IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. XII (Mar-Apr. 2014), PP 96-104
www.iosrjournals.org

Passive Image Forensic Method to detect Copy Move Forgery in Digital Images

Salma Amtullah, Dr. Ajay Koul
School of Computer Science and EngineeringShri Mata Vaishno Devi University Katra, India.
School of Computer Science and EngineeringShri Mata Vaishno Devi University Katra, India.

Abstract: *Tampering in digital images has become very easy due to the availability of advanced image editing softwares to the users. Images are being tampered in a very efficient manner without leaving any visual clue. As a consequence, the content of digital images cannot be taken as for granted. There are various types of image tampering techniques. One of the most common tampering techniques is copy-move forgery. In copy-move forgery one part of an image is copied and pasted in another part of the same image. In this paper, the passive image forensic method is presented to detect copy move forgery in digital images. The proposed method is based on SURF (Speed Up Robust Features) algorithm. In this method the features are extracted and their descriptors are obtained by SURF algorithm and the Nearest Neighbor approach is used for feature matching to identify the copy move forgery in digital images. This detection method is found to be rotation and scale invariant and is robust enough to noise, jpeg compression and blurring. Multiple copy move forgery is also detected by this method.*

Keywords: *Digital Image Forensics, Copy move forgery, SURF, Nearest Neighbor Ratio.*

I. Introduction

With the tremendous use of digital images and the availability of powerful image editing softwares it becomes very important to verify the content of digital images before relying on them. In today's digital world, digital images are one of the principal means of communication. Every day millions and millions of images are uploaded on social networking sites. With the advancement and easy availability of image editing tools like Photoshop, GIMP, it becomes very easy to manipulate or tamper the digital images and create forgeries without leaving any visual clues, and such manipulations may change the whole semantics of the image. The tampered image may totally convey different information than that of the original image. Therefore, digital images have lost their trust and it has become necessary to check the originality of content of the images when they are used in some critical situation like criminal investigation. Digital images found their applications in various fields like media, journalism and sometimes they are used as evidence in courts. Hence it becomes very important to verify that whether the image is real or fake. So, the Digital Image Forensics emerged as research field that aims to detect the forgery in digital images.

The main goal of Digital Image Forensics is to check the authenticity and integrity of digital images. Digital Image Forensics is of two types: Active and Passive. Active image forensics requires the pre embedded information such as watermark or digital signature in digital images for tampering detection. While the passive image forensics detects the tampering without any pre embedding of information. Passive approach does not require any prior explicit information about the images. The main drawback of active image forensics is that it requires pre embedded information in digital images, which is not always available, because most of the cameras available in the market are not equipped with the facility to embed the watermark or digital signature in images that can be used later in forensic analysis. Passive image forensics overcome this drawback and is widely used for forgery detection in digital images as most of the images available today are without any watermark or digital signature.

In this paper the passive image forensic method is presented to detect one of the important tampering techniques known as Copy-Move forgery in which a part of an image is copied and pasted on another part of the same image. Copy-Move forgery is performed in order to hide certain details or to duplicate objects within an image. Since the forgery is performed within a single image, therefore, the tampered region has almost same properties as that of the original image which makes it very difficult to identify by the human eye. Fig.1 shows the example of copy-move forgery which took place in July 2008 in Iran. The tampered image was published in various international newspapers showing four missiles but only three of them were real [12].

(a) (b)

Figure 1: Example of copy move forgery. (a) Original Image. (b) Tampered image after applying copy move forgery. The tampered image shown in (b) has been published by Iran's state media showing their missile tests in July 2008.[12]

It is very common practice in copy move forgery that certain postprocessing operations like, rotation, scaling, adding noise, jpeg compression and blurring are performed on the forged part of the image in order to hide the tampering traces and make the detection difficult. Hence the copy move forgery detection method should be robust enough to such postprocessing operations.

The rest of the paper is organized as follows: Section II presents literature survey related to copy move forgery detection. Overview of SURF algorithm is presented in section III. The proposed methodology is presented in section IV. In section V experimental results are given and finally the conclusion is given in section VI.

