International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-2 Issue-5, April 2013

Copy- Move Attack Forgery Detection by Using SIFT

Swapnil H. Kudke, A. D. Gawande

Abstract*— Due to rapid advances and availabilities of powerful image processing software's, it is easy to manipulate and modify digital images. So it is very difficult for a viewer to judge the authenticity of a given image. Nowadays, it is possible to add or remove important features from an image without leaving any obvious traces of tampering. As digital cameras and video cameras replace their analog counterparts, the need for authenticating digital images, validating their content and detecting forgeries will only increase. For digital photographs to be used as evidence in law issues or to be circulated in mass media, it is necessary to check the authenticity of the image. So In this paper, describes an Image forgery detection method based on SIFT. In particular, we focus on detection of a special type of digital forgery – the copy-move attack, in a copy-move image forgery method; a part of an image is copied and then pasted on a different location within the same image. In this approach an improved algorithm based on scale invariant features transform (SIFT) is used to detect such cloning forgery, In this technique Transform is applied to the input image to yield a reduced dimensional representation, After that Apply key point detection and feature descriptor along with a matching over all the key points. Such a method allows us to both understand if a copy–move attack has occurred and, also furthermore gives output by applying clustering over matched points.

***Index Terms*— tampering, Image forgery, copy-move attack, scale invariant features transform (SIFT), cloning forgery**

I. INTRODUCTION

The availability of powerful digital image processing programs, such as Photoshop, makes it relatively easy to create digital forgeries from one or multiple images. In a Copy-Move forgery, a part of the image itself is copied and pasted into another part of the same image. This is usually performed with the intention to make an object "disappear" from the image by covering it with a segment copied from another part of the image. Textured areas, such as grass, foliage, gravel, or fabric with irregular patterns, are ideal for this purpose because the copied areas will likely blend with the background and the human eye cannot easily discern any Suspicious artifacts. Because the copied parts come from the same image, its noise component, and most other important properties will be *compatible* with the rest of the image and thus will not be detectable using techniques that look for Incompatibilities in statistical measures in different parts of the image, and to make the forgery even harder to detect, one can use the available photo editing software's and image processing tools. As a result, it has become relatively easy to manipulate digital images and create forgeries that are difficult to distinguish from authentic photographs.

Examples of the Copy-Move forgery are given in Figures (1). In Figure, you can see a less forgery in which a truck was covered with a portion of the foliage left of the truck. It is still not too difficult to identify the forged area visually because the original and copied parts of the foliage bear a suspicious similarity.

In this paper information is concerned with a technique that can efficiently detect and localize duplicated regions in an image. In this approach an improved algorithm based on SIFT is used to detect such cloning forgery. In this technique Transform is applied to the input image to yield a reduced dimensional representation. After that compressed image is divided into overlapping blocks, these blocks are then sorted and duplicated blocks are identified by applying key point detection and feature descriptor along with a matching and clustering, Such a method allows us to understand if a copy–move attack has occurred and, furthermore gives output.

Figure 1 example

Following figure shows two images
a) Original image
b) forged image (copy–move attack)
Over which we apply this method to find result of forgery detection

Figure a) original image

Figure a) forged image

Manuscript published on 30 April 2013.
***Correspondence Author(s)**
Mr. Swapnil H. Kudke, Department of Electronics and telecommunication, Sipna college of engineering And technology, Amravati, India.
Dr. Avinash D. Gawande, Head Department of Computer Science, Sipna college of Engineering and technology, Amravati, India.

II. LITERATURE REVIEW

A number of techniques was proposed before the invention for detecting digital forgeries like DWT based algorithm, SURF based algorithm, pixel based algorithm, kernel principal component analysis (KPCA), watermark approach etc. And all are giving their efforts for detecting such forgeries. Digital watermarks have been proposed as a means for fragile authentication, content authentication, detection of tampering, localization of changes, and recovery of original content [1]. While digital watermarks can provide useful information about the image integrity and its processing history, the watermark must be present in the image before the tampering occurs, and this is become a limitation to this approach. Another possibility for blind forgery detection is to classify textures that occur in natural images using statistical measures and find discrepancies in those statistics between different portions of the image ([2], [3]). At this point, however, it appears that such approaches will produce a large number of missed detections as well as false positives.

