An Enhanced Method to Detect Copy Move Forgery in Digital Images processing using 2D-DWT Approach

Rajni[1], Mr. Parminder Singh[2]

[1] M.Tech Student, Department Of ECE, Doaba Institute of Engineering & Technology, Punjab, India
[2]Assistant Professor , Department Of ECE, Doaba Institute of Engineering & Technology Kharar , Punjab, India

---

Abstract - *Communication in visual form is very important in itself. It is also a very convincing medium of transfer of information. Numerous fields of technology depend vastly on better quality and correctness of source image. But digital image forgery creates problems for these technologies. Manipulation of images is now a very easy job due to availability of numerous images editing software's. It is now possible to add, modify, or remove important features from an image without leaving any perceptual traces of tampering. Image forensics is a domain dedicated to stop such attempts and preserve the data in an image. Through this project, we would like to detect a faulty image from image move forgery attack.*

Key Words: GIMP, SIFT, RANSAC, DWT, SURF, FFT, LDP

1. INTRODUCTION

Images are one of the natural sources of information. Currently they are the most common and convenient way for expressing and transmitting information. Information expressed in thousands of words can be easily expressed by a digital image. The human being visual system has a high ability in deriving pictorial information from digital images. Nowadays, digital images play a very important role in our community, in a wide variety of applications.

There are mainly three types of image tempering techniques. Enhancing Tempering, Compositing Tempering, and Copy Move Tempering: In Compositing tempering, two or more images are used to make the new tempered image. It changes the whole content of the image. In Copy - Move tempering , technique some parts of the image are copied than pasted into same image then some post processing steps are apply to tempered image. It is difficult to identify which parts of image is copy and where it is pasted. It is difficult to identify this type of tempering.

Tempering detection methods : Active method, Passive method.

Active method : In Active method, some information are added in the original images. When unauthorized person can change the content of image by applying any post processing techniques, it is identify by the comparing tempered image with original image and we can detect the tempering. In this method Water marking and digital signature are used to detect tempering. it use algorithm or key to add the information in the original image. Some camera available in market which automatically add the algorithm or key into image to authenticate the images. But this method is not robust because it require knowledge of image source like digital camera.

Passive method: In passive method, this method sometime known as blind method to detect image tempering. This method take advantage of processing steps like acquisition and storage of digital images. This trace can be treated as the watermarking/digital signature of digital images. This technique not required any prior knowledge of original image/ camera sources. When we applying post processing step to original images its cause change the image characteristic and it is key to detect tempering in digital images. Passive method can be categorized by statistical method, this method depend on the pixel value of the images, and it required more images to estimate the internal traces and another method based on visualization. But this method is fail because of some tie user can't identify the tempering in digital image because of availability of post processing tool such as Adobe Photoshop.

1.1 Related Work

Recently, there has been growing research on passive forensic methods devoted to the security and protection of multimedia information. Each technique targets addressing different aspects related to verifying the authenticity of digital data. This introduces the techniques and methods currently available in the area of digital image tempering detection. A survey of the current research is presented as well as an analysis of the current techniques and methods available to detect image tampering. This area of research is relatively new and only a few sources exist that directly Related to the detection of image forgeries, therefore techniques are presented that apply to general digital image processing, but show promise in the detection of digital forgeries..

1.2 Types of Image Forgery

There are basically three types of digital image forgery. It includes image enhancing or retouching, image composition /splicing and image copy - move forgery.

1.2.1 Image enhancing or retouching Forgery

It is less harmful kind of digital image forgery. It does not significantly change an image but enhances or reduces certain features of an image. One can enhance certain features of

an image to make it more attractive but it is ethically wrong.

Figure 1 shows an original image of lady's face whereas figure 2 shows the same face with enhanced effects applied to it.


Fig -1 Original Image Fig-2 Enhanced Image

1.2.2 Image composition or splicing Forgery

It is a technique that involves a composite of two or more images to create a fake image. Regions from various images are combined together in base image is known as image composition. Figure 3 shows a base image. Figure 4 shows shark inside sea. From figure 4region occupied by shark is copied and it is pasted below the helicopter in the base image. This copy-paste operation from one image into another image forms a spliced image as shown in figure 5.



