Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 03, March-2016

An Empirical way for Detecting and Comparing Image Antiforensics

D. Dharani
Information Technology
Anna University Regional Campus
Coimbatore, India

Dr. P. Marikkannu
Information Technology
Anna University Regional Campus
Coimbatore, India

Abstract - The generation depends upon the digital images to share their visual information. Nowadays one of the principal ways of communication is digital visual media. In this digital world all types of advancement are become possible and at the same time the motivation to make manipulation of images also increases simultaneously. This kind of image Antiforensics is increasing constantly. Hence in the digital image communication the main problem is its authenticity. In order to verify the image integrity, authentication, and tampering detection a number of forensic techniques have been developed. There are many categories in the existing image forensic system there is still an increase in image Antiforensics. The two techniques namely Copy-Move based and Double compression based on image Antiforensics is focused in the proposed method. The proposed system provides Antiforensic detection algorithms and also compares both the mechanisms based on empirical results.

Keywords: Copy Move image Antiforensics, Double compression image Antiforensics, Antiforensic Detection.

I INTRODUCTION

A. Antiforensics and its Detection

The usage of digital images has been increased with the invention of several image processing technologies. The digital images are handled in many places for different purposes. We are living in an age, where anything can be tampered and misused with the help of new technologies. For decades, photographs and the digital images have been used to document in crime cases and they also have used as an evidence in courts. The process of creating fake image has been tremendously simple with the introduction of modern and powerful editing software which are freely available such as Photoshop, Picasa, and Corel Paint Shop. It can also be achieved using software code with image processing tools. Sometimes it is difficult to identify the tampered portions of the fake image. The detection of forged portions is of much important to maintain the originality of an image. In the proposed system, the survey has been done on existing techniques and it highlights copy–move detection and Double compression detection methods based on their robustness.

B. *Image Processing*

Image processing is manipulation of images or objects using mathematical operations for which the input is an image, series of images or a video, such as a photograph or video frame. There are varieties of image operations. For example, Image enhancement is to reduce the noise and to sharpen the details using which the enhanced image can be retrieved from the dark image. Image restoration is to improve the quality of an image using which the blurred image can be restored. Image compression eliminates the redundancy to transmit and store the images with minimized size. The images can also be manipulated or tampered using digital image processing techniques. Such image manipulations can be termed as Image Antiforensics or Image forgeries. The image Antiforensics can be broadly categorised into two classes such as active approach and passive approach. Active approach deals with pre embedded details such as digital watermarking and digital signatures. The passive approach deals with tampers such as copy-move image forgeries and splicing and so on.

Copy-Move image forgery is to copy an object from the image and pastes it in the same image. These kinds of alterations may confuse the situation of the actual image. Image retouching is actually done with the help of available photo editing applications such as Photoshop, Corel draw to enhance the appearance of an image. Image splicing is as same as that of the copy-move image forgeries. The difference is that the splicing deals with two different images. An object from another image would be copied to the actual image. Double compression based image forgeries deals with the multiple compressions. Single compression can be applied to reduce the size of an image but if it is compressed more than once then we may tend to lose few portions of an object. The two Antiforensic mechanism namely Copy-Move and Double compression based Antiforensics and also its detection are followed in this proposed approach.

In this paper ***Section (2),***deals with the literature review. ***Section(3),***focuses on the proposed method for detecting image Antiforensics and its analysis ***Section(4),***explains the Results of the proposed model which is been developed using Matlab.

II LITERATURE REVIEW

Most of the existing approaches focus on efficient way of applying the image tampers by considering quality of the tampered images as in the case done by Xiaoyu Chu *et al.*[1]. In this system Concealability-rate-distortion trade-

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 03, March-2016

off in anti-forensic systems is proposed. Specifically, the system defines Concealability and characterizes the C-R-D trade-off in double image compression based anti-forensics. To obtain the trade-off, the system proposed a flexible anti-forensic dither to deal with the effectiveness of an anti-forensics and also provided an anti-forensic transcoder to more efficiently accomplish the anti-forensics. Then experimentally characterize the C-R-D trade-off by polynomial surfaces based on whether the secondary quality factor is lower or higher than the first one. From the experimental results two surprising results are derived. The first one is that if the forger recompresses using a lower secondary quality factor, the anti-forensics with greater strength will decrease the data rate. The second one is that the forger is incentivized to recompress with a lower secondary quality factor. This is because the results have proven that, for any combination of Concealability and distortion values achieved by a higher secondary quality factor, the forger might choose a lower secondary quality factor that will achieve the same Concealability and distortion values yet at a lower data rate.