Since the key characteristics of Copy-Move forgery is that, copied part and the pasted part are in the same image, one method to detect this forgery is exhaustive search, but it is computationally complex. A. C. Popescu and H. Farid proposed a similar detection method[4], in which the image blocks are reduced in dimension by using Principal Component Analysis (PCA). But the efficiency of detection algorithm was bad, because, blocks are directly extracted from original image, resulting in a large number of blocks, D. Soukal, proposes DCT based copy-move forgery detection in single image[5], In which The image blocks are represented by quantized DCT coefficients, and a lexicographic sort is adopted to detect the duplicated image blocks. B.L.Shivakumar and Dr. S.Santhosh Baboo have proposed copy-move forgery detection method based on SURF[6], which detects duplication region with different size. It shows that the proposed method can detect copy-move forgery with minimum false match for images with high resolution. To increase the speed of operation process many researchers use blocking approaches[7]. G.Li, Q.Wu, developed a sorted neighborhood method based on DWT[8] and SVD (Singular Value Decomposition).In this method the computation of SVD takes lot of time and it is computationally complex.

This proposed method is used SIFT and able to detect and to estimate the homographic matrix in a copy–move forgery attack. Multiple copy–move forgeries are managed by performing a robust feature matching procedure and then a clustering on the key point coordinates in order to separate the different cloned areas, by using key point detection, matching on key point and clustering approaches.

III. PRACTICAL METHODOLOGY

Concept behind this paper is to Detection of malicious manipulation with digital images. In particular, we focus on detection of a special type of digital forgery – the copy-move attack, where an improved algorithm based on scale invariant features transform (SIFT) is used to detect such cloning forgery.

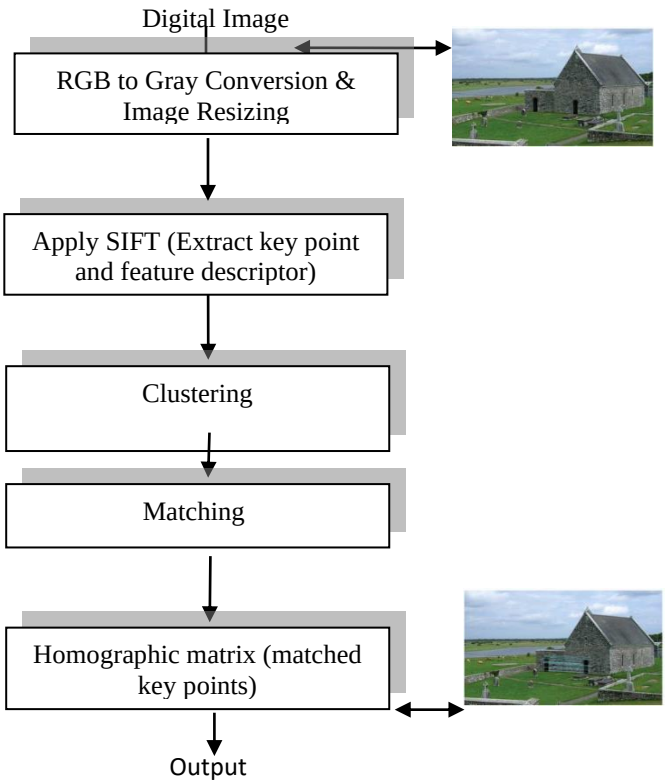


Figure 2 Practical Methodology

The proposed method is based on the SIFT algorithm to extract robust features which can allow it to discover if a part of an image was copy–moved. In fact, the copied part has the same appearance of the original one, thus key points extracted in the forged region will be similar to the original ones. Therefore, matching among SIFT features can be adopted for the task of determining possible tampering. The process flow of this method is shown in figure 2.

A. Image conversion and pre-processing

Axial Image is loaded as the input. Loaded image is converted into gray scale format. Then image is resized. Image may consist of film artifacts but images which we processed are free from noise so there is no need to apply filtering. So the pre-processing stage makes the image ready for further processing.

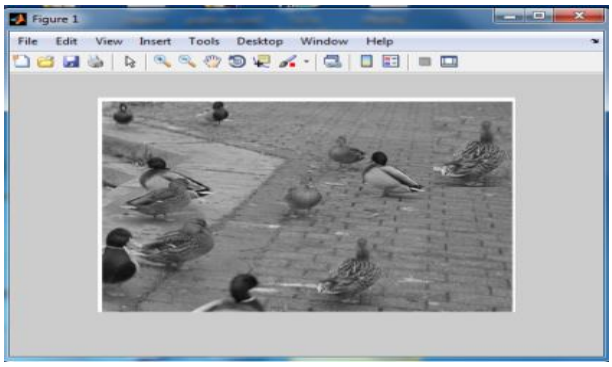


Figure 3. Result after Image converted to Gray Scale & resized

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

B. Apply SIFT

Applying SIFT is the first stage of proposed method, which contains the different steps which are generally used to finding the key points, key point detection and feature descriptor which apply on entire image. This approach has been named the Scale Invariant Feature Transform (SIFT), as it transforms image data into scale-invariant coordinates relative to local features. This mainly concerned with finding key points, by converting RGB image into grayscale image. Here, we present a new region duplication detection method based on the image SIFT features, we first detect SIFT key points in an image and compute the SIFT features for such key points. At each key point, a 128 dimensional feature vector is generated from the histograms of local gradients in its neighborhood.

