International Journal of Advanced Engineering & Innovative Technology (IJAEIT)
ISSN: 2348 7208
ISRA IMPACT FACTOR: 0.42

Image analysis and forgery Detection

Kuldeep S. Pawar, Yogesh S. Satav, Pandurang V. Shinde, Tejas R.Gadgil

Guided by Prof. Poonam. S. Toke

Abstract- In early years, photography quickly became the chosen method for making portraits, and portrait photographers learned that they could improve sales by retouching their photographs to please the sitter. Photo manipulation has become more common in today's age of digital cameras and image editing software. But the main problem is that if one person sends the image over network so many chances to forge the image & send to the receiver. So in that case receiver can't receive the original image. So this software is useful for avoiding the forgery. It can also provide security. This software checks the original image and forged image using some techniques and recovers the original image as well.

Keywords- Steganography, Watermark, DCT Evaluation, αchannel.

INTRODUCTION

The art of making an image forgery is almost as old as photography itself. In its early years, photography quickly became the chosen method for making portraits, and portrait photographers learned that they could improve sales by retouching their photographs to please the sitter. Photo manipulation has become more common in the age of digital cameras and image editing software. Gathered below are examples of some of the notable instances of photo manipulation in history. So we focus here on the instances that have been most controversial or notorious, or ones that raise the most interesting ethical questions. The photographers have also experimented with composition, i.e., combining multiple images into one. Digital images offer many attributes for tamper detection algorithm to take advantage of specifically the colour and brightness of individual pixels as well as an image's resolution and format. These properties allow for analysis and comparison between the fundamentals of digital forgeries in an effort to develop an algorithm for detecting image tampering. This paper focuses on images saved in the jpeg format.

Therefore a research work on basis of compression .scheme is discussed to determine what information can be gathered about a digital forgery saved in this format. Other fundamental properties of any digital forgery are used to develop additional detection technique such as direction filter, which is used to detect the forgery region when we conduct the experiments on gray level of photos. In this paper, we propose a novel scheme for identifying the location of copy-create and copy move supported tampering algorithms and authenticating an image by applying the jpeg block and direction filter techniques.

RELATED WORK

Fridrich *et al.*, proposed a faster and more robust approach for detecting duplicated regions in images [1]. The authors use a sliding window over the image and calculate the discrete cosine transform (dct) for each region. Each calculated dct window is stored row-wise in a matrix. In order to perform matching for non-exact cloned regions, lexicographically sorting matrix and searching for similar rows are finished. Johnson and Farid investigated lighting inconsistencies across specular highlights on the eyes to identify composites of people. The position of a specular highlight is determined by the relative positions of the light source, the reflective surface and the viewer (or camera). Ac-

Kuldeep S. Pawar, Yogesh S. Satav, Pandurang V. Shinde, Tejas R.Gadgil, Reserach students of Padmabhooshan Vasantdada Patil Institute Of Technology, Bavdhan , Pune 411 021

cording to the authors, specular highlights that appear on the eye are a powerful clue as to the shape, color, and location of the light source(s). Inconsistencies in these properties of the light can be used as telltales of tampering. Ng and chang proposed a feature-based binary classification system using high order statistics to detect image composition. Bayram *et al.*, framed the image forgery detection problem as a feature and classification fusion problem. The authors develop single weak "experts" to detect each image processing operations.

