

An Efficient Image Forensic Mechanism using Super pixel by SIFT and LFP Algorithm

SHAHABUDDIN.S.K¹, DR. A.R.ASWATHA²

¹ Mtech Student, 4th semester, Department of Telecommunication, Dayananda Sagar College of Engineering, Bangalore -78, Karnataka,India

²Professor and Head, Department of Telecommunication, Dayananda Sagar College of Engineering, Bangalore-78, Karnataka,India

Abstract—Image forgery is a very significant and challenging area in the field of image processing and its applications. One of the very commonly used image forgery technique is the copy-move technique which is not only a common technique but also a challenging technique. Initially a wavelet decomposition method is applied in order to compute the size of super pixels which is further applied to segmentation block. Post segmentation the feature extraction and feature matching is performed using suitable methods. Consequently region growing is performed in order to detect the forged area in the image. Finally the region of forgery is detected and evaluated using the measures of precision, sensitivity, specificity and F1 score. Experimental results show an increased performance in the above defined measures.

Key-Words: Image Forgery, Copy-Move Method, Wavelet Decomposition, Segmentation, Region Growing

1. Introduction

In the present day of image processing applications, the sophistication and complexity of images has increased to a considerable extent, which provides a broader scope in variety of areas ranging from military applications to biomedical applications. However, the increase in altering (editing) the image has linearly increased, with the commercialization of image editing tools, the issue has only deepened to the extent where the credibility and authenticity of the image is questionable. One practical application highlighting this issue involves the editing of photography in a crime scene; the aggregator could alter the content in the image deliberately in order to hide the key evidence which might otherwise be visible in the respective image.

Image forgery is defined as a manipulation of digital image in order to conceal or alter the meaningful or useful information present in the image. The first person to have successfully altered the image was in 1840 by a man named Hippolyta Bayard who edited a picture of himself.

However, the extent of digital forgery in the image does not differ much from its original image which makes it difficult for the interpreter to identify the element of forgery in the edited image.

The Copy-Move technique is considered as one of the most commonly used image tampering technique. It is also considered as one of the most difficult technique. This is due to the factor that the manipulation of image content is within the image itself. In this technique, a part of the image is deliberately covered by copying a part of the image and pasting (Moving/ superimposing) it in another place in the same image. The intention of implementing this technique is to alter the image by hiding a portion/part of an image.

Tu and Dong [11] have significantly explained the image feature matching and also the histogram equalization mechanism. The algorithm implemented for features matching of an image will provide the better efficiency with the image scale, rotation, illumination difference for practical applications. The image acquisition process includes various conditions like posture, position and camera performance etc., for the image area. The projective distortion of the image area will affect the accuracy in FP matching/extraction. The author has given the preprocessing mechanism to enhance the significant features of the image by using the histogram equalization. Later the image is subjected to ASIFT and SIFTS algorithms for matching and extraction. The experiment conducted by the author gives the improved way to get more number of feature points by histogram equalization.

The color spaces evaluation to detect the feature point of image for the matching application is explained in Sirisha and Sandhya [12]. The study of the authors includes the inspection of the color information according to the FP detection. These color information's are expressed as HSV, XYZ, RGB, LAB, YIQ, CMY, CbCr and opponent. Later more relevant color space will be problem and hence the processing of color image is done. The image matching is done with the Hybrid color space while the Principal Component Analysis (PCA) is used for feature selection. The experiment is conducted by keeping the total repeatability measurement and total feature points for evaluation.

Wang and Wang [13] have illustrated an algorithm for background image feature point matching. Author has focused on the issues of the matching the feature points of an complex background image having weak robustness and low reliability. The authors have carried multiple time real time experimental analysis over the image by using SURF and SIFT algorithm and hence concluded that,

- Both the algorithms are effective for rotation change, noise, light and other integrated point of concerns.
- The synthesis analysis says that SURF algorithm has efficiency than SIFT algorithm.
- For faster, accurate and robust match SURF algorithm is preferable.

The paper is structured as follows, the first section gives a brief introduction of image forgery and its related works, The second section gives a brief review of literature in the field of image forgery, The third section explains the implementation of the proposed work through a general system architecture. The fourth section shows the simulation results and the results evaluation with respect to proposed system. The last section gives a brief conclusion of the overall proposed system.

2.Literature Review

Author Math et al. [1] have discussed the different kinds of digital forgeries and also the existing challenges/issues in it. The author has mentioned that the advancement in the software trend, variety of capturing tools, processing tools, accessing tools and transmitting tools of digital information, which has made toughest task to identify the tampering by visually or by other processes. The latest research domain for the digital forgery has gained its popularity due to the existing problem complexity. The author's paper satisfactorily concluded the problems seriousness impacting for the future research.

