DHOLE PATIL COLLEGE OF ENGINEERING, PUNE

DEPARTMENT OF INFORMATION TECHNOLOGY

Review on

Image Copy-Move Forgery Detection System.

Presented by -

Pranav Tripathi

Sohail Shaikh

Shreya Srivastav

Samriddhi Sharma

Guided by -

Prof. Shriganesh Mane

Contents

- Introduction.
- Problem Statement.
- Scope.
- Objective.
- Literature Survey.
- Software & Hardware Requirements.
- System Architecture.
- Algorithm & Technology Used In Project.
- Advantages & Disadvantages.
- Flow Chart.
- Conclusion.
- References.

Introduction

- Images have an essential role as effective carriers of information in technology. Through using various advanced imaging devices like smartphones, huge amount of highresolution digital images are taken and exchanged through people daily. There are different types of manipulations that cannot be easy to observed which effect on the images. The manipulation may either add, delete or alter any of the properties of the image, without offering any hint as to the update. Therefore, recently, digital image forgery detection has become an active research field.
- There are several copy-move image forgery detection (CMFD) techniques based on transform domain.
- IC-MFDs rely on five stages: Image pre-processing, dividing the image, computing the mean and standard deviation statistical features of each block, Sorting the feature into matrix, then feeding the feature vector to the SVM classifier to identify the image as authentic or forged.

Problem Statement

Low Robustness: **Robustness** is the property of being strong and healthy in constitution. When it is transposed into a system, it refers to the ability of tolerating perturbations that might affect the system's functional body.

Domain Name: Artificial intelligence.

Scope

1. **Pixel-based image forgery detection:**

Pixel based techniques focuses on the pixels of image and finds the statistical anomalies at the pixel level. These techniques are further categorized: Image Resampling, Image Splicing, Copy-Move forgery.

2. Format-based image forgery detection:

Format based techniques are based on image formats and works mainly in JPEG formats. Format based techniques can detect forgery in the compressed images. These techniques can be divided into three types: JPEG Quantization, JPEG Blocking.

3. Camera-based image forgery detection:

When the image is captured from a digital camera, the image moves from camera sensor to memory. It has to undergo a series of processing steps that includes Quantization, White balancing, Filtering, JPEG compression etc. these techniques can be divided into four categories: Chromatic Aberration, Sensor

4. **Physical environment-based image forgery detection:**

Consider the creation of an image by splicing together two individual images captured at different places. Here is often difficulty arise to exactly match the lighting effects under each image was originally photographed. These lightening differences can be used as evidence of forgery. Physical environment based techniques works on the basis of lightening environment. These techniques are categorized as: Light Direction 2-D, Light Environment, Light Direction 3-D.

5**. Geometry-based image forgery detection:**

Geometry based methods make measurement of objects in the real world and their position relative to the camera. Geometry based methods are: Principal Point, Metric Measurements.

Objective

- Image Resampling: It is considered to be less harmful kind of forgery. Image Resampling do no change the image, it only reduce or enhance the features of image. This technique is most popular among Magazines, Newspaper photo editors. This is not proven ethically wrong. It includes rescaling, resizing, rotating the image etc.
- Image splicing: Image splicing is defined as a paste-up produced by sticking together photographic images. Image Splicing is a technique which involves composite of tw or more images to create a new fake image. Image Splicing is more aggressive than the Resampling.
- Copy-Move forgery: it is the most common kind of forgery technique in which one part of image is copied and pasted into different location of the same image in order to hide information or to change the meaning of image; hence a strong correlation exists between these that can be used as an evidence to detect copy-move forgery.

Literature Survey

K. Kiruthika et al. used the key point based method SURF(Speeded Up Robust Features) for feature extraction. The g2NN strategy is done for identifying the matched points and hierarchal clustering is done on matched points to reduce false detection rate. Takwa Chihaoui et l. proposed a method that automatically detect duplicated regions by identifying local characteristics of the image using SIFT (Scale Invariant Feature Transform) and by using SVD (Singular Value Decomposition) for matching between identical features. This hybrid method is robust to Geometrical Transformations and able to detect with high performance duplicated regions. Sudhakar. K et al.

