



A Hybrid Approach Based on Fourier-Mellin Transform for Copy-Move Forgery Detection Using Sift

Diksha Sharma¹, Mahender Tyagi²

M.Tech Student, Dept. of ECE, L.R.College of Engineering and Technology, Solan, H.P, India¹

HOD, Dept. of ECE, L.R.College of Engineering and Technology, Solan, H.P, India²

ABSTRACT: Copy move forgery in which an object is copied from one place and pasted on another place within the same image has become most common in the field of image processing. Various Copy-move Image forgery detection schemes are used to solve these problems. In this paper, a hybrid scheme is used to detect the copy-move object or region of an image. This hybrid scheme is basically a combination of keypoint based method and block based method. The proposed algorithm is tested on a number of digital images. The experimental results prove the FMSIFT algorithm is a novel approach in its accuracy.

KEYWORDS: Image Forgery, copy-move, Segmentation, Fourier-Mellin transform (FMT).

I. INTRODUCTION

Rapid advancement in imaging technology has made it remarkably easy to and expedient to tamper digital images, even for the non-professionals. The traces of tampering are hard to recognize by the naked eyes. The simplest method of tampering is to copy one or two region(s) and past to other regions of the same image. This kind of forgery is usually called copy-move [2]. Copy-Move forgery is performed with the intention to make an object “disappear” from the image by covering it with a small block copied from another part of the same image. Because the copied part comes from the same image, noise components, Brightness, the color palette, and the other properties will be well matched with the rest of the image, therefore it is very difficult for a human eye to detect such forgery [3]. In order to solve the copy-move image forgery problem in digital images, a number of methods have been proposed. There are two types of approaches used in the detection of image forgery. First is block based methods i.e. Zernike moments, DCT, DWT, FMT etc and second is keypoint based methods i.e. SIFT. The first approach to the image forgery problem was proposed by Ryu and Kirtchner [4]. This approach is known for its superior insensitivity to image noise, their information content, and ability to provide robust image representations. “Discrete cosine transform”, was another approach to the copy-move image forgery detection problem suggested by Fridrich [5]. The quantized Discrete Cosine Transform (DCT) coefficients are used to describe the content of the square sub-blocks. A.C. Popescu proposed to extract the block features using Principle Component Analysis (PCA) [2].

In this paper, a fourier-mellin scale invariant feature transform (FMSIFT) algorithm is proposed to solve the image forgery detection problem of digital images by making use of the SIFT algorithm defined in [8]. In order to improve the implementation efficiency of the, a Bregmanized operator splitting algorithm is employed.

The rest of this paper is organized as follows. In Section II, the FMSIFT algorithm is formulated. The parameters description and experimental results are presented in Section III. Section IV is the conclusion.

II. RELATED WORK

In [1] authors had proposed a scheme to detect the copy-move forgery in an image mainly by extracting the key points for comparison. The main difference to the traditional methods is that the proposed scheme first segments the



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 3, March 2017

test image into semantically independent patches prior to key point 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, we find the suspicious pairs of patches that may contain copy-move forgery regions, and we roughly estimate an affine transform matrix. In the second stage, an EM-based algorithm is designed to refine the estimated matrix and to confirm the existence of copy-move forgery. In [3] authors had introduced an improved algorithm by applying DWT into an image to reduce the dimension representation. The feature vectors will be extracted from the small overlapping blocks of the compressed image and sorted lexicographically to find the duplicated blocks. The detection was carried out on the lowest level image representation and also proved best performance on small size copy move forgery, detected the multiple Copy-Move forgery with lower computational complexity. In [4] authors had proposed a forensic technique to localize duplicated image regions based on Zernike moments of small image blocks. They exploit rotation invariance properties to reliably unveil duplicated regions after arbitrary rotations. As to the limitations, they note that detectors based on Zernike moments are inherently incapable of localizing duplicated regions that underwent strong affine transformations other than rotation. In [5] authors had investigated the problem of detecting the copy-move forgery and describe an efficient and reliable detection method. The method may successfully detect the forged part even when the copied area is enhanced/ retouched to merge it with the background and when the forged image is saved in a lossy format, such as JPEG. The performance of their method is demonstrated on several forged images. In [12] authors had described a specific type of forgery which is Copy-move forgery investigated and an efficient detection method proposed based on Fourier transform. In this paper, we have considered the problem of copy-move image forgery detection. Our emphasis was on detecting and extracting duplicated regions with higher accuracy and robustness.