II. Literature Survey

At different times researchers use different approaches in image forensics to detect the copy -move forgery in digital images. Copy move forgery detection methods using passive approach for detection can be divided into two groups: Block based methods [3], [4], [5], [10] and keypoint based methods [6], [7], [8].The very first passive method for detection of copy move forgery is presented by Fridrich et al [3] that uses Discrete Cosine Transform (DCT) for the detection of copy move forgery. In this method the image is divided into overlapping blocks and then DCT is performed on each block. These DCT coefficients of each block are quantized. Each DCT quantized block is stored as a row in a matrix and then the lexicographical sorting is used for matching purpose to identify the tampered regions. Using this approach the flat and uniform regions lead to false matches. In [10] Popescu and Farid apply PCA on overlapping image blocks to yield a reduced dimension representation. In this approach Copy move forged regions are also detected by lexicographical sorting of the image blocks. This method is robust to minor variations in image due to additive noise and lossy compression [10]. Another method presented in [5] applies Fourier Mellin Transform on each block. This method handles minor variations in rotation and scaling. In [4] the authors use the Discrete Wavelet Transform to compress the image, then the compressed image is divided into overlapping blocks and phase correlation is used as similarity criterion to identify the duplicate blocks in an image. This method shows robustness towards noise and jpeg compression but fails to be rotation and scale invariant. The block based methods are sensitive to rotation and scaling and they are computationally very complex. To overcome the limitations of block based methods the researchers use keypoint based methods: SIFT and SURF for detection of copy move forgery. Amerini et al.[6] proposes a method that is based on Scale Invariant Feature Transform (SIFT). In this method the SIFT features are extracted from the image which are then matched with each other to locate the forged duplicate regions in an image. The drawback of this method is the high dimensionality of the SIFT descriptors. Another method is presented by Xu Bo et al. in [7] that use Speed Up Robust Features (SURF) for copy move forgery detection. In [7] multiple copy move forgery detection has not been addressed.

In this paper the passive image forensic method for detection of copy move forgery is presented which is based on SURF. In this method the keypoints are extracted and their descriptors are computed using SURF algorithm. The keypoint descriptors are then matched by using Nearest Neighbor approach to detect the copy move forged regions in an image. This method is robust enough for various manipulations like adding noise,

jpeg compression, blurring and is also scale and rotation invariant. This method also detects multiple copy move forgeries also known as multiple cloning.

III. Surf Overview

Speed Up Robust Features (SURF) is rotation and scale invariant keypoint detector and descriptor. It is computationally very fast. This is achieved by the use of integral images. In SURF the keypoint detection uses basic Hessian-matrix approximation. The keypoint descriptors are formed by using Haar wavelet responses in the neighborhood of the specified keypoint [11].

A. Interest Point Detection.

For interest point detection SURF uses a basic Hessian-matrix and the integral images which reduce the computation time. Hessian matrix at any point can be calculated as: consider a point $X = (x, y)$ in an image I, the Hessian matrix $H(X, \sigma)$ in X at scale σ is defined as follows:

$$H(X,\sigma) = \begin{bmatrix} L_{xx}(X,\sigma) & L_{xy}(X,\sigma) \\ L_{xy}(X,\sigma) & L_{yy}(X,\sigma) \end{bmatrix} \quad (1)$$

In the above matrix,$L_{xx}(X,\sigma)$ denotes the convolution of the Gaussian second order derivative $\frac{\partial^2}{\partial x^2} g(\sigma)$ with the image I at point X, similarly for $L_{xy}(X,\sigma)$and $L_{yy}(X,\sigma)$.

SURF approximates Gaussian second order derivatives with box filters. With these box filters image convolutions can be computed speedily by using integral images. The approximation of the second order Gaussian derivatives in x, y and xy direction is denoted as $D_{xx,}$ D_{yy} and D_{xy} respectively. By choosing the weights of the box filters adequately, an approximation for the Hessian determinant is calculated by (2).

$$|H| = D_{xx}D_{yy} - (0.9D_{xy})^2 \quad (2)$$

For localization of interest points in an image and over scales, non-maximum suppression is applied in a 3 × 3 × 3 neighborhood [11]. The points which are associated with the maxima of the determinant of Hessian matrix are considered as interest points.