Software & Hardware Requirements

HARDWARE REQUIREMENTS:

- System : Pentium Dual Core.
- Hard Disk : 120 GB.
- Monitor : 15” LED
- Input Devices : Keyboard, Mouse
- Ram : 1GB.

SOFTWARE REQUIREMENTS:

- Operating system : Windows 7.
- Coding Language : MATLAB.
- Tool : MATLAB R2013A/2018

Algorithm Used In Project

Duplication Detection Algorithm:

The technique of discovering separate or many references to a same real-world thing or object is known as duplicate detection. Even if it has a different picture size, file format, or other
changes to its look, an image can be identified as a duplicate. Furthermore, the image's semantic
content can be used to circumvent the constraints of perceptual hashes. The steps of the algorithm that we used this as a model for our system are listed below.
Step 1: Dividing the suspicious image into fixed-size blocks.
Step 2: DCT is applied to each block to generate the quantized coefficients.
Step 3: Representing each quantized block by a circle block and extracting appropriate features
from each circle block.
Step 4: Searching similar block pairs.
Step 5: Finding correct blocks and output them.

Basic Flow Chart Of Algorithm

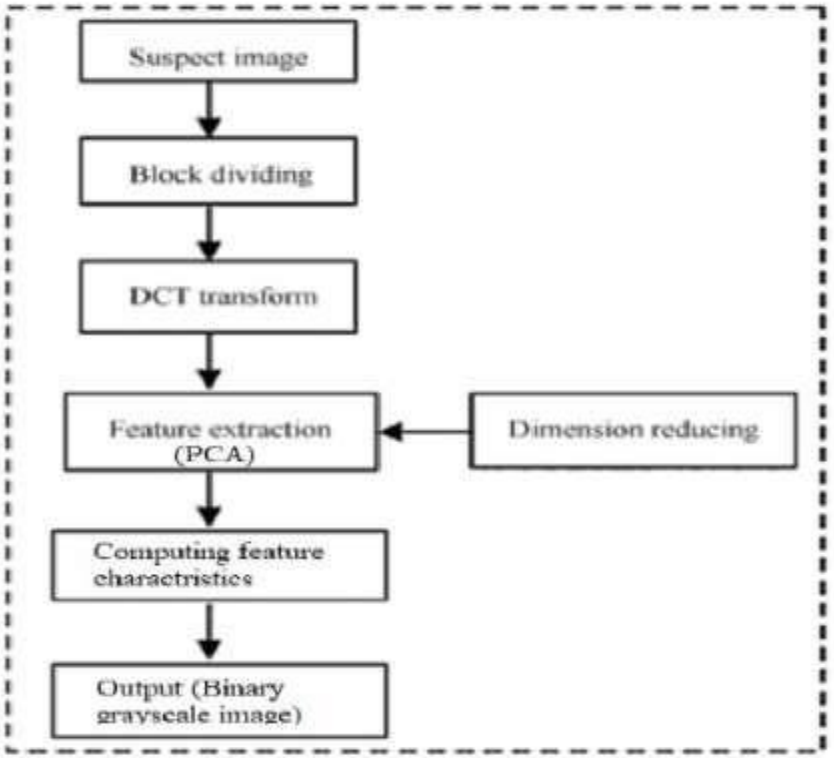