Fig 3: Base Image Fig 4: Shark image Fig5: Base image With shark.

1.2.3 Image copy-move forgery

It is a technique that copy background or other features from one part of the image and paste into the same image at another location to hide or alter regions from the image. In this type, instead of having an external image as the source, it uses portion of the original base image as its source. Part of the original image is copied and moved to desired location and pasted into it.

Figure 6 shows original image of a garden view.

In figure-7 a region occupied by a deer is copied and pasted on the grass at front side in the same view. [2]


Figure 6: Original Image Figure 7: Forged Image

The copy-move forgery is one of the difficult forgeries to detect in image processing. It is common image tampering technique used now a day. In this some part of the image needs to be covered to add or remove information of an image. There are two approaches for detecting digital image forgery. One is active approach and the other is passive approach [2].

2. LITERATURE SURVEY

Bharat M. Prajapati, Nirav P. Desai[8] - Digital images have been widely used from last few years in various applications such as forensic evidences, medical, insurance and military etc. With easy availability of low - cost image modification and editing software such as Adobe Photoshop, GIMP (GNU Image Manipulation Program), paint etc. digital image content is not considered as safe. There are various types of image tempering techniques but Copy - move is the mostly used. In this technique, some part of image is copied then it is pasted on same Image, which changes the visual contents of image.

•**An efficient algorithm for image copy-move forgery detection based on DWT and SVD [2014]** In this paper, an efficient algorithm is presented for image copy-move forgery detection and localization based on DWT and SVD.

Experiment results demonstrate that our proposed algorithm can effectively detect multiple copy-move forgery and precisely locate the duplicated regions, even when an image was distorted by Gaussian blurring, JPEG compression and their mixed operations [1]

•**A Survey of Copy-Move Forgery Detection Techniques for Digital Images [April 2015]** The objective of copy- move forgery may be to conceal some unwanted features, or to add some local features which are otherwise absent. Extensive research has been done to device methods to detect copy-move forgery in both intensity domain and frequency domain. Various image analysis techniques using image moments, dimensionality reduction, texture analysis etc. Has been experimented. This paper presents a study of various image forgery techniques a survey of various attempts in copy-move forgery detection. A comparative analysis of major techniques is also presented.[2]

•**Forensic analysis of digital image tampering [June 2015]** In recent decades, digital images have been used In a growing number of applications such as medical, Insurance,

military and forensic analysis etc. With Increasing popularity and the availability of low-cost image Editing software such as Adobe Photoshop, GIMP (GNU Image Manipulation Program), paint etc. So the integrity of Digital image content can no longer be taken for granted. In this some part of image is copy then it is pasted on same Image, it cause change visual contents of image. This paper introduces a new methodology for the forensic analysis of Digital image tempering. In this, we propose detection Method based on SIFT (Scale Invariant Features Transform).This method is robust and less time required to detect tempering in digital images than other Method. [3]

•A Scheme for Copy-Move Forgery Detection in Digital Images Based on 2D-DWT [Sep 2014] In this paper, a copy-move image forgery detection Scheme is developed based on a block matching algorithm. Instead of considering spatial blocks, 2D-DWT is performed on The forged image and then DWT domain blocks are considered, Where only approximate DWT coefficients are utilized. In order To reduce the computational burden, unlike conventional Approaches, instead of performing block matching operation among all blocks, some candidate blocks are first selected from The no overlapping blocks based on a similarity measure. [4]

•Detecting Multiple Copies of Copy-Move Forgery Based on SURF [March 2014] An Extensive growth in software Technologies results in tampering of images. A major Problem that occurs in the real world is to determine whether an image is authentic or forged. Copy-Move Forgery Detection is a special type of forgery detection Approach and widely used under digital image forensics. In copy-move forgery, a specific area is copied and then Pasted into any other region of the image. The main Objective of this paper is to detect the multiple copies of The same region and different regions. In this paper, Key point-based method is used. In key point-based Method, SURF (Speeded Up Robust Features) method is Used for feature extraction. The g2nn strategy is done for identifying the matched points. Then the Agglomerative Hierarchical Clustering is done on the matched points so that false detection rate can be reduced [5]

