International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 3, May-June-2021, ISSN (Online): 2395-566X

A Implementation of Digital Image Forgery using DWT and SIFT Features

Research Scholar Chavi Rana, Asst. Prof. Gyanendra Kumar Singh
Dept. of Computer Science
Sunder Deep Group of Institutions,
Ghaziabad

***Abstract*- The use of digital photography has increased over the last few years and this trend has opened the door for image forgery. Image forgery has become a central issue in many applications. Common techniques used to create fake digital images (copy-moving images) Existing systems integrate block-based and key point-based forged detection in this work methods DWT extraction and SIFT Features with SLIC super pixel segmentation algorithms is proposed to detect the forgery area from the dataset. Existingwork can roughly indicate suspicious, forged areas. The proposed system approach reduces image debugging increase the accuracy and detects copy-moving image forgery region. The most important contribution of this proposed work is to use local termination criteria for each cluster to avoid cluster and image region audits, and there have been no major changes since the last iteration. Adaptively, the algorithm divides the host image into non-overlapping and irregular blocks, extracts function points from each block, and matches the block functions to each other to locate the selected function points. An effective method of detecting image forgery is proposed. This simulation executed in MATLAB simulation.**

***Keywords*- Image Forgery, DWT, SIFT Features, SLIC, Feature Extraction.**

I. INTRODUCTION

The significant advantage of the digital image is they do not deteriorate from the time of capture. The progress in digital photography in the recent decades amplified the use of pictorial information and has become easier due to advances in digital photography.

The mobile phone camera is becoming very familiar and we know the impact of it in day to day life. But the question ascends with this growing world, where malicious attacks are made in every possible filed, is it acceptable to believe which is seen. The surety to check whether the image is original is obligatory. The authenticity of the image is important since it is the information.

As the world conquers technological development, confidence in digital imaging technology falls. In everyday life, people will see fake or counterfeit images from tabloid magazines for business. In addition, fake images in the media, scientific journals, political activities, courts and photo scams that fall into our email boxes are more and more often displayed in unique ways, failing to identify fake images with the required complexity.

The nominal progress from film photography to digital photography is possible, but not reliable. After recording, traditional movie photos cannot be edited, while digital photos can be edited and edited. On the contrary, with the encouragement of today's computer technology, more complex software (such as Adobe Photoshop, Corel Draw or Gimp) can be used to change the original image and thereby manipulate the image. Image editing has a long history of [1] Seen from digital works, image memory can be considered a creative work, but in some cases the manipulated images are maliciously abused.

This serious situation occurs when the images appear to be evidence of medical reports, crime scenes, etc., where the falsified images cause the death of the patient and the criminal escape respectively. [2-3] The falsification of the original image led to illegal distribution, causing the data hunger problem. In the submitted research report, the data owner was careful to publish images without ownership and copyright, which reduced the researcher's data availability.

Due to image falsification, many problems have also emerged in various fields. Some of the recognized examples of the image forgery are listed below; as per the survey conducted by the Wall Street Journal, in the USA 10% of the color photographs published in the magazines, newspapers etc. are digitally altered and retouched.

In scientific community has also been subjected to the image forgeries. Here, the result of a research work is retouched and reused by a different researcher leading to patent problem. Authenticity and integrity of the digital images are well-thought-out to be important to overcome these issues because of the forging in fields such as forensic, medical imaging, e-commerce, industrial photography, etc.

The authenticity verification check of the image is popularly used where the images are considered to supporting evidences, historical records, insurance claims, etc. Because of the drastic increase in the software availability for the advanced image manipulation and processing, the original images are tampered i.e. altered and modified without leaving any trace for forgery detection.

This results in revising the old saying "A picture is worth a thousand words" to "A picture unworthy a thousand true words". The semantic information of an image is altered by addition or extracting information from the image. In order to achieve the image forging, numerous ways are used by the forgers.

In general, there exist different types of the image forgery. The categorization of the types of image forgery is a tedious task; this is because the forgery types are grouped based on the process involved creating the fake image.

But in the current technical world, new innovations are made in the digital photography, which ascend new malicious forging techniques day by day. However, based on the existing types, a categorization is made in this research explaining different types of the image forgery [5] [10]

Statement of Problem Passive approaches based detection technique are applied for the image forgery detection since it is more advantageous than the active approaches which utilize prior knowledge about the image for the authentication. The passive approaches acceptance with computational risk is considered tolerable because of its capability to detect the fake images forged with any image forgery. However, the forgery image with shadow and reflection inconsistencies always appears to be a problem. The major challenges in this research are

II. LITERATURE REVIEW

Mobile forgetting is the most common form of forgetting. For monitoring the writing process, a wall-based approach and a keypoint-based approach can be used. I, keypoint-based features are selected because the difficulty of following them is lower than that of block-based features.

