and G. Minglun, "An Efficient Match-based Duplication Detection Algorithm," in Computer and Robot Vision, 2006. The 3rd Canadian Conference on, 2006, p. 64.

[5] H. Huang, W. Guo, and Y. Zhang, "Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm," in Proceedings - 2008 Pacific-Asia Workshop on Computational Intelligence and Industrial Application, PACIIA 2008, 2008, vol. 2, pp. 272–276.

[6] R. Achanta, A. Shaji, K. Smith, A. Lucchi, P. Fua, and S. Süsstrunk, "SLIC superpixels compared to state-of-the-art superpixel methods," IEEE Trans. Pattern Anal. Mach. Intell., vol. 34, no. 11, pp. 2274–2282, Nov. 2012.

[7] Y. Huang, W. Lu, W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery in images," Forensic Science International, vol. 206, no. 1–3, pp. 178–184, 2011.

[8] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," Information Forensics and Security, IEEE Transactions on, vol. PP, no. 99, p. 1, 2011.

[9] X. Pan and S. Lyu, "Region Duplication Detection Using Image Feature Matching," IEEE Transactions on Information Forensics and Security, vol. 5, no. 4, pp. 857–867, 2010.

[10] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image Copy-Move Forgery Detection Based on SURF," in International Conference on Multimedia Information Networking and Security (MINES), 2010, pp. 889–892.

[11] Chi-Man Pun, Senior Member, IEEE, Xiao-Chen Yuan, Member, IEEE, and Xiu-Li Bi, " Image forgery detection using adaptive oversegmentation and feature point matching, " IEEE Transactions On Information Forensics and Security, Vol 10, NO. 8, pp. 1705 – 1716, DOI : 10.1109/TIFS.2015.2433261, 2015.