International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Research Article

A Key-Point Based Robust Algorithm for Detecting Cloning Forgery

Mariam Saleem[Å*]

[Å]Department of Electrical Engineering, College of Electrical & Mechanical Engineering (NUST), Islamabad, Pakistan

Accepted 12 August 2014, Available online 25 Aug 2014, **Vol.4, No.4 (Aug 2014)**

Abstract

Digital image have its significance in several applications from financial documents, scientific literatures /journals, medical records, journalism or evidences in a court of law. However, with the mushroom growth of handy, inexpensive editing software the truthfulness or uprightness of image can no longer be taken for granted. So there is a need to establish techniques in order to declare the integrity of digital images. Digital Image Forensic has somehow solved this problem. The main objective of this field is to develop detection technique to estimate the authenticity of images and to reveal the possibility of image being forged. A wide range of forgery detection techniques have been established in the recent years. Blind Forensic Detection technique-cloning is one of the most common forgery methods. In this paper an attempt is made to develop a robust and effective key-point based forgery detection approach. In this work first SIFT is employed to find image key-points (Location which carries definite details of image) and to extract image features at the detected key-points. For effective matching and detection a productive algorithm called Multi Hop Jumping is then utilized to jump over unnecessary or false key-point matching. A rational framework is developed at the end by providing relative results using previous key-point based forgery detection techniques to witness the proposed technique which is not only efficient, reliable, effective but can also reduce processing time as compared to other key-point based techniques.

Keywords: *Digital Forensic, Copy-Move Forgery, Cloning, Pixel-Based, Key-points, SIFT*

1. Introduction

In this advanced era accepting digital image as an official document have become common practice since it's the most appropriate and fast way of communication. With the advancement in digital photography, the manufacturers of photo editing software quickly catches up momentum by introducing inexpensive and handy tools that has introduced several security issues and have eroded our trust in the authenticity of digital images. Photojournalists manipulate images to create dramatic scenes and propaganda by exaggerating any spectacular or strange event. Now, we can't rely simply on Seeing is Believing.

Inserting some foreign content in the image or removing some of the actual content and replacing with desired content is termed as image tampering & the resulting image is said to be forged image.

Various effective techniques have been developed in the field of digital image forensic. There are two approaches for ratifying the authenticity of digital image. The Active approach uses a known code or information for assessment i.e. digital water mark or digital signature (J.Fridrich,1998) .This approach is limited to specially equipped advanced digital camera like Nikon or canon only whereas passive or blind techniques operates in the absence of any prior information (Avcibas I, Bayram S, Memon N, Ramkumar M, Sankur,2008). These forgery techniques are further classified into a) Image montage or splicing that significantly changes the original image by combining one or more image to create forged image (Fig 1).b) Image retouching that enhance certain features of an image by blending or sharpening it to make the image attractive & c) copy- move (cloning) forgery in which instead of having an external image as the source, the textured region from the same image is copied and pasted to a desired location for disappearance or addition of certain feature in an image (Fig 2). The complete hierarchy is shown in (Fig 3).

Fig1. An example of Image Splicing Forgery, The Guardian's Amelia Hill in her article (Amelia Hill, 2011)

*Corresponding author: **Mariam Saleem**

added that corpse is a composite of first two separate photos from left.

Fig2. An example of Copy-Move Forgery, Iran's show of military might was doctored to remove a launcher which failed to fire-by cloning it with a projectile from same scene. Courtesy: Sepah News

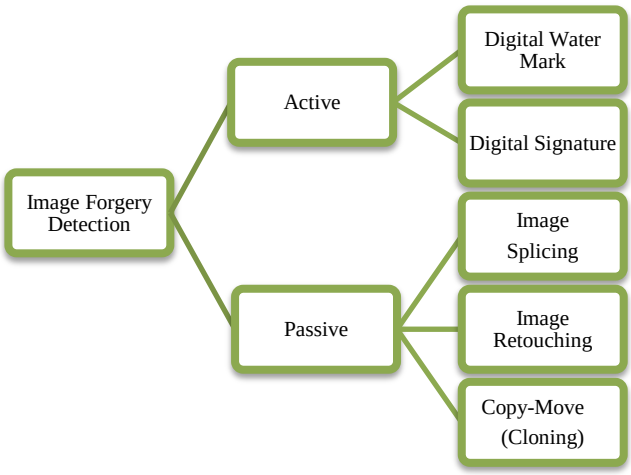

Fig. 3 Hierarchy of Image Forgery

The rest of paper is organized as follows: a comprehensive overview of the previous key-point based cloning techniques in Section 2. In Section 3, we will present the proposed algorithm, In Section 4 we will provide some simulations results and then finally we conclude the paper in the last section.