The Copy-Move image Antiforensics is also achieved similarly by Jian Li *et al.[2]*. The system proposes a scheme to detect the copy-move forgery in an image, mainly by extracting the keypoints for comparison. The main difference to traditional method is that the system first segments the test image into semantically independent patches prior to keypoints extraction. As a result, the copy-move regions can be detected by matching between these patches. The matching process has of two different stages. In the first stage, the suspicious pairs of patches that may contain copy-move forgery regions are found. Then the affine transformation matrix is estimated roughly. An Expectation Maximization based algorithm is performed to refine the estimated matrix and to confirm the existence of copy-move forgery in the second stage. However, the re-estimation of transform matrix is more complex.

III PROPOSED METHOD

Two different techniques are to be analysed in the proposed system. SIFT (Scale Invariant Feature Transform) Algorithm is used to detect the Copy-Move Antiforensic technique which constructs a scale space of an image and extracts its key features. SIFT features are generally based on the appearance of an object at particular point of interest. The Key point Localisation is to eliminate edges and low contrast regions which makes the algorithm efficient and robust. Detecting double JPEG compressed images plays an important Role in image forensics and crime detection. In this system we proposed a detection method based on the coefficients of DCT that is expressed in histograms and Support vector machines. At last the comparison and analysis is done between the nature and characteristics of both the techniques.

A. System Architecture

The input of the system is antiforensically modified image. The Antiforensic can be done in many ways. As the objective of the system is to compare and analyze two different techniques such as Copy-Move based and Double compression based Antiforensics. In order to Analyze Experimentally both the Antiforensic techniques are implemented first and then the detection mechanisms are applied. Then the Double compression is applied using DCT (Discrete Cosine Transform) and Quantization. JPEG format is the commonly used format for images. First, the image is separated into 8 by 8 blocks. Within every block, discrete cosine transform (DCT) is applied on the pixel values to obtain the DCT coefficients x_{ij} ,i, j = 0, 1, ..., 7, where x_{ij} is the coefficient in subband (i, j). Then, quantization is applied on each DCT Coefficient using quantization table **Q**, with the elements denoted as q_{ij}. The quantized coefficients are shown in *Eqn(2).*

$$a_{ij} = \text{round}(x_{ij} / q_{ij}), \text{ for } i, j = 0, 1, \ldots, 7. \qquad (1)$$

Finally, for the purpose of transmission and storage lossless entropy coding is applied on the quantized coefficients of DCT. Inorder to forge the image the compression is taken place more than once. The system focuses on double compression. Here the quantization table used for second compression may or may not be the same as that of the first one. Fig.2 shows the sequential steps that are followed in the double compression. The next step is the detection mechanisms which are applied to both of the Antiforensics. At last it will be compared experimentally as shown in the Fig.1. The Forged image is applied for detection based on its type of Antiforensic. The Copy move forged image is applied for sequential steps to detect its forged portions. First the Discrete wavelet transform is applied on the image to identify the discrete values of an image. The image features are to be derived using SIFT feature extraction and the features are to be clustered and matched based on its similarity. At last the copy move forged portions will be detected. If the image is tampered using double compression then the DCT is being applied in tampered image and histograms and Fourier transform will be calculated. Based on the support vector machine the double compression forgery will be identified. At last, the two detection mechanisms are to be compared and analyzed to determine its features.

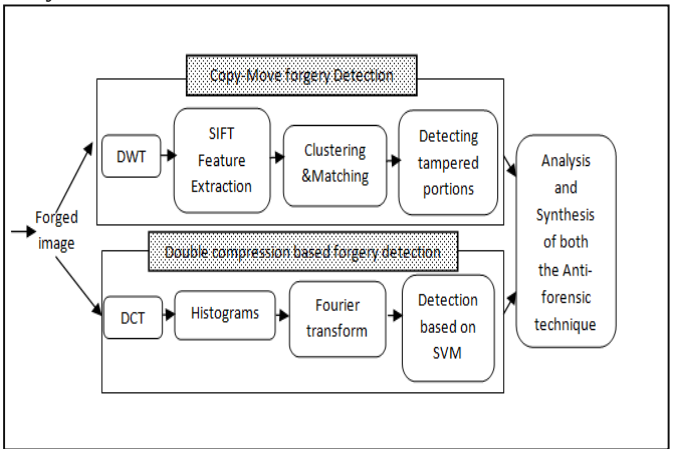

Fig.1 Detection mechanisms for forged image and analysis of both the techniques

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 03, March-2016

IV ANALYSIS AND RESULTS

The output produced here is the result of applying Antiforensics in an image and process of efficient detection of forged portions using the image processing techniques. Fig.2 Depicts the Copy-Move image forgery that consists of Erosion, Dilation and Segmentation as its sequential steps.