SIFT consist of the following stages:

1) Scale-space extrema detection: The first stage of computation searches over all scales and image locations, which is used to find the local extremas in scale-space. It contains

- Search over scales and image locations
- Locate local extremas
- A cascade filtering approach
- Scale-space images for octave

2) Keypoint localization: to determining location and scale at each candidate location a detailed model is fit. And Keypoints are selected based on measures of their stability.

- Selects keypoints from local extremas
- Detection of local keypoints
- Elimination of keypoints

3) Orientation assignment: At each keypoint location one or more orientations are assigned based on local image gradient directions. All future operations are performed on image data that has been transformed relative to the assigned orientation.

4) Keypoint descriptor: The local image gradients are measured at selected scale in the region around each keypoint. These are transformed into a representation that allows for significant levels of local shape distortion and change in illumination.

C. Clustering

This is another important stage in this proposed method, to identify possible cloned areas, feature matching based clustering is performed on coordinates of the matched points. It creates a hierarchy of clusters which may be represented by a tree structure. The algorithm starts by assigning each keypoint to a cluster; then it computes all the cosine distances among clusters, finds the closest pair of clusters, and finally merges them into a single cluster. Such computation is iteratively repeated until a final merging situation is achieved. The way this final merging can be accomplished is basically conditioned both by the linkage method adopted and by the threshold used to stop cluster grouping.

Important point's are-

1) Feature matching based approach is used.
2) Cluster the best matching key points in one group.
3) Cosine distance between features are calculated

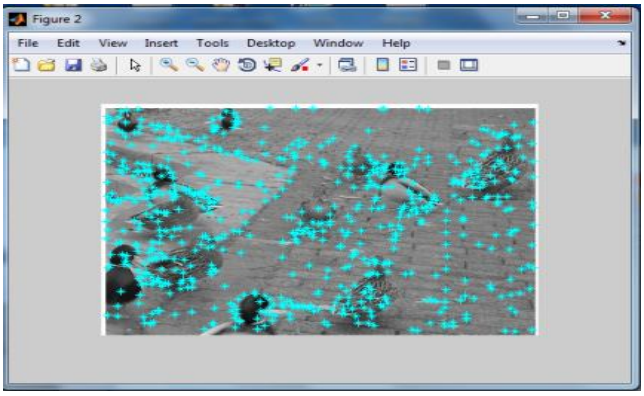
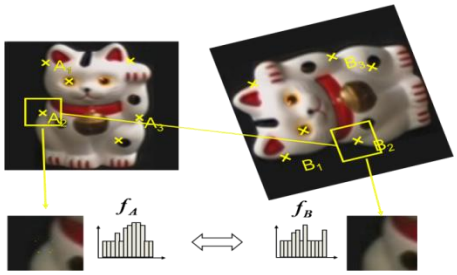


Figure 4 Result After Applying Sift And Clustering

D. Key point matching

Key point matching is another important stage of the proposed method, which mainly concern with the matching of extracted feature keypoints from SIFT algorithm. In key point matching first reads the keypoint from given input image then, Compare the keypoints of images and if the keypoints matches then draw a line which indicating the matched keypoints, Then append the two images and draw a line which indicate the matches.



1) Find a set of distinctive keypoint
2) Define a region around each keypoint
3) Extract and normalize the region content
4) Compute a local descriptor from the normalized region
5) Match local descriptor

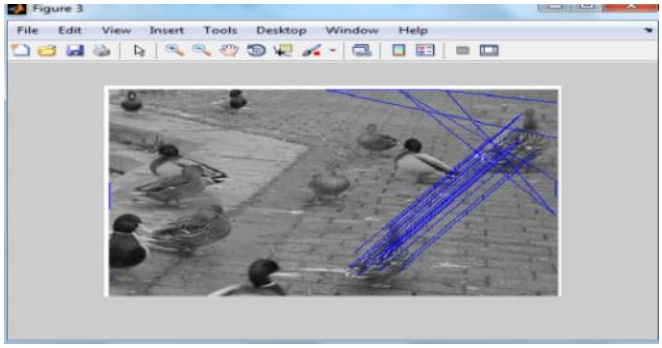


Figure 5 Result After Applying Sift And Key Point Matching

Hear this result shows that forgery is present hear and this is shows directly.