II.Techniques

A. DCT Evaluation

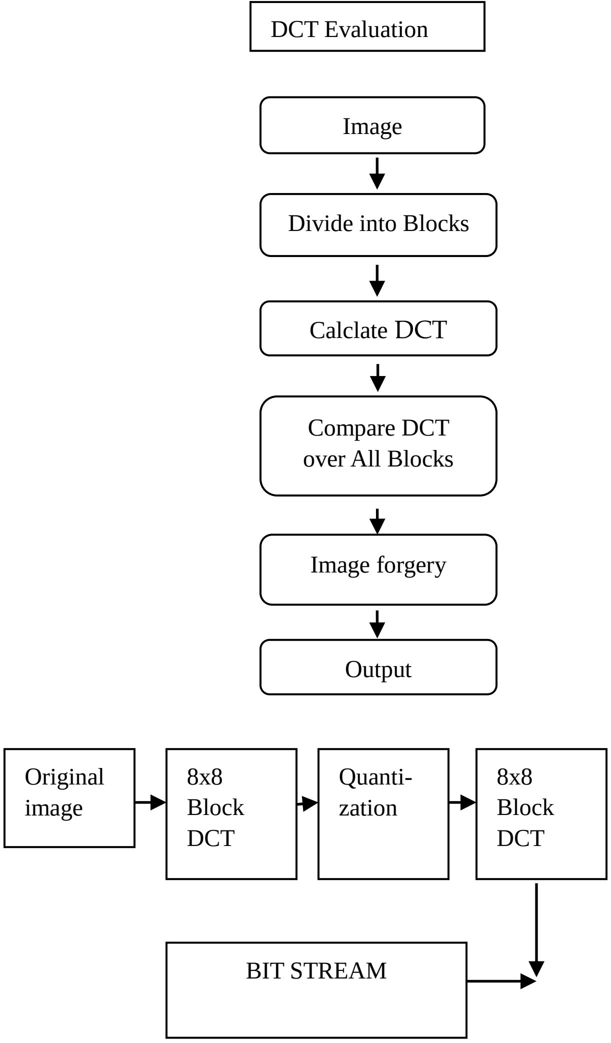


Fig.1 DCT Evaluation

The DCT domain is used to convert a signal into coefficient values with the ability to perform truncating and rounding operations, thus allowing compression of this signal to take place. The JPEG compression process starts by calculating the DCT of each 8x8 blocks in the image based on the following formula:

$$Di,j = \sum_{K,j=0}^{7} akl(i,j)\ Bkl$$

The quantized coefficients, Dij, are then arranged in a zigzag order, encoded using the Huffman Algorithm, and inserted into what makes up the JPEG file.

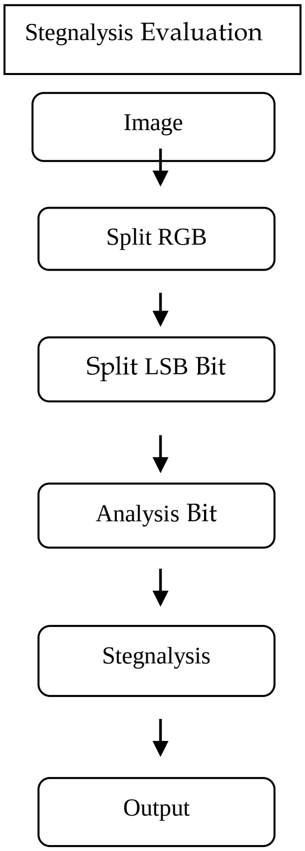
Decomposition works similarly just in reverse order. By rounding the ratio above, an integer value is obtained and thus allows an image to be compressed. A threshold is set to determine what integer values should effectively be discarded. The parts to be discarded are carefully calculated based on a "Quality Factor", which is a reference number between 0 and 100. The higher the Quality Factor, the less compressed and the better quality the image is. A trade-off between file size and image quality is always necessary in this type of lossy compression.

B. STEGNOANALYSIS

Steganography is a technique of communicating between sender and a receiver over a communication channel by hiding the relevant information in the cover media so that avoiding the information to be exposed to an intruder. A possible carrier of secret information is applied to media such as images, text, video clips, music and sounds. The process of detecting stenographic messages is known as steganalysis and particular steganalysis techniques called an attack.

Steganalysis can be viewed as a two-stage process:

Classification of an image as being stego-bearing or not, and 2) Finding the location of steno-bearing pixels (i.e. the pixels containing the hidden message bits) with an aim to extracting, manipulating or sterilizing the message is applied to media such as images, text, video clips, music and sounds.



Data Hiding Algorithm

The difference between our application and the other programs implementation on LSB embedding is that our application ranks the seeds based on their suitability as cover images for our data. In our scheme we are using L.F.S.R's to generate random permutations of binary string. Details about rL.F.S.R. In this, any random number generator can be used to permute the string instead of L.F.S.R's but information of the generator should also be communicated along with message. In the application the user first specifies the data that they would like to hide is in any file format, and encrypts this data using the recipient's El Gamal public key. Once the encrypted data is obtained, follow the below procedure.

2. Encryption Algorithm

As mentioned previously, the secret information is first encrypted using El Gamal Cryptosystem. The encryption process before hiding it provides defense in depth and makes job of the attacker more difficult to recover the secret data. The application uses the El Gamal cryptosystem, mainly for two reasons. First, it eliminates the need for a private shared key between the sender and recipient. A public key of a person can be distributed easily by emailing, or publishing it on a website. Second, the El Gamal encryption is the most extensively used as an alternative to RSA. There is no known polynomial-time algorithm, if prime (p) is carefully chosen and is a primitive element modulo (p).

III.DIFFERENT IMAGE TYPES

• COLOR – GRAYSCALE - BLACK & WHITE

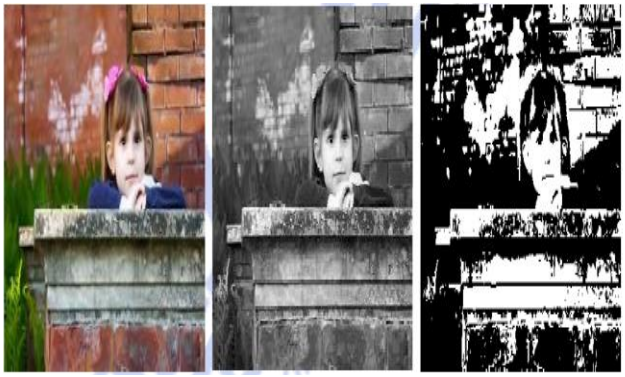
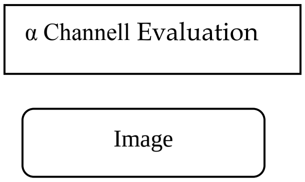
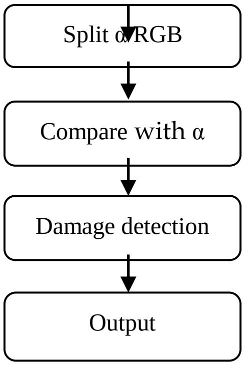