III. OVERVIEW OF THE PROPOSED FMSIFT SYSTEM

In order to obtain convincing detection results, the proposed method takes the advantage of the existing scale invariant feature transform and fourier-mellin transform methods.

From these methods we can infer that image forgery detection technique based on block matching generally include the following main steps:

- Dividing the image into overlapping blocks
- Extracting features from each block
- Searching the similar block pairs
- Deciding the duplicated regions.

The first step of this technique is dividing the image into overlapping blocks. The second step is a feature extraction process. The biggest challenge of this technique is to determine the features, which would get the same or very similar values for duplicated blocks, even under modifications. Ref. [9] chose quantized DCT coefficients as the block features; in [10] they chose PCA, SVD, FMT coefficients as the block features respectively. These features, except FMT coefficients, are only robust to signal process, not robust to geometrical transformation such as rotation and scaling. The third step is to find the similar block pairs by feature matching in a reasonable time. In order to save computing time, the references mentioned above used a common match based on lexicographically sorting [8].

SIFT method is used to detect region duplication based on local image statistical features. This is keypoints based method and used to detect forgery in non-flat areas. SIFT descriptors of an image are invariant to changes in illumination, rotation, scaling etc. First the SIFT descriptors of the image is extracted, and descriptors are then matched between each other to seek for any possible forgery in images [11].

This paper chooses Scale Invariant Feature Transform (SIFT) feature to be as the matching feature. SIFT feature is a type of local invariant feature, which is propose by Lowe et al. and proved to be invariant to image scale and rotation, also robust to a substantial range of affine distortion, change in 3D viewpoint, compression, addition of noise, and change in illumination[12].



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 3, March 2017

A. Image Segmentation:

Image segmentation is typically used to locate objects and boundaries in images. More precisely, image segmentation is the process of assigning a label to every pixel in an image such that pixels with the same label share certain characteristics.

Here we use watershed algorithm for segmentation. The watershed algorithm can segment image into several homogeneous regions which have the same or similar gray levels. To perform meaningful segmentation of image, regions of different gray levels should be merged if the regions are from the same object. Watershed algorithm is a widely used super pixel-based image segmentation method. It has three properties: First, each super pixel's boundary adheres well to image boundaries. Second, the algorithm is simple and the processing speed fast. Third, each super pixel in smooth region is regular lattice. Watershed algorithm is executed on gradient of the image. This method includes two main steps:

- Calculated gradient image values.
- Using watershed algorithm step [6].

B. Scale Invariant Feature Transform (SIFT):

SIFT is a method to extract distinctive invariant features from images. It includes key point detector and local feature descriptor. There are several steps to compute these features as follows:

- Select candidates for features by searching peaks in the scale space from difference-of-Gaussian function.
- locate key points using measures of their stability,
- Assign orientations based on local image gradient directions and
- Calculate the local key point descriptors based on the set of surrounding image gradients [4].

C. Fourier-Mellin Transform:

The properties of Fourier-Mellin Transform are translation, scaling, and rotation invariance. It is a block based scheme. Fourier space image registration methods provide a way to recover all rigid transformation parameters, i.e. rotation, translation and scale. They differ from other registration methods in that they search for the optimal match in the frequency domain. These methods make use of the Fourier Shift Theorem and the Fourier Rotation Theorem to provide invariance to rotation, translation and scale. It is possible to compute the Fourier Transform of an image efficiently by using the Fast Fourier Transform (FFT).

D. FMSIFT:

In FMSIFT scheme we have combine two techniques. One of the schemes is block based and other one is keypoint based scheme. In this first step is to input the image which can be tampered or original. In the second step we have to calculate gradient of the image. We have used watershed algorithm which work only on gradient of the image. After this we apply watershed algorithm for segmentation of image in segments. Then SI-CMFD is applied which is used to extract the keypoints of the image. Due to this we can find out some areas in which same keypoints are obtained and we can find out that this area is copied and moved within the same image. But in this dataset SI-CMFD does not work for all images. So in this paper with SIFT we have used FMT which is block based scheme. The images on which SIFT has not detected any forged area a combination of SIFT and FMT that is FMSIFT can detect the copy-move region.