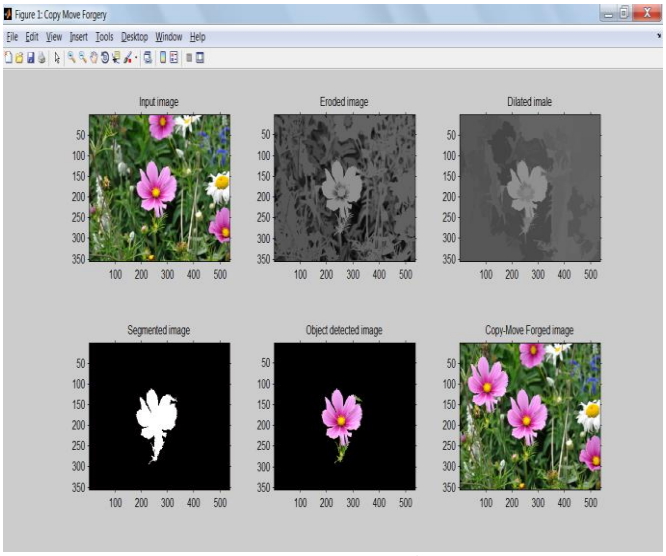

Fig.2 Copy-Move image Antiforensics

Fig.3 depicts the Copy move forgery detection. It can be detected using SIFT feature extraction which contains the steps such as Scale space extrema Detection. The convolution among the image and the variable scale Gaussian is done to determine the scale space extrema. Keypoint localization and orientation assignment is to be done further. Based on the properties of local image it assigns orientation to the keypoints. Finally the tampered portions can be cropped separately. The Screenshot is as follows.

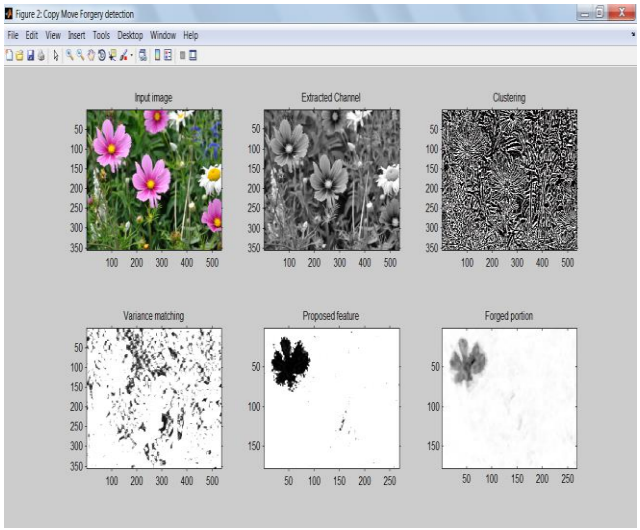

Fig.3 Copy-Move Antiforensic detection

The Fig.4 and Fig.5 depicts the Double compression based Antiforensics. This compression of an image can be done with the help of user defined compression ratio. Based on the compression ratio the strength of the compression will be defined. The more the compression ratio the higher the compression of an image will be. The Analysis is being done on detecting the double compression footprints.