Fig.2 Image in different colors

1. RGB To Grayscale Conversion
   - Steps / Algorithm
2. Traverse through entire input image array.
3. Read individual pixel color value (24-bit).
4. Split the color value into individual R, G and B 8- bit values.
5. Calculate the grayscale component (8-bit) for given R, G and B pixels sing a conversion formula.
6. Compose a 24-bit pixel value from 8-bit grayscale value.
7. Store the new value at same location in output image.

C.Alpha channel





Data hiding represents a class of processes used to embed data, such as copyright information into various forms of media such as image, audio, or text with a minimum amount of perceivable degradation to the "host" signal; its goal is not to restrict or regulate access to the host signal, but rather to ensure that embedded data remains inviolate and recoverable. A watermarking technique makes use of a data hiding scheme to insert some information in the host image, in order to make an assertion about the image later. In this paper, data hiding scheme simply means the technique to embed a sequence of bits in a still image and to extract it afterwards. Watermarking techniques can be classified as either "robust" or "fragile." Robust watermarks are useful for copyright and ownership assertion purposes. They cannot be easily removed and should resist common image manipulation procedures. On the other hand, fragile watermarks (or authentication watermarks) are easily corrupted by any image processing procedure. However, watermarks for checking the image integrity and authenticity can be fragile because if the watermark is removed, the watermark detection algorithm will correctly report the corruption of the image.

Data Hiding Scheme

This technique ensures that for any pixel that is modified in the host image, its visibility is very less. Thus, the existence of secret information in the host image is difficult to detect. The data hiding scheme is very simple. In each block, the position of the pixel to be used for hiding the information is fixed, that is, the middle pixel. Hence the complexity is not in identifying the position, but in identifying the sub-blocks that are ready to hide the information. Since the middle pixel is used to hide the information always, another level of security is introduced by shuffling of the Roadblocks. This provides another advantage also. It distributes the hidden information in all parts of the image. It is an efficient and effective tool to equalize uneven embedding capacity.

CONCLUSIONS

The main focus on methods to detect digital forgeries created from multiple images called as copy-create image forgeries. Some forgery images that result from portions copied and moved within the same image to "cover-upon something is called as copy-move forgeries. Therefore, the experimental design and analysis herein focuses on copy-create and copy-move image forgeries. A crafty individual, who wants to perfect an image forgery, with time not a factor, can usually give any detection method trouble. If image tampering occurs in a compressed then JPEG Block methodologies is to support and predict forgery region along with different image format at the same time uncompressed image and then that image is converted to the JPEG image format, the JPEG Block Technique will fail to capture evidence of tampering. This conversion process destroys all proof of tampering since the original tampering does not affect any JPEG blocks. Additionally, any image tampering performed on an image prior to an image size reduction will eliminate detectable anomalies for the direction filter technique. The remainder of the test images returns definitive signs of image tampering when using the JPEG Block Technique for analysis. This method captures the forged area after using various threshold values for testing. The larger threshold value effectively filters out the false positives caused by edges since tampering with an area on the image usually causes greater variability in the JPEG blocks. Consequently, if no pattern arises using different threshold values, the image is most likely authentic or requires analysis by other methods. Overall, the JPEG Block Technique shows promise when used to test an image for tampering. A multifaceted approach is the best practice to follow to decide if an image is forged or authentic when direction filter is used as evidence of tempering.

REFFRENCES

[1] J. Fridrich, D. Soukal and J. Lukas, "Detection of Copy-Move Forgery in Digital Images", Proceeding of the Digital Forensic Research Workshop, **(2003).**

[2] M. K. Johnson and H. Farid, "Exposing Digital Forgeries through Specular Highlights on the Eye", Proceeding of the 9th International Workshop on Information Hiding, Saint Malo, France, **(2007)**, pp. 311-325.

[3] T. -T. Ng and S. -F. Chang, "Blind Detection of Photomontage using Higher Order Statistics", Proceeding of the 2004 IEEE International Symposium on Circuits and Systems, Vancouver, BC, Canada, **(2004)**, pp. V-688-V-691.

[4] S. Bayram, I. Avcibas, B. Sankur and N. Memon, "Image Manipulation Detection", Journal of Electronic Imaging, vol. 15, no. 4, **(2006).**

[5] M. Chen, J. Fridrich, J. Lukas and M. Goljan, "Imaging Sensor Noise as Digital X-ray for Revealing Forgeries", Proceeding of the 9th International Workshop on Information Hiding, **(2008)**, pp. 342-58.