•A Review on Copy Move Forgery Techniques [March 2015] With the presence of image editing software and digital cameras, techniques for digital image tampering are Becoming more and more sophisticated and widespread. How to prove the integrity and authenticity of digital images Becomes a more and more urgent problem at present, especially in some critical applications, such as court evidence, News broadcast photos, medical images, defense photos, sports pictures etc., in which preserving the exact fidelity of The original image is a legal, moral or technical requirement. In this paper an overview of passive image authentication is presented and the different copy move Forgery detection techniques are reviewed.[6]

3. PROPOSED METHOD

In copy-move forgery, there exists a strong correlation between the copied and pasted parts which can used as evidence for detecting copy-move forgery. Given a tampered image of size M*N, the major steps involved in the detection is as follows.

A. Pre-processing

The aim of pre-processing is the improvement of image data that suppresses unwanted distortions or enhances some image features important for further detection. The given image is converted into grey-scale (color conversion). When applicable (except for algorithms that require color channels). Other pre-processing techniques includes, dimension reduction, image resizing, low-pass filtering etc. In both block-based and key-point based methods necessary pre-processing can be applied.

B. Feature Extraction

For block-based methods, feature vectors are extracted for each block. While for key-point based methods, feature vectors are computed only key-points in the image such as regions with entropy etc.

C. Matching

After feature extraction, the potential copy-move pairs are identified by searching blocks with similar features. High similarity between feature descriptors can be interpreted as duplicated regions. In block-based method lexicographically sort similar features and Best-Bin-First search method to get approximate nearest neighbor in key-point based methods helps in the feature matching.

D. Filtering

A single similarity criterion is not enough to claim the presence/absence of duplicated regions. Filtering schemes are thus used to reduce probability of false matches. Finally post-processing can be done to preserve matches that exhibit a common behavior. [7]

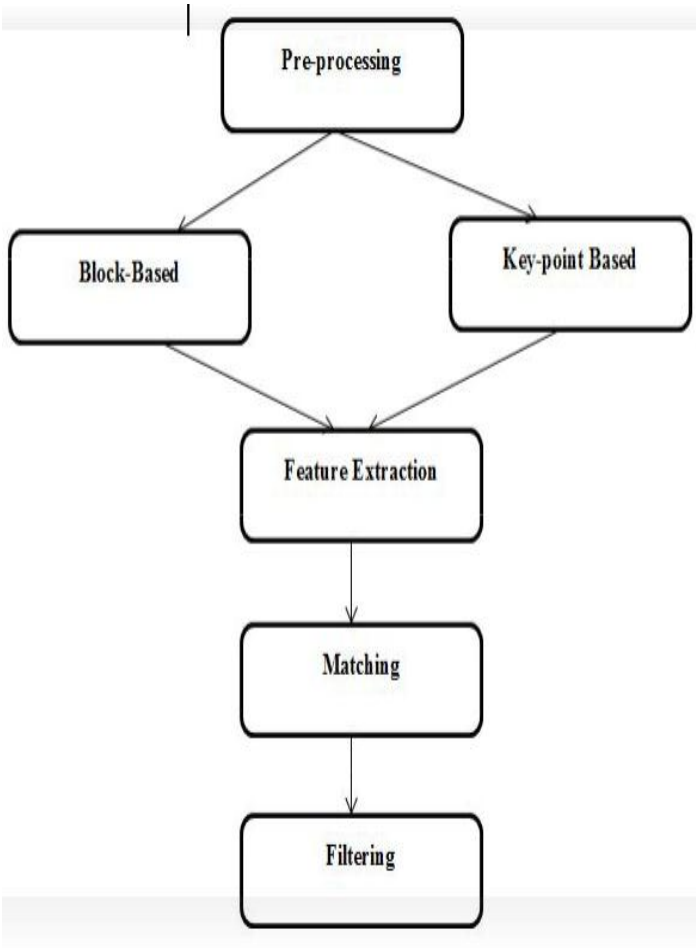


Fig 8: Filtering Method

4. RESULT ANALYSIS

In this section we first show a few examples of copy–move forgery and their corresponding detection result, then give the statistic results of experiment. The experiments were carried out with MATLAB 2016A with a total of 220 images. User can also add images as per his/her need. You just have to put images in the folder given with the code.