IV. SIMULATION RESULTS

In this section, various experiments have been presented to demonstrate the efficiency of the FMSIFT model. In order to verify the performance of the FMSIFT-model, different image quality evaluation methods are determined which work for various kinds of image degradations. Furthermore they are compared with the existing copy-move image forgery algorithm presented in [1].

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017



(a) Tampered Image (b) Original Image

Fig.1: A digital image as an input to the algorithm

Fig.1 (a) shows a tampered image in which a tree is copied and placed in another location inside the image and (b) shows an original image on which forgery has to be detected.



(a) Gradient of the tampered image



(b) Gradient of the Original image

Fig. 2: Image of calculating gradient of the image

Fig.2 (a) shows the gradient calculated on tampered image and Fig.2 (b) shows the gradient calculated on an original image.



(a) Tampered image (b) Original Image

Fig. 3: Image Segmented by watershed algorithm

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

In Fig.3 (a), the tampered image segmented by using watershed algorithm and Fig.3 (b) shows the original image segmented by watershed algorithm.



(a) Tampered Image (b) Original Image

Fig.4: Forgery detected by SI-CMFD

Fig.4 (a) shows the tampered image and Fig.4 (b) shows the original images on which existing SI-CMFD algorithm is applied to detect forgery.



(a) Tampered Image (b) Original Image

Fig.5: Forgery detected by FMSIFT Algorithm

In Fig.5 (a), the forgery has been detected by proposed FMSIFT method and Fig.5 (b) shows the forgery detected on an original images by proposed FMSIFT.

Parameters	SI-CMFD	FMSIFT
True Positive	0.70	0.78
False Positive	0.30	0.21
True Negative	0.73	0.81
False Negative	0.26	0.18
Precision	0.70	0.78
Recall	0.73	0.81
F-Measure	0.71	0.79
TNR	0.70	0.79
FPR	0.29	0.21
FNR	0.25	0.18
NRM	0.27	0.19
Accuracy	71.6%	80%