The LU decomposition and cellular automata based forgery detection of gray scale image is illustrated by presenting the active algorithm in Far et al. [2]. Authors paper has mentioned that the detecting the image forgery is a still open challenge for research in image processing area. Since last few years, many of the authors have expanded their study to identify the image forgery according to the advancement image forgery techniques. The image forgery detection algorithms can be classified as two categories active and passive. The *active approach*: followed with the creation and embedding of invaluable data and will be considered as cipher key, which helps in protecting the real image against the forgery. The *passive approach* will be followed with the investigation of image features, compressions and correlations for forgery detection. The author has suggested some important aspects for future study. Similar study is explained in Nodeh [3] and has introduced the active approach based image forgery detection.

Musthafa et al. [4] surveyed the image forgeries and authentication techniques based on passive approaches. The author has expressed the existing issues of image forgery, where the advanced image manipulation tools are used by which the detection becomes very complicated. The existing research towards the forgery detection is reviewed and state of art suggests that the passive methods can be used for digital image authentication.

AL-Quershi et al. [5] have presented the passive approach to detect the copy move type of image forgery. Author has expressed that the passive approach can be used most in image forensics. In this copy move based image forgery is focused for the research, where the some part of the image will be copied and moved to another place of the same image. According to the active approach of water marking method was used to overcome the authenticity issue, but the problem with this approach is that it requires specially equipped camera or the human intervention. In order to overcome these kind of issues the research institutes and researchers are proposed the passive approach, which doesn't requires specially equipped camera or the human intervention. The authors study helps in understanding the copy move image forgery detections state of art, key points required to develop the proper detector are addressed along with the issues and solutions for those issue.

Alahmadi et al. [6] have addressed the local binary pattern and Discrete Cosine Transform (DCT) based passive approach for image copy move based forgery detection. The approach is implemented as follow.

- The discriminative features and chrominance features are extracted by the application of two dimensional Discrete Cosine Transform (2DDCT) in local binary pattern space.
- For detection purpose support vector machine (SVM) is implemented. The experiment for the detection was carried out which outcomes with the superior results with accuracy than the existing methods.

Hashima et al. [7] have presented the combined (SIFT and DyWT) algorithm method for detecting the copy paste based image forgery. These two algorithms are implemented for following purpose:

- Dyadic Wavelet Transform (DyWT): To decompose the image as Low-low, Low-High, high-low and high-high parts.
- Scale Invariant Feature Transform (SIFT): To extract the key features exist in Low-Low part of the image and identify the identity among these key features. The presented method was efficient in identification aspects.