E. Homographic matrix (key point finding)

- It tells about the translational relation between key points from original and forged object

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

- The transformation matrix from correspondent points are calculated
- Gives total key points

This is one of the another stage in proposed method, the proposed method determines which geometrical transformation was used between the original area and its copy–moved version. Let the matched point coordinates are, $x_i = (x, y, 1)^T$ and $x'_i = (x', y', 1)^T$; their geo-metric relationships can be defined by an affine homography which is represented by a 3 * 3matrix .This matrix can compute by resorting to at least three matched points. In particular, we determine using maximum likelihood estimation of the homography .

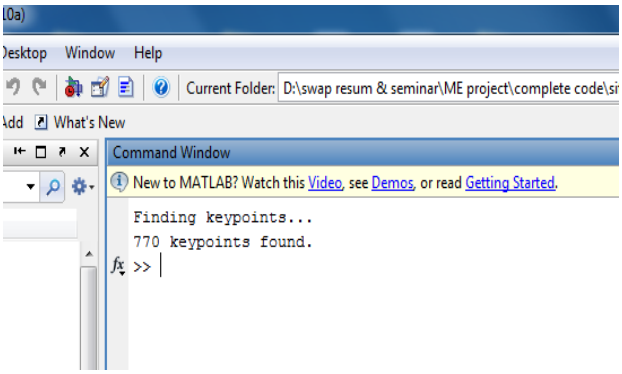


Figure 6 Result For Calculation Of Keypoints

IV. CONCLUSION

In this paper a method for forgery detection in digital image based on SIFT is used. This SIFT based technique is dependant on feature extraction by using key point detection and feature descriptor after that apply matching and clustering over all the key points and matching points for getting output with homographic matrix. This method is mostly used to Detection of malicious manipulation with digital images (digital forgeries) in case of copy-move attack.

ACKNOWLEDGMENT

We would like to acknowledge the Faculties of Electronics & Telecommunication Department, Sipna College of Engineering & Technology, Amravati for their support. I Swapnil H. Kudke specially want to thank my guide Dr. A. D. Gawande sir for their guidance and constant encouragement towards the work.

REFERENCES

1. J. Fridrich, "Methods for Tamper Detection in Digital Images", *Proc. ACM Workshop on Multimedia and Security*, Orlando, FL, October 30−31, 1999, pp. 19−23.
2. S. Saic, J. Flusser, B. Zitová, and J. Lukáš, "Methods for Detection of Additional Manipulations with Digital Images", *Research Report, Project RN19992001003 "Detection of Deliberate Changes in Digital Images"*, ÚTIA AV ČR, Prague, December 1999 (partially in Czech).
3. J. Lukáš, "Digital Image Authentication", *Workshop of Czech Technical University 2001*,Prague, Czech Republic, February 2001.
4. A.C.Popescu and H.Farid, "Exposing digital forgeries by detecting duplicated image regions,"‖ Dartmouth College, Hanover, New Hampshire, USA: TR2004-515, 2004.
5. J. Fridrich, D. Soukal, and J. Lukas, ―Detection of copymove forgery in digital images,‖ Proceedings of the Digital Forensic Research Workshop. Cleveland OH, USA, 2003
6. B.L.Shivakumar and Lt. Dr. S.Santhosh Baboo "Detection of Region Duplication Forgery in Digital Images Using SURF"‖ IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011
7. Sarah A. Summers, Sarah C. Wahl ―Multimedia Security and Forensics.Authentication.of.Digital.images‖http://cs.uccs.edu/~cs525/studentproj/proj52006/sasummer/doc/cs525projsummer.sasummer/doc/cs525projsummersWahl.doc
8. G.Li, Q.Wu, D.Tu, and Shaojie Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD,‖" IEEE International Conference on Multimedia & Expo, 2007.

AUTHOR PROFILE

Mr. Swapnil H. Kudke currently pursuing Master Engineering in Digital Electronics in Amravati university. Have already completed Bachelor Engineering in Electronics and telecommunication from Amravati university with a Diploma in Electronics From MSBTE. Also getting participated in national level paper and poster presentation along with a roborace and robowar events. Achieved 1STprize in event"ROBO WAR**"** in National level science & technical festival.

Dr. Avinash D. Gawande did his B. E. from Amravati university in electronics, M. E. and Ph.D. in Electronics Engineering from Amravati University. He is working as the Head of Department in computer science department at Sipna College of Engineering & Technology, Amravati.He has more than 18 years of Teaching Experience

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)