Figure 1: Flow diagram for Duplication Detection Algorithm

Advantages/Disadvantages

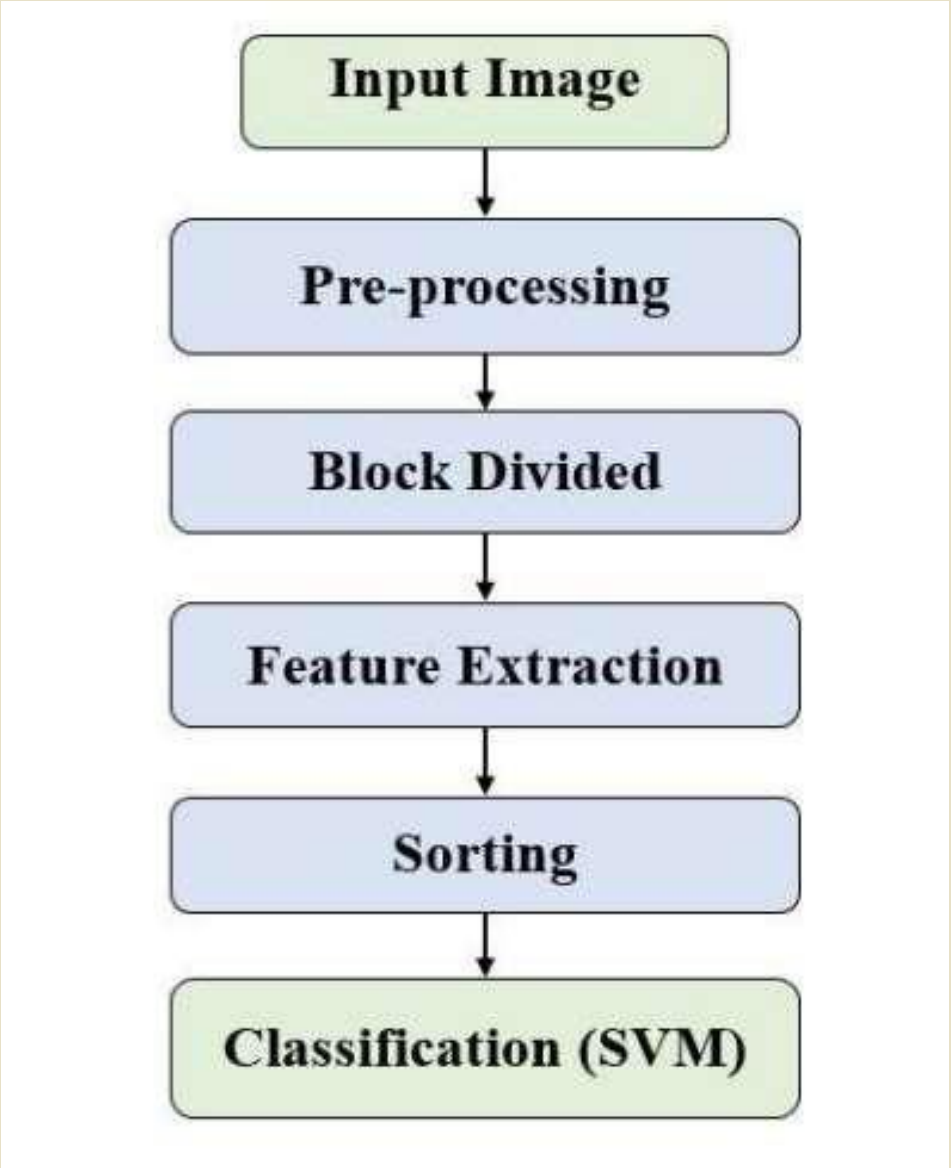
Advantages:

- **Computational complexity is less.**
- **Efficient for real time applications.**
- **False matches are less.**

Disadvantages:

- **Unable to differentiate copy paste region of image.**
- **It cannot be used for color images.**
- **Not robust against scaling.**

Flow Chart


Input Image
Pre-processing
Block Divided
Feature Extraction
Sorting
Classification (SVM)

Conclusion

- The proposed IC-MFD consists of five steps: image preprocessing, dividing the image into overlapping blocks, determining the statistical features mean and standard deviation of each block, sorting the feature into a matrix, then feeding the feature vector to the SVM classifier to classify the image as authentic or forged.
- Our experimental findings show that copy-move forgery can be successfully detected by the proposed IC-MFDs with high accuracy (98.44 %). We compared the results of our proposed ICMFD with many current CMFD methods. The findings revealed that our proposed produces higher outcomes than others. We plan to expand the application of our proposed in the future to distinguish other kinds of image forgeries, such as splicing.

THANK YOU!