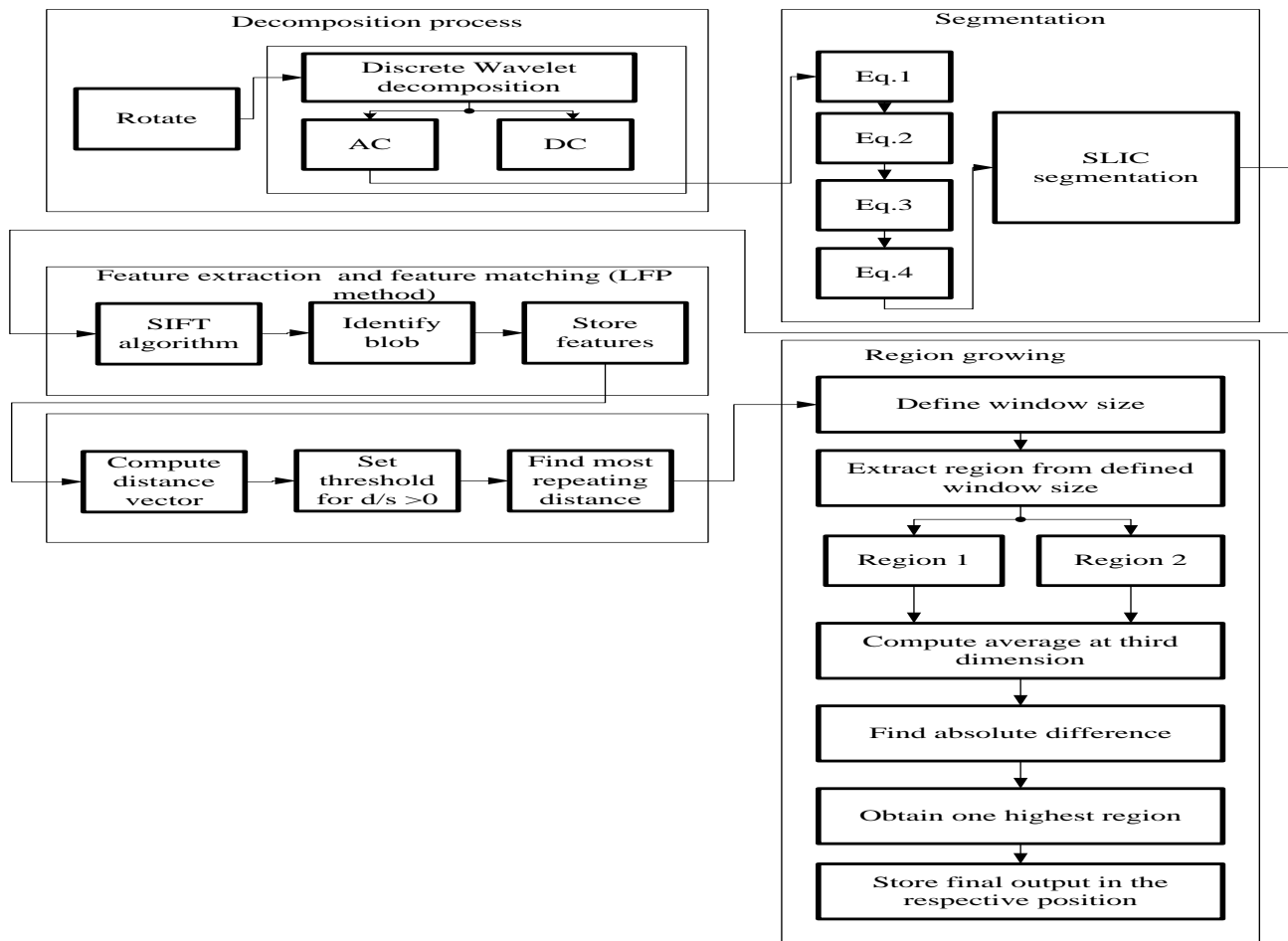
Maind et al. [8] have given the block representation method to identify the copy move based image forgery. The method is implemented by dividing the image into fixed block sized parts and subjecting the DCT (represents every block). The blocks transformed by DCT will be forwarded and represented as circle block and the image dimension is reduced by extracting the four features. Later these features will be sorted and matched with threshold value of the image block. The wrong blocks were eliminated to make efficient algorithm. The method was experimentally successfully helps in detecting the copy move based forgery and also helps in noise adding or blurring within less computational complexity.

Kasyap and Joshi [9] have given the wavelet decomposition based copy move image forgery detection. The approach has achieved the low computation time and 87% accurate detection scheme of detection. In Deshpande et al. [10] have discussed the image forgery detection techniques based on its pixel. The author has described the two kinds of image pixel based forgery detection scheme along with the copy move forgery detection (deals with only shifting of copied area). These techniques are compared with the fast copy move technique by analysis and suggested the future work flow.

3. Implementation

The general system architecture of the proposed system is shown in fig 1. The decomposition of the image data is performed by applying discrete wavelet transformation (DWT) using Haar wavelet as the basis function (mother wavelet). The operation of decomposition is performed post angle rotation of the image. The decomposition results in two coefficients which are the low frequency approximation coefficients and the high frequency detail coefficients. Using the low frequency and the high frequency components the size for the super pixels is computed.

Squared special distance is computed for the decomposed image coefficients. The difference between the squared color distances is then computed after which a combination of color distance and special distance is measured. The segmented image is finally obtained by combining edge distance and its weight along with total distance. Clustering based method is used in the SLIC algorithm which provides a tradeoff between color similarity and proximity with respect to compactness parameter



The SIFT algorithm is used in the process of feature extraction in the proposed system. This algorithm mainly consists of five important stages. In the first stage the feature detection is performed which is scale invariant (which is also known as dilation). The features are matched and respective labels are mentioned (which is used for the purpose of indexing). Consequently clustering based method is used for identification of feature and the Hough transformation is used for the purpose of voting. The model is verified by applying the least square method and finally the outlier is detected.

4.Simulation Results

The database considered in this project is a set of images of bmp and .png format. The images are of type double with intensity level representation of 2^8 bits range, i.e. the intensity levels in the image ranges from 0 to 255. The above database with the following attributes mentioned in table 1. The simulation results are shown in table 2,3,4 and 5.