B. Interest point description

For interest point description SURF first constructs a circular region around the detected interest points to assign them a unique orientation. This step is used to achieve invariance to rotation. Then for the extraction of the descriptor, a square region is constructed around the interest point. The square region centered on the interest point is divided into 4 × 4 sub-regions. For each sub-region Haar wavelet responses at regularly spaced sample points are computed. Then the wavelet responses in horizontal d_x and vertical d_y directions are summed up over each sub-region and form a set of entries in the feature vector. To bring the information about the polarity of the intensity changes, SURF also extract the sum of the absolute values of the responses,$|d_x|$and$|d_y|$. Hence each sub-region has a descriptor vector $\boldsymbol{V}$ given in (3).

$$\boldsymbol{V} = (\sum d_x, \sum d_y, \sum |d_x|, \sum |d_y|) \quad (3)$$

Concatenating this for all 4×4 sub-regions, a descriptor of length 64 is obtained [11].

IV. Proposed Method

The proposed method is to detect the copy-move forgery without using embedding of any explicit information in digital images. The method is based on SURF algorithm. In this method the input image is taken and if it is not a gray scale image then convert it into gray scale before further processing. In this method the feature extraction and description is performed by using SURF algorithm and then these features are matched

with each other in order to locate the copy-move forgery in digital images. The work flow of the proposed method is shown in Fig2.

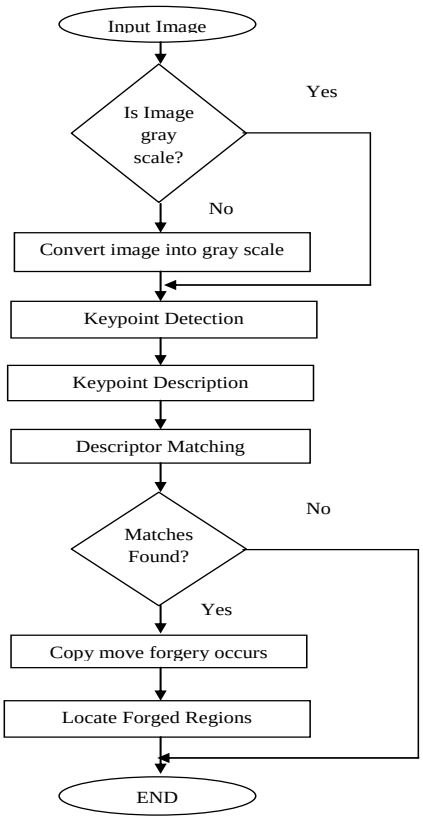


Figure 2: Work flow of proposed system

A. Keypoint Detection and Description

In this method the keypoints are detected and described by SURF algorithm as mentioned in section III. For the sake of clarity, in this step, given an input image a set of keypoints **P**={p_1, p_2,….,p_n} are detected and their corresponding descriptors{d_1,d_2,…,d_n} are computed which are further processed.

B. *Descriptor Matching*

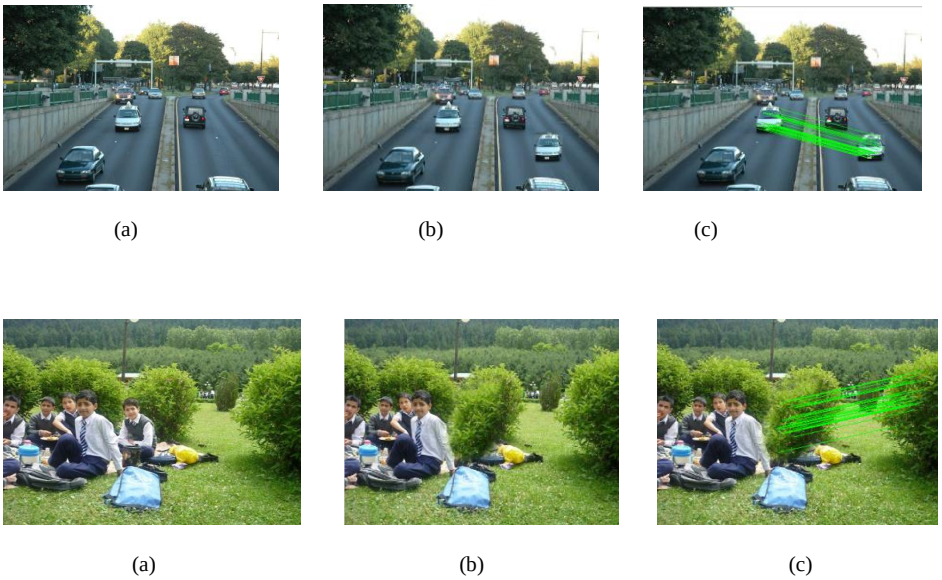
In this step the keypoint descriptors are matched with each other to identify the matching keypoints. The best match of the keypoint can be found by identifying its nearest neighbor i.e. the keypoint with minimum Euclidian distance. The matching algorithm used in this method is Nearest Neighbor Ratio. For detection of copy-move forgery in digital images the matching procedure based on Nearest Neighbor Ratio is described as follows:

1) Take the set of keypoint descriptors obtained in keypoint description step.
2) Calculate the Euclidian distance of a keypoint descriptor to all other descriptors and obtain a distance vector. The distance vector contains distances of the test descriptor to all other descriptors.
3) Sort the distance vector in ascending order of distances.
4) Calculate the ratio of nearest neighbor to the second nearest neighbor.
5) If the ratio obtained in step 4 is less than a predefined threshold T, then the keypoint is matched to its nearest neighbor, otherwise it is discarded. The threshold T used in this paper is 0.5.
6) Repeat step 2 to step 5 for all descriptors.
7) Retain the matched keypoints and display them on the image to locate the copy move forged regions.

V. Experimental Results

The proposed method is evaluated on a dataset MICC-200 [13] and some personal collected images. The images are tampered by using image editing softwares Photoshop and GIMP. Experiments are performed on various images, starting from the basic case of plain copy-move forgery in which no postprocessing operation is applied on the forged part. But it is very common to apply postprocessing operations like adding noise, blurring, jpeg compression, scaling, rotation, and combined transformations on the forged region of an image in order to make the detection harder. To check the robustness of the proposed method experiments are also performed on the images in which the different operations mentioned above are applied on the forged region of an image. The method is also evaluated to detect the multiple copy move forgeries.

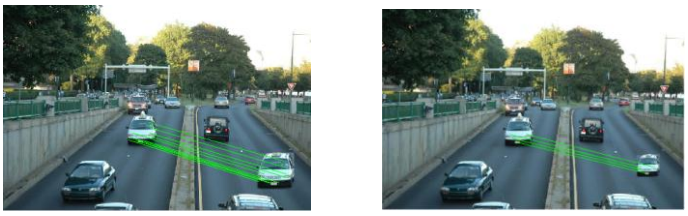
Fig. 3 shows the results of the method for detection of plain copy move forgery. The detection results show that the proposed method identifies the forged regions with high accuracy. Scaling and rotation are the most common transformations which are applied to the forged part in order to hide the trace of forgery. Fig. 4 and Fig. 5 show the detection results for scaling and rotation respectively.



(a) (b) (c)