The four different optimization algorithms based on the main points, namely, SURF, KAZE, Harris corner and BRISK, are estimated to test their effectiveness in tracking copying events. The methodology consists of four steps: image preparation, interesting detector, vector description and feature mixing.

The results are compared to the true, the number fl, and the accuracy, which is calculated using a single strategy in the matching algorithm. It can be concluded that in all practical directions the KAZE function can provide the best results, and since the Harris corner is not aligned and the corners are detected instead of the corner, the Harris corner is not suitable for operation. [6-7]

Navdeep Kanwal (et. al. 2019) Multimedia security is one of the key challenges in today's world, as dependency on multimedia information is increasing day by day. Easily available image editing software has enabled every common user of a smart phone and computer, to hack into the information of the images and video and alter it to some extent. To authenticate the genuineness of images, detection of image tempering is need of the time. Various techniques have been proposed to use image features for detection of image forgery.

The techniques of forgery detection work in two domains of image forgery; copy-move forgery detection (CMFD) and image splicing detection (ISD). This paper presents a comprehensive comparative analysis for the use of local texture descriptors i.e. local binary pattern (LBP) and local ternary pattern (LTP) for forgery detection in an image.

The paper also presents a technique to integrate fast Fourier transform (FFT) with local texture descriptors for image forgery detection using existing block-based methodology. Performance of the technique(s) and descriptor(s) is tested for benchmarked dataset CASIA v1.0. Results are evaluated by using standard detection metrics detection accuracy and recall. The paper also suggests a relatively better texture descriptor. [1]

Gul Muzaffer et.al (2019) Because the image processing program is so easy to use, forgetting the action is the simplest way to change the image, which aims to copy or delete the objects in the image.

How to fix this fake product is divided into: a keypoint-based, user-friendly method that uses manual operation. There is a new forgetfulness tracking strategy based on deep learning. AlexNet's existing training model is used to break down the image vectors by fully rotating the image. After the feature was acquired, the similarities between the feature vectors were learned to find and construct the memory. [7]

B Chaitra et al. (2019) with the significant development of digital image processing software tools and their propaganda has enabled users to easily manipulate and convert digital images. Digital photography sometimes establishes essential principles and creates useful evidence in various fields such as forensic investigations, criminal investigations and legal investigations, medical imaging, and news. It raises questions about the origin, legality and security of digital photography.

This article first introduced new image processing technologies, tools for writing, and discussed strategies for introducing various image processing technologies. [9]

III. PROPOSED SYSTEM

There are two main goals of any forgery detection algorithm; firstly, reducing complexity represented in execution time, and Secondly, increasing the algorithm accuracy against different processing operations used in copy-move forgery. There are main steps which any copy-move forgery detection algorithm performs.

First, gray-scale conversion is applied by combining the red, green, and blue channels to operate in a form of a gray-scale image. The second division operation is performed based on two types of classification; pixel-based type and block-based type Third, image processing transformations are applied to extract the image features. A descriptor or classifier is used to calculate the feature vectors as noise distribution, color, light, shadow, resolutions, or edges.

Finally, a lexographical representation is used as a map to examine the image feature vectors to compare values and match the identical ones. The block diagram in Figure 1 shows the copy-move operation methodology. Splicing Image Forgery Detection using Wavelet Decomposition. In this method first step is to apply Wavelet Decomposition on the forged image then perform block matching operation after that detect duplicated regions. Copy-move and splicing are the common picture manipulation techniques, if these manipulations are done with very carefully then no one can identify visually. Some researchers have proposed several techniques to identify these manipulations.

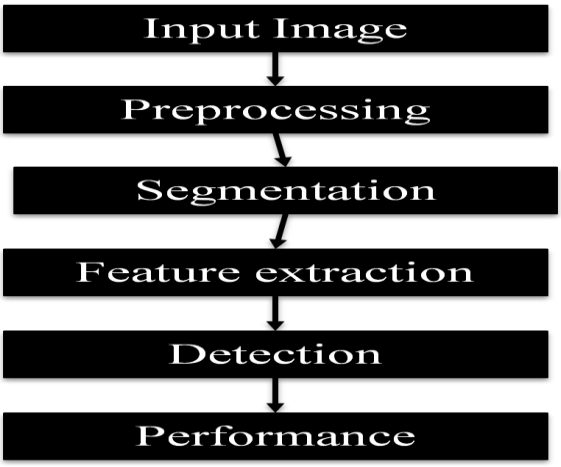


Fig 1. Proposed Flow Diagram.