Table 1: Database for the implementation of project

Sl.no	Input	Image format	Image size	Bytes	Class
1	Input1	.png	512x512x3	786432	uint8
2	Input2	.png	600x800	480000	uint8
3	Input3	.png	532x800	425600	uint8
4	Input4	.bmp	512x512x24	786486	uint8
5	Input5	.bmp	600x800x3	1440000	uint8
6	Input6	bmp	532x800x3	1276800	uint8

Table 2: Input image and ground truth







 <p>input 1</p>	 <p>input 2</p>	 <p>input 3</p>
 <p>ground truth image 1 (input 4)</p>	 <p>ground truth image 2(input 5)</p>	 <p>ground truth image 3 (input 6)</p>

Table 3: Feature extraction using SIFT algorithm

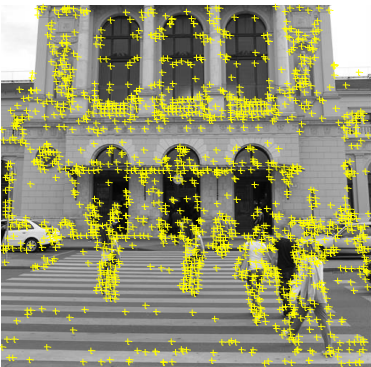
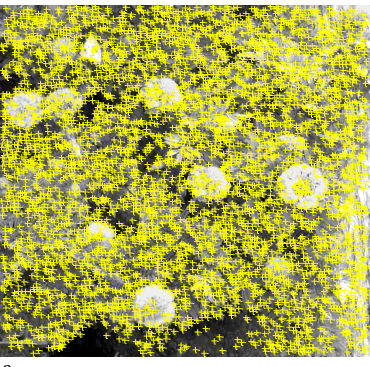
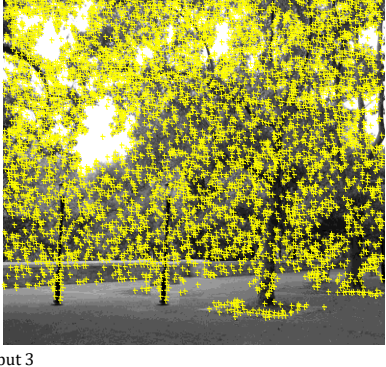
Feature extraction using SIFT algorithm		
 <p>input 1</p>	 <p>input 2</p>	 <p>input 3</p>

Table 4: Feature matching using LFP method

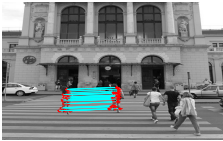

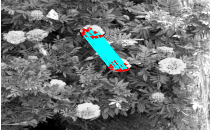

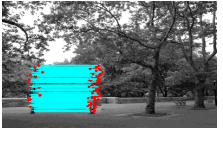







Feature matching using LFP method	
Feature detection	LFP method
	
	
	

Table 5: Detected forgery region

Detected forgery image	
<p style="text-align: center;">GT</p>  <p style="text-align: center;">input 1</p>	<p style="text-align: center;">Detected region</p> 
<p style="text-align: center;">GT</p>  <p style="text-align: center;">input 2</p>	<p style="text-align: center;">Detected region</p> 
<p style="text-align: center;">GT</p>  <p style="text-align: center;">input 3</p>	<p style="text-align: center;">Detected region</p> 

5.Result Analysis The evaluation performed with respect to image forgery detection is mentioned as follows,

1. **Precision:** The precision for the detection of forgery is considered as one of the factors in evaluation. The precision is defined as the ratio of true positive to sum of true positive and false positive. It is mathematically defined as shown in eq. 1,

$$precision = \frac{TP}{(TP+FP)} \dots\dots\dots (1)$$

Where, $TP \rightarrow$ true positive, given as

$$TP = \sum \sum \frac{bw1 \text{ AND } GT}{bwGt}$$

Where, $bw1 \rightarrow$ binary image (i.e. region growing)

$GT \rightarrow$ ground truth

$bwGT \rightarrow$ extracted area from ground truth

$FP \rightarrow$ False positive

$$FP = \sum \sum \frac{(bw1) \text{ AND } NOT(GT)}{NOT(bwGt)} \dots\dots\dots (2)$$