Table 1: Values of various parameter calculated for the all dataset images

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

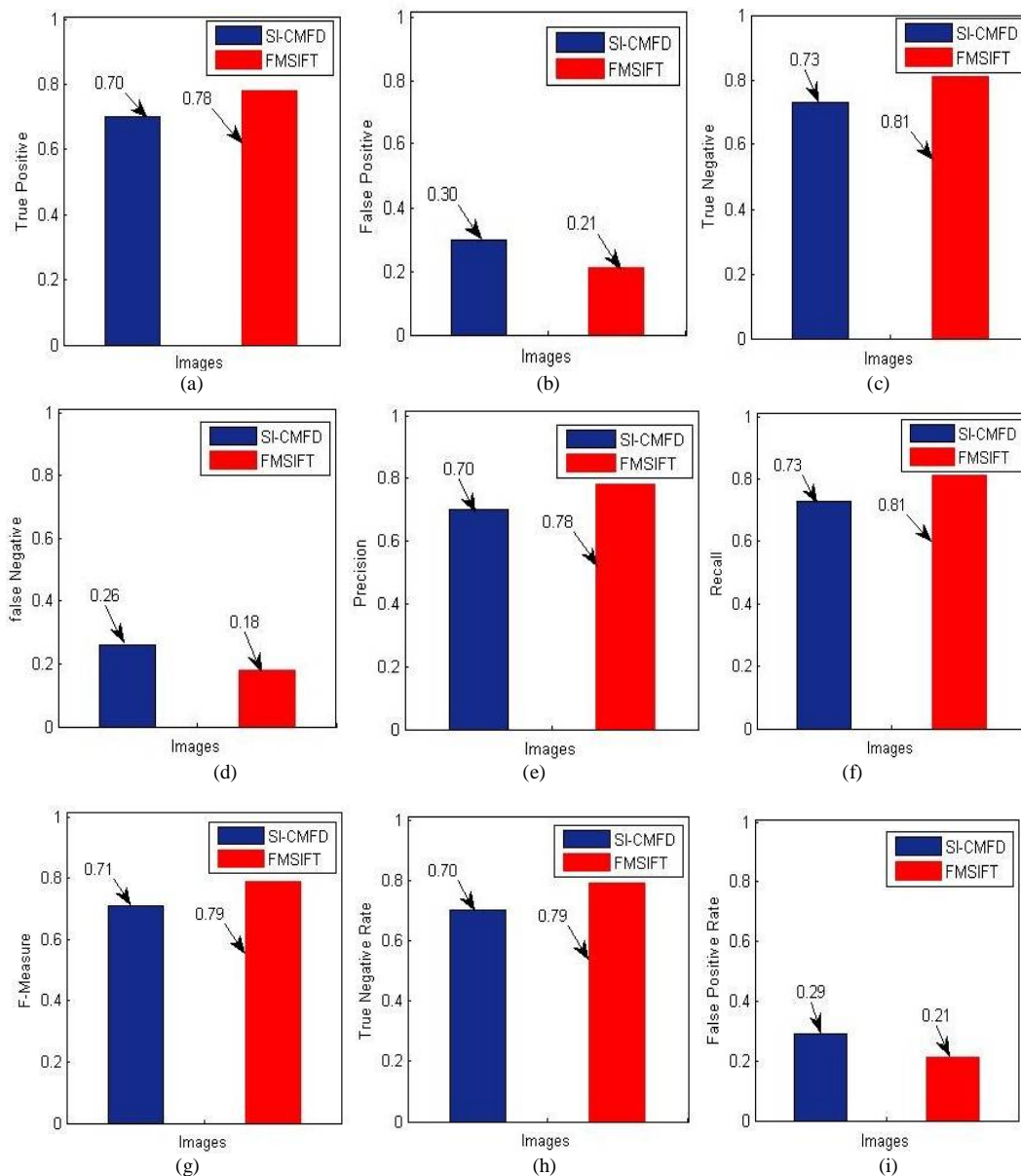
Website: www.ijirccce.com

Vol. 5, Issue 3, March 2017

Table 1 shows the values of TP, FP, TN, FN, Precision, Recall, F-Measure, TNR, FPR, FNR, NRM and Accuracy calculated for the sixty tampered and sixty original images. The conclusion from this table is that the FMSIFT algorithm is 11.73% more accurate than SI-CMFD algorithm.

Here, in the database we have taken total 120 images. Out of these 120 images, 60 images are original and other 60 are tampered. Simulation has been done on all of these images and twelve parameters has been calculated which proved that proposed method is more efficient and accurate than the existing one.

GRAPHICAL REPRESENTATION OF PARAMTERS CALCULATED FOR THE ALL DATASET IMAGES:



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 3, March 2017

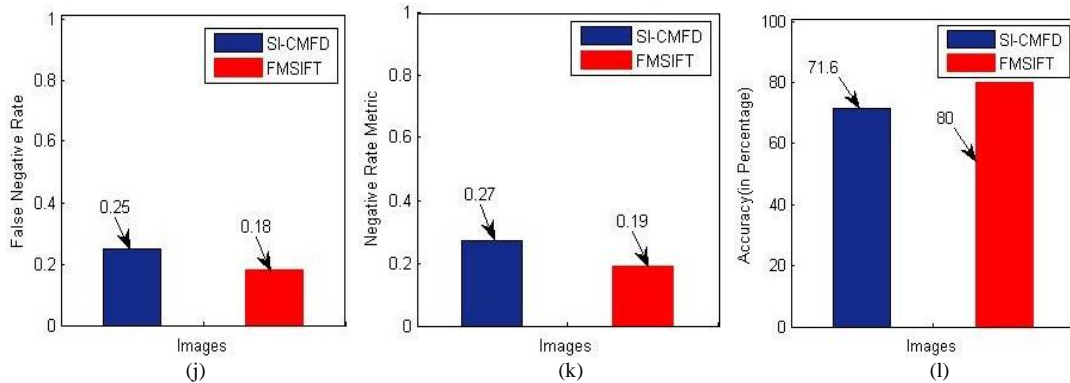


Fig.6: Graphical representation of TP, FP, TN, FN, Precision, Recall, F-Measure, TNR, FPR, FNR, NRM and Accuracy values.