2. Related Work

In recent years Cloning Forgery Detection has found significant interest in the scientific field. This is evident from the graph (Fig 4) which shows there had been significant focus on the topic in major journals and conference.

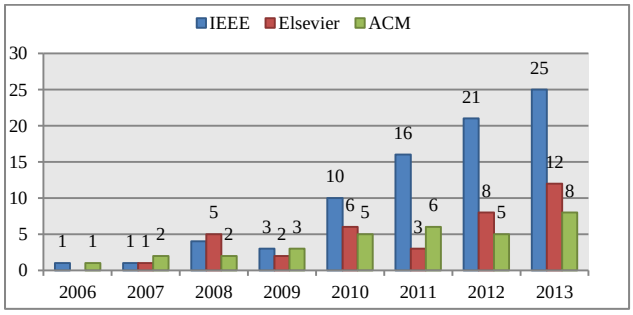

Fig. 4 Chart on Publications of Copy-Move Detection Algorithm

A popular workflow of copy–move image forgery detection is described in (Fig 5). Since our focus is on pixel based only so, one way to detect Copy-Move forgery is using an exhaustive search (A.C. Popescu and H. Farid, 2005). The original image is compared with the circular shifted version of forged image. This approach works well for small-sized images but is impractical for large as it requires $(MN)^2$ computations for every MxN image. An intuitive suggestion was to use Auto Correlation (G.Li,

Q.Wu, D.Tu, and Shaojie Sun, 2007) which involves a correlation between the original segment and the pasted one. This method does not have large computational complexity and often fail to detect forgery. So a Block Matching Procedure was introduced. The task is to divide the image into small overlapping blocks and then extracting features from each block by taking into account the fact that similar blocks would yield similar features. Afterwards, a matching step takes place to search for the duplicated blocks based on their feature vectors. The detected block is said to be forged only if same features are detected within the same distance of features associated to connected blocks. Another approach to detect copy move forgery is key-point based method which searches key points in image without dividing the image (D. G. Lowe, 2004).

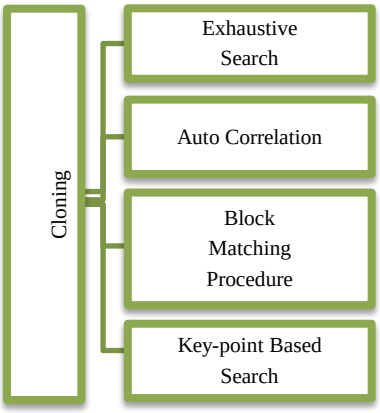

Fig. 5 Work Flow of Copy-Move image Forgery

In this paper we will establish a robust cloning detection technique based on key-point. (B. L. and S. Baboo, 2011) proposed the first technique which employs Speeded up Robust Features (SURF) as a key-point feature. This method successfully detects forgery with minimum false match but was unable to detect small copied regions. (I. Amerini et al., 2012) presented a technique based on Scale invariant Feature Transform (SIFT) features to detect and localize copy-move forgeries. The SIFT descriptors are invariant to changes in illumination, rotation and scaling. This approach not only produces accurate result but can deal with geometric transformation too. A popular work flow of SIFT based detection technique is shown in (Fig 6). (Zhang, 2008) proposed an efficient technique which not only give efficient result but is able to handle other anomalies like additive noise and post processing operation. The approach is to find image key-points (Location which carries distinct information of image) and to extract image features at the detected key-points. Each

key-point is characterized by a feature vector which consists of a set of digital image statistics collected at the local neighbourhood of the corresponding key-point.