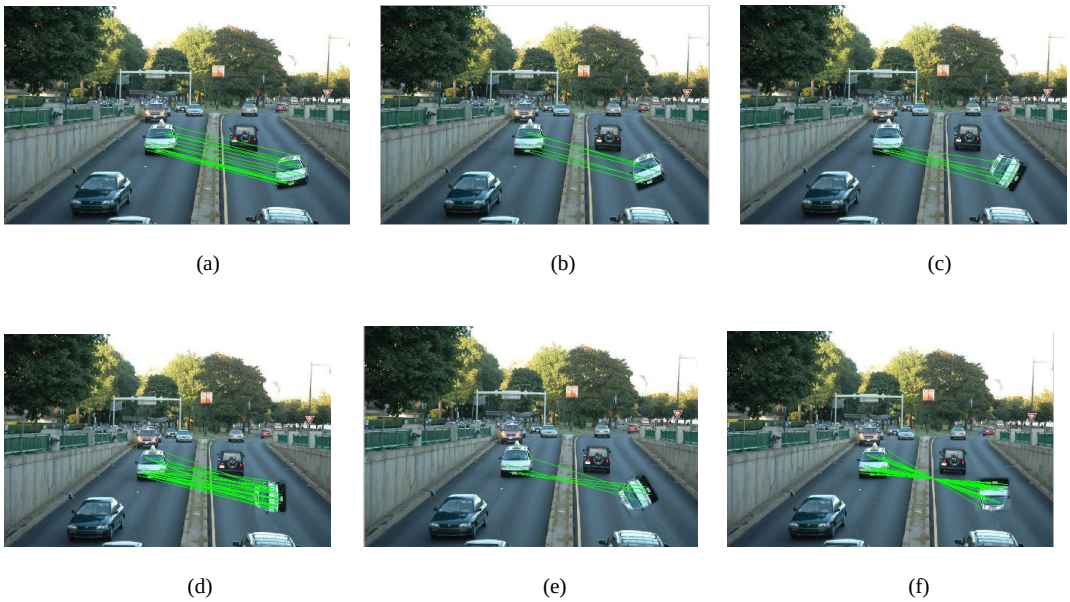
(a) (b) (c)

Figure 3: Plain copy move forgery detection. (a) Original images. (b) Tampered images. (c) Detection Results



(a) (b)

Figure 4: Detection results for scaling. (a) Detection results for scale up (b) Detection results for scale down.



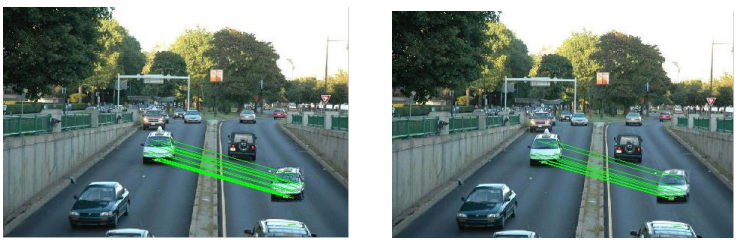
(a) (b) (c)

(d) (e) (f)

Figure 5: Detection Results for various rotations applied on tampered part. (a) 10^0 rotation (b) 20^0 rotation (c) 60^0 rotation (d) 90^0 rotation (e) 120^0 rotation (f) 180^0 rotation

The experimental results in Fig.5 show the rotation invariance of the proposed method. When the forged part is rotated with some angle the number of matches decreases but still the method gives the significant numbers of matches by which we can identify the copy move forged parts in the tampered image. As in Fig.5 (a)-(f) different rotations are applied on the forged part of an image and the method accurately locates the copy move forged parts in them. The results show that the method can also handle higher degrees of rotation.

Subsequent experiments are performed to check the robustness of the method in case of adding noise, blur and combined operations to the forged part of the image. The results of such experiments are shown in Fig.6 and Fig.7.



(a) (b)

Figure 6: Detection results of copy move forgery with noise and blur. (a) Detection result for adding Gaussian noise (b) Detection result for Gaussian blur.