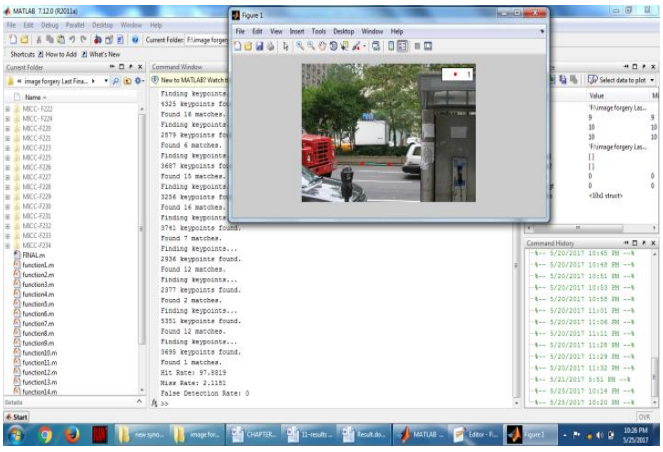
While detecting these images, following cases could be true.

1. Tampered image detected HIT
2. Tampered image not detected MISS
3. Good image detected HIT
4. Good image detected as tampered image MISS

We have conducted this experiment on MICC-F220 set of images available to download http://www.micc.unifi.it/downloads/MICC-F220.zip. These examples include copied and pasted multi-regions and ones with rotation and scale. From these experimental results we can see the proposed method can detect copy-move forgery, even Tampered region operated by geometrical transform. Following are the type of images we have used in the process.

S.No	Image Name	Hit Rate	Miss Rate	False Detection Ratio
1	Set 1	97.1707	2.8293	0
2	Set 2	97.8182	2.1818	0
3	Set 3	100	0	0
4	Set 4	97.9329	2.0671	0
5	Set 5	100	0	0
6	Set 6	97.383	2.617	0
7	Set 7	97.2736	2.7264	0
8	Set 8	97.8432	2.1568	0
9	Set 9	97.3643	2.6357	0
10	Set 10	97.0427	2.9573	0
11	Set 11	97.4795	2.5205	0
12	Set 12	97.6692	2.3308	0
13	Set 13	97.8147	2.1853	0
14	Set 14	97.4374	2.5626	0
15	Set 15	97.2373	2.7627	0
Average Values In Percentage		97.83	2.16	0 %

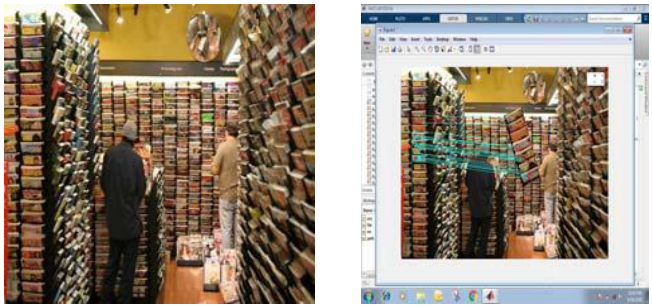
Below Image for the (set 1) with Result:



Following are the percentage values which we calculated after testing a number of such images using the said algorithm.

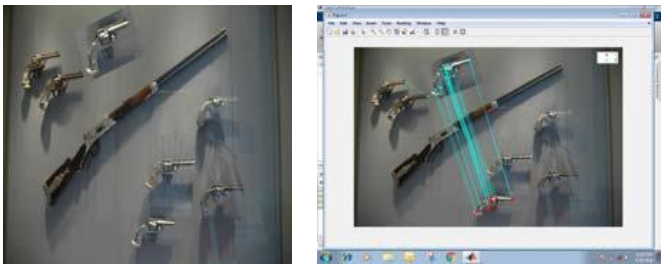
1. Good images with no tampering
2. Tampered image with same scale tampering
3. Tampered image with different scale tampering
4. Tampered image with scaled down and rotated tampering

Our algorithm was able to detect these images effectively. We can conclude easily that the above mentioned processing stands fit to detect copy move forgery attacks in images.