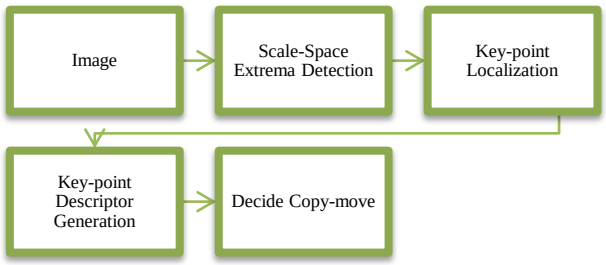

Fig. 6 Work Flow of SIFT based Detection technique

3. Proposed Algorithm

The schematization of proposed algorithm is shown in (Fig 7).

A) Feature Extraction and Key-point Detection

Firstly, the input image is converted to gray scale image. SIFT algorithm is employed in order to find key-points. This algorithm consists of the following steps to find key-point:

a. Scale-space extrema detection
b. Key-point localization
c. Location Orientation
d. Key-point descriptors

SIFT algorithm is employed as it is an extraordinarily robust technique & can handle changes in viewpoints. It can even handle significant changes in illumination sometimes even day vs. night. It is fast and efficient—can run in real time. Moving back to the algorithm SIFT features vectors are computed for detected key-points. At each key-point, a 128 dimensional feature vector is generated from the histograms of local gradients in its neighborhood.

B) Multi-Hop Jumping

In order to make key-point matching more efficient,

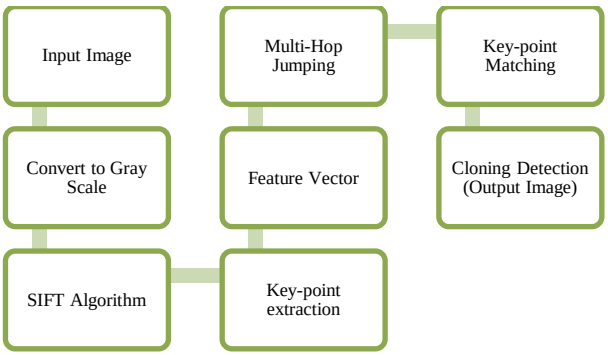

Fig7. A hierarchy of Proposed Algorithm

unnecessary/ false matching is avoided by utilizing the multi-hop jump (MHJ) algorithm. For this purpose the image is first divided into sub-blocks and key-point are searched and matched between each pairs of sub-blocks.

Let A(x, y) denote an image region which is moved and copied into same image, this cloned (copy-moved) region is denoted as A (x', y'), here x'=x+Δx & y'=y+Δy. d = (Δx, Δy) is the distance computed between the original and copy-moved regions. If we start matching the detected key-points there would be several false matches because the region A(x, y) might have some false key-point matches though at same distance d(x, y). If the spatial distances between original blocks (B_j) in region A and the corresponding pasted blocks (B_j') is found to be same, the pairs of original and the copy-moved blocks would then be classified as forged blocks and are said to be false or unnecessary test blocks. So multi-ho jump is applied to avoid such unnecessary blocks. MHJ for block A(x, y) and A' (x', y') is shown in (Fig). Blocks are sorted by their features vectors evaluated by SIFT. To make the matching convenient they are arranged in row. The block number of the first row is the position of the top-left corner point of each block. The second row in the figure shows the distance (D_n) of the block number corresponding to each pair blocks. It is obvious that many pair blocks would correspond to same distance D_n.

Following steps are repeated in an iterative approach considering the principles of multi-hop jumping.

1. Place the sorted feature vectors in a Matrix M. let the matching pointer be denoted by p. Initialize p to the first line of M with the current D_n. Assume the jump distance (n) to be [m/16], m denotes the number of rows of matrix.

2. An array u (i) is generated which contain the record of D_n, and is then initialized to 0. Now p would jump n block forward until the last row of M is reached.

3. Evaluate the new D_n' and compare it with D_n. If D_n is found to be same as D_n' then u (D_n) = u (D_n) + n, and the algorithm precede to the Step 2.If not the algorithm proceeds to the Step 4.

4. A threshold T_d is defined which states that the blocks whose D_n does not exceed T_d are considered to be replication. Furthermore, the blocks whose distances are minor are ignored for robustness. After the elimination of unnecessary blocks key-point based matching is employed.

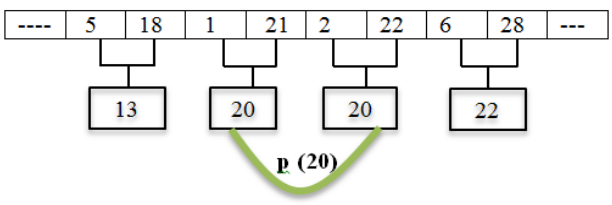

Fig4. An example of matching two regions by multi-hop jumping.