1. Input Image:
An image is a rectangular array of values (pixels). Each pixel represents a measure of certain attributes of the scene measured over a limited area. There may be many of this attribute, but we usually measure the average brightness (one value) or brightness (three values) of the image filtered through the red, green and blue filters. These values are usually represented by eight-bit integers that provide 256 brightness levels. We're talking about the resolution of an image: this is defined by the number of pixels and the number of brightness values.

Image resolution can be measured in many ways. Resolution quantifies the close distance between lines and is still clearly visible. Resolution units can be related to physical dimensions (e.g., lines per mm, lines per inch), For example, an image consisting of 200 rows and 300 columns of dots of different colors is stored in a 200 x 300 matrix. Some images (such as RGB) require a three-dimensional matrix where the first plane of the third dimension represents red pixel intensity, the second plane represents green pixel intensity, and the third plane represents blue pixel intensity.

2. Preprocessing:
Image Resize: In computer graphics and digital imaging, image scaling refers to adjusting the size of digital images. In video technology, the expansion of digital materials is called expansion or resolution enhancement. When scaling vector graphics, you can use geometric transforms to scale the graphic primitives that make up the image without degrading the image quality. When scaling a graphic raster image, a new image with a higher or lower pixel count must be generated. When you adjust or deform an image from one pixel grid to another pixel grid, image interpolation occurs.

When you need to increase or decrease the total number of pixels, you need to adjust the image size, and when you correct lens distortion or rotate the image, re-alignment may occur. Scaling refers to increasing the number of pixels so you can see more details as you scale the image.

Interpolation is performed using known data to estimate the value of unknown points. Image interpolation works in both directions and tries to obtain the best pixel intensity approximation based on the values of the surrounding pixels. Common interpolation algorithms can be divided into two categories: adaptive and non-adaptive. The adaptive method will vary depending on its interpolated content, while the non-adaptive method will treat all pixels equally.

3. Feature Extraction:
Scale Invariant Function Transformation SIFT -The block function extraction process is used to calculate the similarity of the functions extracted from the block region based on scale invariant function transformation process (SIFT). This process identifies key points from the image.

The main points extracted from the block are matches based on the calculated distance. The SIFT extraction process is as follows. Calculate the derivative of the image. The calculated value gives the change in the color and gray value of the image and indicates the information in the image. The Laplace function calculates the edge of

the image based on the derivative. Then arrange the values in matrix format in order. First, select the value in the specific circle area. The value in the selected area expands. During the expansion process, the values are compared and the value with the lowest value is combined. Then the value with the smallest value is deleted.

IV. SIMULATION RESULTS WITHOUT FORGERY IMAGE

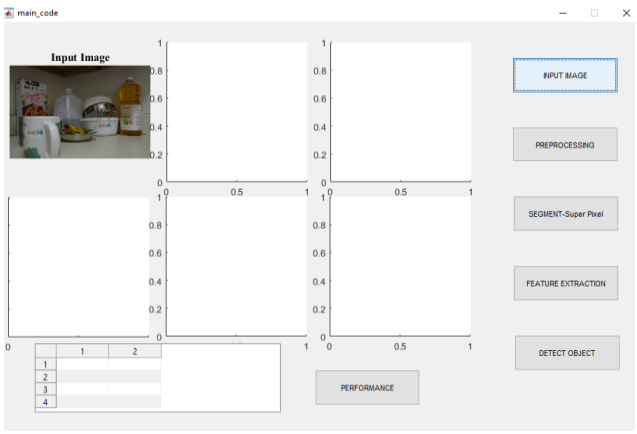


Fig 2. input image GUI window.

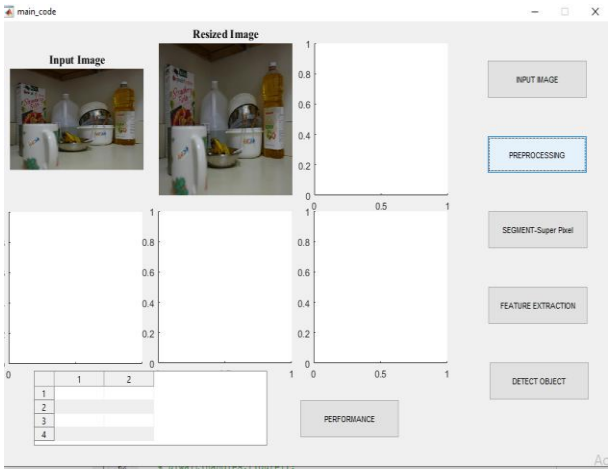


Fig 3. Resized Image GUI window.