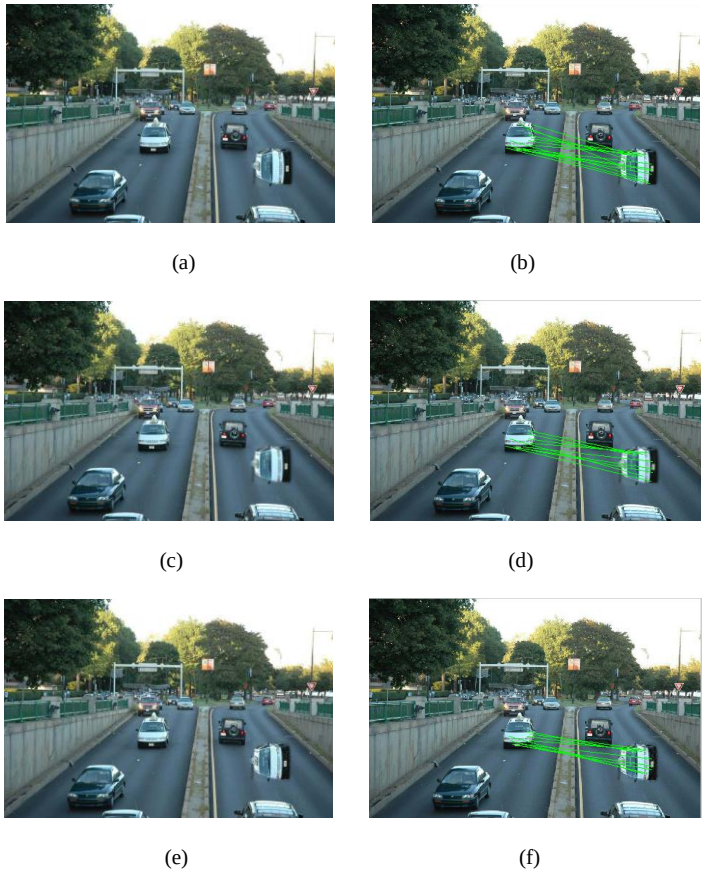
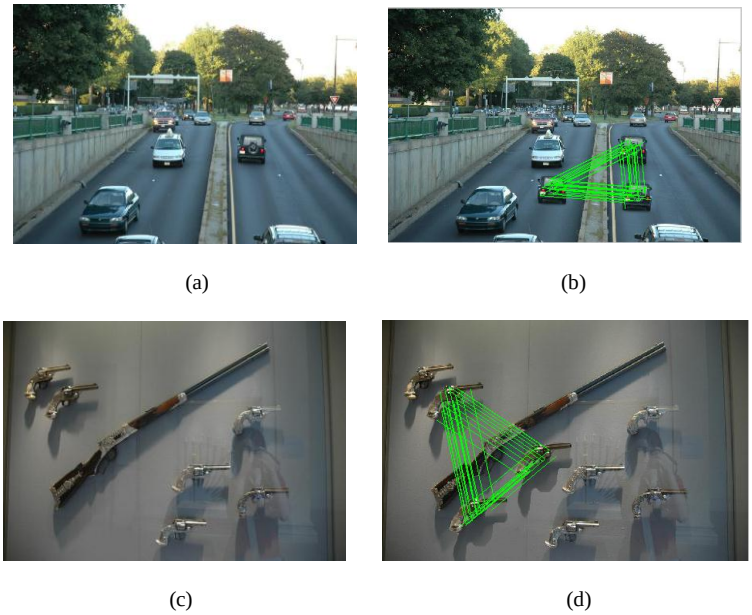


Figure 7: Detection results of copy move forgery with combined transformations. (a) Copy move forgery with scaling and rotation.(b) Detection results of (a). (c) Copy move forgery with scaling, rotation and blurring. (d) Detection results of (c). (e) Copy move forgery with scaling, rotation and Noise. (f) Detection results of (e).

It is very common in copy move forgery that same part of image is copied again and again in the image which results in multiple cloning. To handle multiple cloning, step 5 of the matching algorithm is iterated between the distance values v_i/v_{i+1} in a distance vector of a descriptor until the ratio is >T. If at certain valve v_j the stopping condition is reached. Then the keypoints which correspond to the distances up to v_j are considered as a match for the test keypoint. Fig. 8 shows examples of images with multiple cloning and their detection results using the proposed method.

The experimental results show that the proposed method is highly robust to postprocessing operations such as adding noise, blurring, jpeg compression, scaling and rotation, which are applied on the forged part of an image. The method detects the copy move forgery with high accuracy even when the tampered regions undergo certain severe manipulations.



(a) (b)

(c) (d)

Figure 8: Detection Results of multiple copy move forgeries. (a) and (c) are original images. (b) and (d) contains multiple copy move forgery with their detection results.

To measure the performance of the method two metrics True Positive Rate (TPR) and False Positive Rate (FPR) were used.

$$\text{TPR} = \frac{\text{Number of forged images detected as forged}}{\text{Total number of forged images}}$$

$$\text{FPR} = \frac{\text{Number of original images detected as forged}}{\text{Total number of original images}}$$

The TPR of the method is 100% and that of FPR is 5%. These values show that the proposed method performs well having low FPR while maintaining the high True Positive Rate.