C) Key-point Matching

After applying the multi-hop jumping algorithm the unnecessary matched blocks are thus eliminated and the remaining or accurate key-point is thus matched on their feature.

4. Simulation Results & Discussion

In this section we will examine the quantitative performance of the proposed algorithm through simulation experiments on tampered/forged images. The Experiments was implemented in Matlab R2012a on a machine with an Intel Core i5, 2.4 GHz processor with 4GB memory.The experimental dataset MICC-F220 consists of 220 images: 110 are tampered (cloned only) and 110 are originals. The images in this data set are in one of three formats: JPEG, BMP, and TIFF. The image resolution varies from 722 × 480 to 800 × 600 pixels and the size of the forged patch covers, on the average, 1.2% of the whole image.

Following the algorithm of proposed method described in Section 3 the results are shown in (Fig 5).

(a) (b)

Fig5. Input image a) Original b) Forged

The original image was forged by copy-moving the flower in the same image as evident from (figure 5).Rest of the results following the proposed methodology is shown in (Fig 6,7,8,9,10).

Fig6. Converting the forged image to gray scale

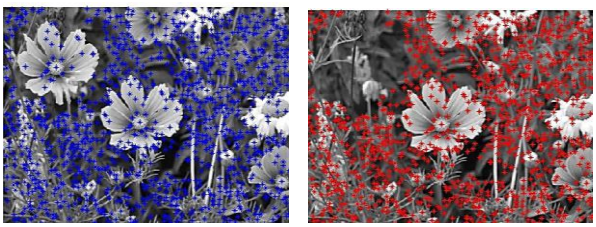

Fig7. Feature Descriptors extraction using SIFT algorithm

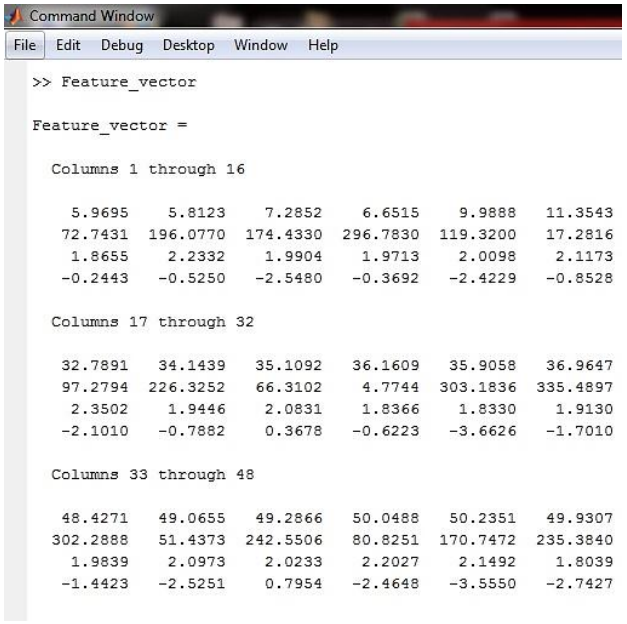

Fig. 8 Feature Vector Calculation

Fig.9 Key-point matching

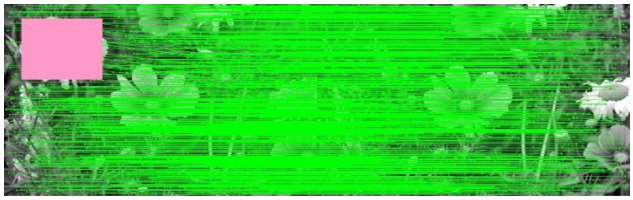

Fig.10 Cloning Detection

Now moving towards the comparative analysis of the proposed method with previous & recent key-point based detection methodology, the analysis is based on following quantitative parameters: True Positive (number of tampered blocks declared tampered), True Negative (number of un-tampered block declared un-tampered), False Positive (number of un-tampered blocks detected tampered), & False Negative (number of tampered blocks declared un-tampered) and parameters like overall performance accuracy, sensitivity or the ability to detect presence of forgery .