2. **Sensitivity:** Sensitivity is defined as the ratio of true positive to sum of true positive and false negative. It is mathematically defined as shown in eq.3,

$$sensitivity = \frac{TP}{(TP+FN)} \dots\dots\dots (3)$$

Where, FN → False negative, given as shown in eq.4

$$FN = \sum \sum \frac{NOT(bw1) AND GT}{bwGt} \dots\dots\dots (4)$$

3. **Specificity:** It is defined as the ratio of true negative to sum of true negative and false positive. It is mathematically represented as shown in eq.5,

$$specificity = \frac{TN}{(TN+FP)} \dots\dots\dots (5)$$

Where, TN → true negative, given as shown in eq.6

$$TN = \sum \sum \frac{NOT(bw1)AND NOT(GT)}{NOT(bwGT)} \dots\dots\dots (6)$$

4. **F1 score:** It is defined as twice the ratio of product of precision and sensitivity to sum of precision and sensitivity. It is mathematically defined as shown in eq.7,

$$F1 = 2 \times \left(\frac{precision \times sensitivity}{precision + sensitivity} \right) \dots\dots (7)$$

The simulation results for the above evaluation is given as follows in table 6,

Table 6: Parametric evaluations with respect to forgery detection

Parameters	image 1	image 2	image 3
Elapsed time	33.82 s	74.02 s	277.70
total number of key points	1886	5810	6363
total matches	154	254	351
TP	0.8401	0.9453	0.8455
TN	0.9956	0.9989	0.9980
FP	0.0042	0.0010	0.0018
FN	0.1563	0.0517	0.1536
Precision	0.9949	0.9989	0.9978
Sensitivity	0.8430	0.9481	0.8461
Specificity	0.9957	0.9989	0.9978
F1 score	0.9127	0.9728	0.9157

6. Conclusion

In this project the copy-move forgery detection is considered which is the most common and significant type of forgery method. Post wavelet decomposition, a feature extraction is performed using SIFT algorithm and the feature matching is performed using LFP. The region growing is performed finally to obtain the region where the image is forged. The evaluations considered for the proposed system are precision, sensitivity, specificity and F1 score. Experimental results show that the proposed system had better efficiency and performance with respect to above evaluations.

References

- [1] Math, Shrishail, and R. C. Tripathi. "Digital Forgeries: Problems and Challenges." *International Journal of Computer Applications* 5.12 (2010): 9-12.
- [2] Far, Mohammad Amin Moghaddasi, Faezeh Rohani, and E. Brhravesh. "An Active Algorithm to Gray-scale Digital Image Forgery Detection based on Cellular Automata and LU Decomposition." *J Comput Sci Softw Dev* 1.001 (2015).
- [3] Nodeh, Maryam Pahlavan. "Active Image Forgery Detection: State of the Art and Possible Enhancements." *J. Elec. Commu. Eng. Resol* 1.1 (2016): 11-13.
- [4] Mushtaq, Saba, and Ajaz Hussain Mir. "Digital Image Forgeries and Passive Image Authentication Techniques: A Survey." *International Journal of Advanced Science and Technology* 73 (2014): 15-32.
- [5] Al-Qersh, Osama M., and Khoo Bee Ee. "Passive Detection of Copy-Move Forgery in Digital Images: State-of-the-art."
- [6] Amani Alahmadi, Muhammad Hussain^{1,a}, Hatim Aboalsamh, Ghulam Muhammad, George Bebis, Hassan Mathkour, "Passive Detection of Image Forgery using DCT and Local Binary Pattern".
- [7] Mohammad Farukh Hashmia, Vijay Anand^b, Avinas G. Keskar^c, "Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform, "AASRI Conference on Circuit and Signal Processing, pp.84-91, 2014.
- [8] Rohini.A.Maind, Alka Khade, D.K.Chitre, "Image Copy Move Forgery Detection using Block Representing Method ", *International Journal of Soft Computing and Engineering (IJSCE)* pp.2231-2307, Volume-4, Issue-2, May 2014.
- [9] Kashyap and S. D. Joshi, "Detection of copy-move forgery using wavelet decomposition," *Signal Processing and Communication (ICSC)*, 2013 International Conference on, Noida, 2013, pp. 396-400.
- [10] Deshpande, Pradyumna, and Prashasti Kanikar. "Pixel based digital image forgery detection techniques." *IJERA* 2.3 (2012): 539-43.
- [11] L. Tu and C. Dong, "Histogram equalization and image feature matching," *Image and Signal Processing (CISP)*, 2013 6th International Congress on, Hangzhou, 2013, pp. 443-447.
- [12] B. Sirisha and B. Sandhya, "Evaluation of Color Spaces for Feature Point Detection in Image Matching Application," *Advances in Computing and Communications (ICACC)*, 2013 Third International Conference on, Cochin, 2013, pp. 216-219.
- [13] X. Wang, D. Liu and L. Wang, "A Feature Point Matching Algorithm for Complex Background Image," *Big Data and Cloud Computing (BDCloud)*, 2015 IEEE Fifth International Conference on, Dalian, 2015, pp. 243-247.