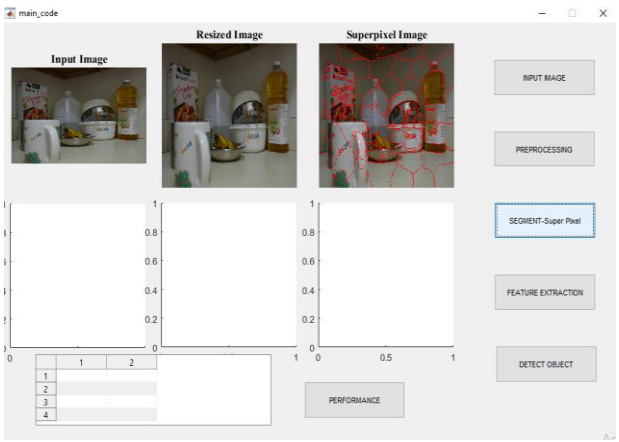
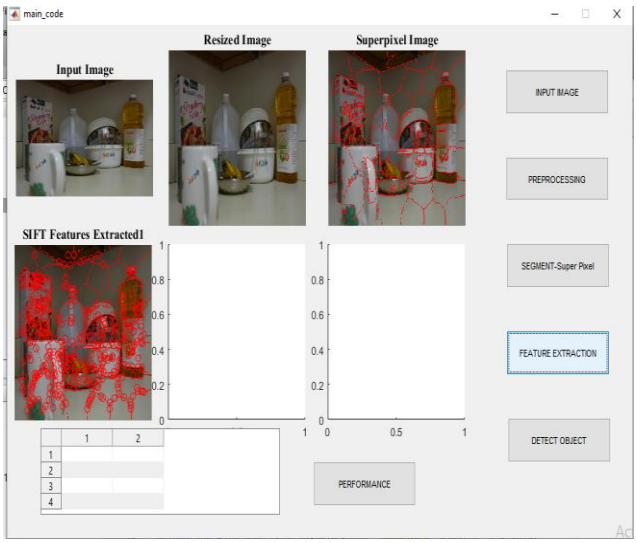


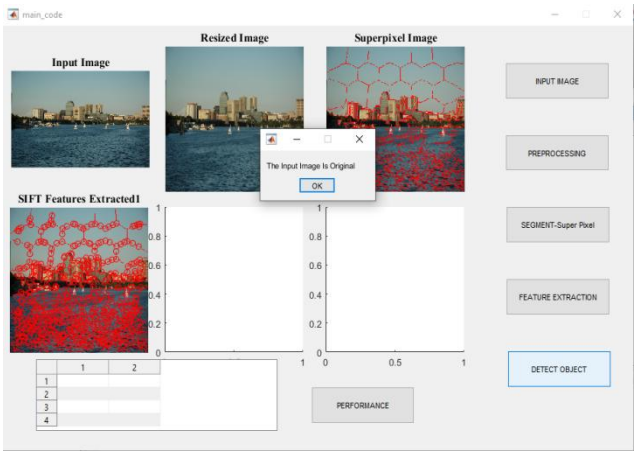
Fig 4. Superpixel Image GUI window.

The process of extracting segmentation functions and feature customization can be used to identify copy-insert forgery in the input image. Initially, the input image was over segmented using SLIC algorithm.

Based on scale-invariant feature extraction algorithm (SIFT) to extract functions from each block. From the extracted functions, falsification is detected based on block matching and labeling of function point matching..



(a)



(b)

Fig 5. SIFT Feature Extraction original image GUI window.

V. RESULT WITH FORGERY DATASET

There are many considerations when extracting these features and how to record them. SIFT image functions provide a set of functions of an object unaffected by the many complexities encountered in other methods (such as object scaling and rotation). While allowing objects to be recognized in larger images, the SIFT image feature also allows objects in multiple images at the same location (taken from different locations in the environment).

Fig 6. Detected Forgery Image GUI window.