I *j*

Fig.9. Copy Move forgery and its implementation. (i)Original image, (j) Resultant Image.



I *j*

Fig.10. Copy Move forgery and its implementation. (i)Original image, (j) Resultant Image

4.1 Comparison of Average Forgery Detection:

Methods	Average Hit Rate (%)	Average Miss Rate (%)	Average FDR (%)
Proposed	97.83 %	2.16 %	0 %
Method	93 %	7 %	5 %

5. CONCLUSIONS AND FUTURE SCOPE

In this project firstly we find the image that is tempered or not tempered with the method of key points matching feature. Then we computed three main parameters named hit rate, miss rate and false detection ratio on the different set of images accordingly and found the exact values of that three parameters. Then in the last we computed the average values of these three parameters and found the hit rate nearly 97%. Local invariant features are widely used in image recognition and image retrieval. In this project we introduce them for copy-move image forgery. Since SIFT feature is a type of good local invariant feature with strong stability and distinctness, the proposed method in this project combines SIFT feature and matching technique based k-d tree and BBF, and gets better performance for copy-move forgery. It can detect tampered regions with some post-operations such as JPEG compression, Gaussian blurring, rotation, scale. Fortunately tampers seldom work in these areas because the forgeries are detected by eyes easily. Copy-move forgery detection based on local invariant feature is a direct method, its performance is decided by local feature algorithm and matching technology. Next work will concentrated on improving existing feature extracting and matching method.

REFERENCES

[1]"Feng Liu, Hangzhou" and Hao Feng " An efficient algorithm for image copy-move forgery detection based on DWT and SVD" International Journal of Security and Its Applications Vol.8, No.5 (2014), pp.377-390 http://dx.doi.org/10.14257/ijsia.2014.8.5.33

[2] "Rani Susan Oommen Sree Buddha" "A Survey of Copy-Move Forgery Detection Techniques for Digital Images" International journal of innovations in engineering and technology (IJIET).

[3] "Bharat M. Prajapati and Nirav P.Desai" "Forensic analysis of digital image tampering" International Journal For Technological Research In Engineering

Volume 2, Issue 10, June-2015.

[4] "S. A. Fattah M.M.I. Ullah. M.Ahmed I. Ahmmed and C. Shahnaz ""A Scheme for Copy-Move Forgery Detection in Digital Images Based on 2D-DWT"

[5]"K.Kiruthika,S.Devi Mahalakshmi, K.Vijayalakshm" Detecting Multiple Copies of Copy-Move Forgery Based on SURF" ISSN (Online): 2319 -8753ISSN (Print) : 2347 -6710 International Journal of Innovative Research in Science, Engineering and Technology Volume 3, Special Issue ,3, March 2014

[6]"Rajdeep Kaur and Amandeep Kaur" A Review on Copy Move Forgery Techniques" International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 .6, No.2, Mar-April 2016.

[7]"Muhammad Hussain and Sahar Qasem " "Evaluation of Image Forgery Detection Using Multi-scale Weber Local Descriptors [2015]" International Journal of Artificial Intelligence Tools 24(4) · August 2015 with 24 Reads DOI: 10.1142/s0218213015400163

[8]"Hitesh Batra, Dr.Sanjay Badjate" ,A Review on Copy Move Forgery Techniques, International Journal of Advanced Research in Computer and Communication Engineering" Vol. 4, Issue 7, July 2015.

BIOGRAPHIES

Rajni has received B.Tech degree in Electronics and Communication Engineering from Shaheed Udham Singh of Engineering and Technology, Tangroain Punjab Technical University, Jalandhar, Punjab. She is currently pursuing M.Tech degree in Electronics and Communication Engineering from Doaba Institute of Engineering and Technology, I.K.Gujral Punjab Technical University, Jalandhar, Punjab.