The results of the analysis between these techniques are evaluated using complete data set. The previous key-point based detection techniques were also implemented. The implementation was based on material provided in corresponding literature. It might be different from author's original implementation so we can expect to have slightly different results.

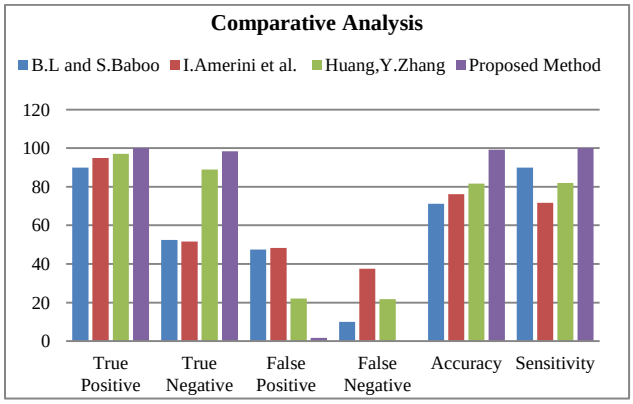

Fig11. Comparative Analysis of Cloning Techniques

The performance analysis of above mentioned parameters is shown in (Figure 11). More over the time complexity of the previous methods with the proposed is shown in (table 1).

Table1 Processing time Complexity

Algorithm	Time Complexity
(B. L. and S. Baboo, 2011)	61.86
(I. Amerini et al., 2012)	56.32
(H. Huang, W. Guo , and Y. Zhang,2008)	27.22
Proposed method	10.17

From the performance analysis chart and table it is evident that the proposed method is accurate as compared to previous cloning techniques since the true positive and true negative rate is much higher as compared to other methods moreover the false positive rate is less and false negative is negligible. This is just due to the utilization of multi-hop jumping in key-point matching. If we look at the time processing the reduced time computation is due to the reduced feature vector length in proposed algorithm which results in faster computations.

Conclusions

Passive-Blind Cloning technique is one of the emerging areas of research in order to validate the integrity of digital image. In this paper, we have proposed an effective & efficient key-point based method to detect cloning forgery. The proposed methodology doesn't require prior knowledge of the image content or any embedded watermarks or signature. Our algorithm is based on local image SIFT features, which is effective in detection of passive duplications with region scaling and rotation. To reduce false key-point matching and to speed up the method, MHJ algorithm is employed in the matching process. Experimental results demonstrate that this method can accurately and quickly detect the cloned region with the processing time greatly reduced. We then compared the proposed algorithm with previous techniques which shows that the proposed algorithm gives better performance.

However, the proposed algorithm is weak in case of repetitive image contents. In future, we would try to deal with this problem.

References

J. Fridrich (1998), Image Watermarking for Tamper Detection, *Proc. of Intl. conference on Image Processing (ICIP), vol. 2*, pp. 404-408.

Avcibas I, Bayram S, Memon N, Ramkumar M, Sankur (2011),A classifier design for detecting image manipulations *In: Proc. International conference on image processing (ICIP*). p. 2645–8.

Amelia Hill (2011). Osama bin Laden Corpse Photo is Fake, *The Guardian*.

A.C. Popescu and H. Farid (2005). Exposing digital forgeries by detecting traces of resampling, *IEEE Transactions on Signal Processing, vol. 53(2),* pp. 758–767.

G.Li, Q.Wu, D.Tu, and Shaojie Sun (2007), A sorted Neighbourhood approach for detecting duplicated regions in image forgeries based on DWT and SVD, *IEEE International Conference on Multimedia & Expo*.

D. G. Lowe, (2004) Distinctive image features from scale-invariant key-points, *International Journal of Computer Vision*, vol. 60, no. 2, pp. 91–110.

B.L.Shivakumar, S.Baboo (2011), Detection of region duplication forgery in *International Journal of Computer Science Issues* 8(4)) 199–205.

I. Amerini , L. Ballan, R. Caldelli, A. Del Bimbo, G. Serra (2010) , Geometric tampering on estimation by means of the SIFT-based forensic analysis, *Proceedings of the IEEE ICASSP*, Dallas, TX, USA.

H. Huang, W. Guo, and Y. Zhang (2008), Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm, in *Proceedings of IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, Vol. 2, pp. 272-276.

Data Set: http://www5.cs.fau.de/research/data/image-manipulation/