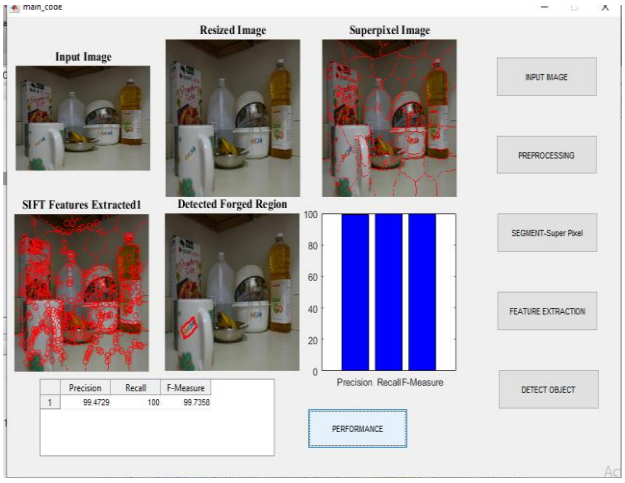


Fig 7. Performance Evolution GUI window.

Table 1. Perforamnce Parameters.

	Dataset	Precision	Recall	F-Measure
Normal Forgery	Dataset 1	97.80	100	98.20
	Dataset 2	99.41	100	99.50

VI. CONCLUSION

This paper discusses some important issues related to detect copy forgery image, a new method based on wavelet decomposition and SIFT based feature extraction is proposed, which can process large size images and solve the time complexity problem.

The extracted quality are used to block matching, and with the forensic physician identified in the image, the identified local feature points are matched to identify similar parts in the image. The performance of this process is calculated by performance indicators such as precision and recall accuracy. Our method gives better results than existing systems. Using various image segmentation algorithms can further improve the process.

REFERENCES

[1] Navdeep Kanwal Jaskaran Singh Bhullar Akshay Girdhar Detection of Digital Image Forgery using Fast Fourier Transform and Local Features International Conference on Automation, Computational and Technology Management (ICACTM) Amity University 262 978-1-5386-8010-0/19/$31.00 ©2019 IEEE.

[2] Amanpreet Kaur Savita Walia Krishan Kumar Comparative Analysis of Different Keypoint Based Copy-Move Forgery Detection Methods 2018 Eleventh International Conference on Contemporary Computing (IC3) Year: 2018 ISBN: 978-1-5386-6835-1 DOI: 10.1109/IEEENoida, India.

[3] Taranjit Kaur Akshay Gerhard Geetika Gupta A Robust Algorithm for the Detection of Cloning Forgery 2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) Year: 2018 978-1-5386-1508-9 DOI: 10.1109/ IEEE Madurai, India.

[4] Ali Mumcu Ibrahim SavranCopy move forgery detection with using FAST key points and SIFT description vectors 2018 26th Signal Processing and Communications Applications Conference (SIU) Year: 2018 ISBN: 978-1-5386-1501-0 DOI: 10.1109/IEEE Izmir, Turkey.

[5] H.M. ShahriarParvez Hamid A. JalabAla'a R. Al-Shamasneh Somayeh SadeghiDiaa M. UliyanCopy-move Image Forgery Detection Based on Gabor Descriptors and K-Means Clustering2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)Year: 2018 ISBN: 978-1-5386-4838-4 DOI: 10.1109/IEEEShah Alam, Malaysia.

[6] Umair A. Khan Mumtaz A. KaloiZuhaib A. Shaikh Adnan A. ArainA Hybrid Technique for Copy-Move Image Forgery Detection 2018 3rd International Conference on Computer and Communication Systems (ICCCS) Year: 2018 ISBN: 978-1-5386-6350-9 DOI: 10.1109/ IEEE Nagoya, Japan.

[7] Gül Muzaffer Eda Sena ErdölGüzin UlutaşA copy-move forgery detection approach based on local intensity order pattern and patchmatch2018 26th Signal Processing and Communications Applications Conference (SIU) Year: 2018 ISBN: 978-1-5386-1501-0 DOI: 10.1109/ IEEE Izmir, Turkey.

[8] Khushkaran Kaur Efficient and Fast Copy Move Image Forgery Detection Technique 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS) Year: 2018 ISBN: 978-1-5386-2842-3 DOI: 10.1109/ IEEE Madurai, India.

[9] B Chaitra P.V Bhaskar Reddy A Study on Digital Image Forgery Techniques and its Detection 2019

International Conference on contemporary Computing and Informatics (IC3I Year: 2019 ISBN: 978-1-7281-5529-6 DOI: 10.1109/ IEEE Singapore, Singapore.

[10] Gul Muzaffer Guzin Ulutas A new deep learning-based method to detection of copy-move forgery in digital images 2019 Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT) Year: 2019 ISBN: 978-1-7281-1013-4 DOI: 10.1109/ IEEE Istanbul, Turkey.