VI. Conclusion

In this paper passive image forensic method to detect copy move forgery is presented which uses SURF algorithm for feature detection and description and Nearest Neighbor Ratio is used for matching purpose in order to locate the copy move forgery in digital images. The proposed method not only detects the simple one to one copy move forgery but also performs well when certain postprocessing operations such as adding noise, jpeg compression, blurring, rotation, scaling or any combined operations which are applied to make the detection difficult. Experimental results show clearly that the method is highly robust to all such operations. This method also detects multiple copy move forgeries with high accuracy. The future work will be concerned with the improvement of the method to detect the copy move forgery when the copied part is of highly uniform texture where the keypoints are not detected by SURF algorithm.

References

[1] J. Redi, W. Taktak, and J.-L. Dugelay, "Digital image forensics: A booklet for beginners," *Multimedia Tools Applicat.*, vol. 51, no. 1, pp. 133–162, 2010.

[2] H. Farid, "Asurvey of image forgery detection," IEEE *Signal Processing Magazine.*, vol. 26, no. 2, pp. 16–25, Mar. 2009.

[3] J. Fridrich, D. Soukal, and J. Lukáš, "Detection of copy-move forgery in digital images," in *Proc. Digital Forensic Research Workshop*, Cleveland, OH, Aug. 2003.

[4] Saiqa Khan, ArunKulkarni, "Robust Method for Detection of Copy-Move Forgery in Digital Images," *International Conference on Signal and Image Processing*, 2010.

[5] S. Bayram,H. Sencar, and N.Memon, "An efficient and robust method for detecting copy-move forgery," in *Proc. IEEE Int. Conf. Acoustics,Speech, and Signal Processing*, pp. 1053–1056, Apr. 2009.

[6] I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, and G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099–1110, Sep. 2011.

[7] Xu Bo, Wang Junwen, Liu Guangjie and Dai Yuewei, "Image Copy-move Forgery Detection Based on SURF," *International Conference on Multimedia Information Networking and Security*,2010

[8] Xunyu Pan, SiweiLyu, "Region Duplication Detection Using Image Feature Matching", *IEEE Transactions On Information Forensics And Security, Vol. 5, No. 4,* Dec. 2010

[9] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches," *IEEE Transactions on Information Forensics and Security*, vol. 7, pp. 1841-1854, Dec. 2012.

[10] A. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Duplicated Image Regions" *Computer Science Dept., Dartmouth College, Hanover, NH, Tech. Rep. TR2004-515, 2004*

[11] H. Bay, T. Tuytelaars, L. van Gool, "SURF: Speeded Up Robust Features," *Computer Vision and image understanding , Vol. 110, No. 3, pp. 346–359, 2008*

[12] http://thelede.blogs.nytimes.com/2008/07/10/in-an-iranian-image-a-missile-too-many/

[13] http://www.lambertoballan.net/research/image-forensics/

[14] Lowe, D. G., "Distinctive Image Features from Scale-Invariant Keypoints", *International Journal of Computer Vision, 60, 2, pp. 91-110, 2004.*

[15] Zhou Guojuan, LvDianji, "An Overview of Digital Watermarking in Image Forensics", *Fourth International Joint Conference on Computational Sciences and Optimization*, 2011.

[16] Hany Farid, " Exposing Digital Forgeries From JPEG Ghosts", *IEEE Transactions On Information Forensics And Security, Vol. 4, No. 1, March 2009*

[17] Ruohan Qian,Weihai Li, Nenghai Yu, Zhuo Hao, "Image Forensics with Rotation-Tolerant Resampling Detection", *IEEE International Conference on Multimedia and Expo Workshops, 2012.*

[18] *S.* Bayram, H. T. Sencar, and N. Memon, "A survey of copy-move forgery detection techniques," in *Proc. IEEE Western New York Image Processing Workshop*, Rochester, NY, 2009.

[19] XiaoBing, ShengMin, "Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensics", *International Conference on Computer Science and Software Engineering 2008.*

[20] K. Mikolajczyk and C. Schmid, "A performance evaluation of local descriptors," *IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 27, no. 10, pp. 1615–1630, 2005.*