Fig.6 shows the graphical representation of the different parameters calculated for the sixty tampered and sixty original images. The graph of TP, FP, TN, FN, Precision, Recall, F-Measure, TNR, FPR, FNR, NRM and Accuracy is shown in Fig.6 (a), (b), (c), (d), (e), (f), (g), (h), (i), (j), (k) and (l) respectively. So from the simulation studies it is concluded that proposed FMSIFT algorithm is better than existing SI-CMFD algorithm.

V. CONCLUSION AND FUTURE WORK

In this paper, Fourier-Mellin Scale Invariant Feature Transform (FMSIFT) model is presented to deal with the fundamental problems of image forgery in which an object is copied from one place and pasted in another place within the same image. Both the SI-CMFD and FMSIFT models are tested over a dataset of 120 images in order to verify their performance. In each image the image forgery is detected by FMSIFT and SI-CMFD approach. On the basis of this detection various parameters are calculated such as True Positive, False Positive, True Negative, Precision, Recall, F-Measure, TNR, FPR, FNR, NRM and accuracy. In all the six experiments, the value of all the parameters calculated by FMSIFT model are better than SI-CMFD. The accuracy of FMSIFT model is 80% whereas the accuracy of SI-CMFD is 71.6%. So the FMSIFT method is 11.4% more accurate than SI-CMFD method. Hence from the simulated data experiments, it is concluded that the results using FMSIFT algorithm are better than the existing copy-move forgery detection algorithm. In the near future, the present work can be extended or will be helpful in video copy-move forgery detection. Furthermore, the simulated work can be planned in order to improve the speed efficiency of the forgery techniques. Also, more parameters such as SSIM (Structural Similarity Index), MPM (Misclassification Penalty Metric) etc. can also be added for the better decision-making for the detection of copy-move forgery in digital images.

REFERENCES

1. J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based Image copy-move forgery detection Scheme", IEEE transactions on information forensics and security, vol. 10, issue 3, pp. 507-518, 2015.
2. L. Li, S. Li, H. Zhu, "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.
3. P. Yadav and Y. Rathore, "Detection of Cop-Move Forgery of Images using Discrete Wavelet Transform", International Journal on Computer Science and Engineering, vol. 4, no. 04, pp. 565-570, April 2012.
4. S-J. Ryu, M. Kirchner, M-J. Lee, and H-K Lee, "Rotation Invariant Localization of propagation Duplicated Image Regions Based on Zernike Moments", IEEE Transactions On Information Forensics And Security, Vol. 8, No. 8, pp. 1355-1369, Aug. 2013.
5. A. J. Fridrich, B. D. Soukal, and A. J. Luk, "Detection of copy-move forgery in digital images", in Proc. Digital Forensic Research Workshop, 2003.
6. N. Salman, "Image Segmentation Based on Watershed and Edge Detection Techniques", The International Arab Journal of Information Technology, vol. 3, no. 2, pp.104-110, April 2006.
7. J. Zhang, Z. Feng and Y. Su, "A New Approach for Detecting Copy-Move Forgery in Digital Images", 11th IEEE Singapore Int. Conference on Communication Systems, pp. 362-366, 2008.
8. Li Jing and Chao Shao, "Image Copy-Move Forgery Detection Based on Local Invariant Features", Journal of Multimedia, vol. 7, no. 1, pp. 90-97, Feb. 2012.
9. A. J. Fridrich, B. D. Soukal, and A. J. Luk, "Detection of copy-move forgery in digital images," in Proc. Digital Forensic Research Workshop, 2003.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

10. S. Bayram, H.T. Sencar and N. Memon, "An Efficient and Robust Method for Detecting Copy-Move Forgery", in proc. IEEE int. conference on Acoustics, Speed and Signal Processing, pp. 1053-1056, 2009.
11. X. Pan, S. Lyu, "Region Duplication Detection Using Image Feature Matching", IEEE Transactions on Information Forensics and Security, Vol. 5, No. 4, pp. 857-867, Dec. 2010.
12. S. A.Thajeel, G. Bin Sulong, "State of the Art of Copy Move Forgery Detection Techniques: A Review", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 6, No 2, pp. 174-183, Nov. 2013.

BIOGRAPHY

Diksha Sharma is a Research Scholar in the Electronics and Communication Department, LR College of Engineering and technology, Solan (HP). She received her B. Tech degree in 2012 from PTU, Jalandhar. Her research interest areas are Digital image processing and wireless communication.