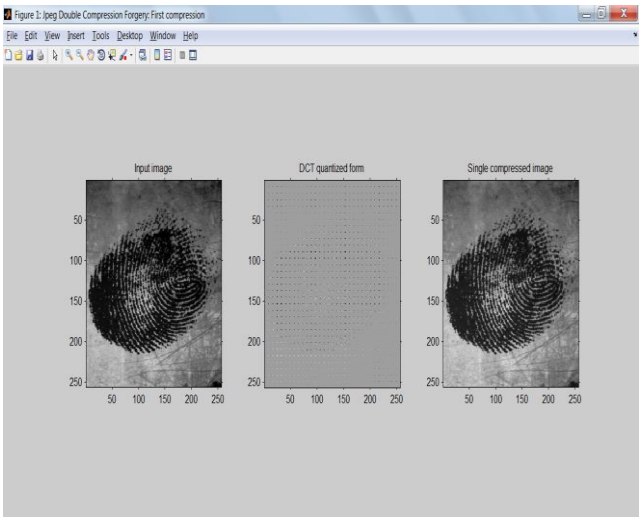

Fig.4 Single Compression of finger print image

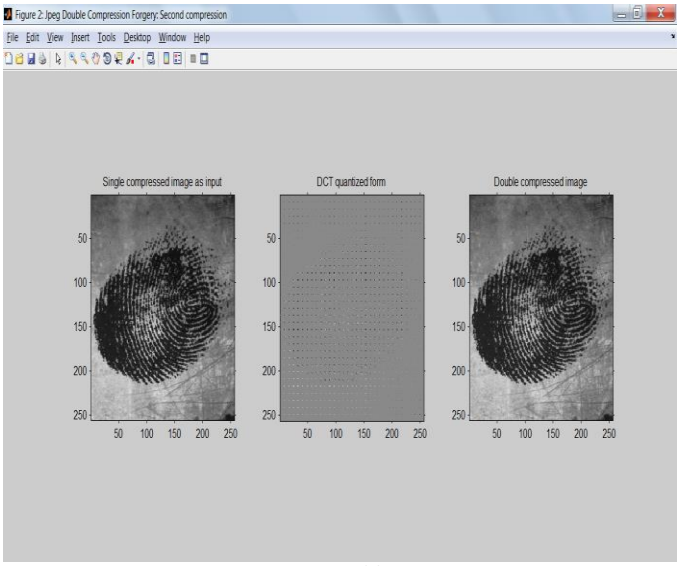

Fig.5 Double compression of finger print image

V CONCLUSION

Antiforensic tools and mechanisms will always provide difficulties and challenges to the digital investigation and forensic communities. Every attempt which made the digital forensics process harder leads to new challenges. This system focuses on a method that detects digital forgeries created using two techniques called Copy-Move image Antiforensics and Double Compression image Antiforensics. Some forgery images that results from portions copied and moved within the same image to forge something are called as copy-move Antiforensics and Some forgery images that loss its data by compressing it to two or more times to produce the fake images are called as Compression Antiforensics. Hence, the empirical design and analysis herein focuses on detecting and analysing such

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 03, March-2016

Antiforensics. However, the system does not recover the original image from its tampered input image. The detective communities and crime departments will be more beneficial if the forged images are recovered by detecting the particular tampered pixels. This enhancement will be considered in future for the efficiency of this system. And, there are numerous ways to tamper the images. But, the System concentrates only on two familiar classifications of Antiforensics. Hence, the analysis of distinct Antiforensic methods and its outcomes are also to be noticed in future.

REFERECES

[1] Xiaoyu Chu, Mathew Christopher Stamm, Yan Chen, and K. J. Ray Liu, "On Antiforensic Concealability with Rate-Distortion Tradeoff," *IEEE Trans. Image Process., vol. 24*, no. 3, Mar. 2015, pp.1087-1100.

[2] Jian Li, Xiaolong Li, Bin Yang and Xingming Sun, "Segmentation-Based Image Copy-Move Forgery Detection Scheme," *IEEE Trans. Information Forensics and Security, vol. 3*, no. 3, Mar. 2015, pp. 507–518.

[3] W. Fan, K. Wang, F. Cayre, and Z. Xiong, "A variational approach to JPEG anti-forensics," in *Proc. IEEE ICASSP.*, May. 2013, pp. 3058–3062.

[4] Y. Chen, W. S. Lin, and K. J. R. Liu, "Risk-distortion analysis for video collusion attacks: A mouse-and-cat game," *IEEE Trans. Image Process., vol. 19*, no. 7, Jul. 2010, pp. 1798–1807.

[5] Z. Fan and R. L. de Queiroz, "Identification of bitmap compression history: JPEG detection and quantizer estimation," *IEEE Trans. Image Process., vol. 12*, no. 2, Feb. 2003, pp. 230–235.

[6] Jan Lukas and Jessica Fridrich, "Estimation of Primary Quantization Matrix in double compressed JPEG Images," in *Proc. Digital Forensic Res. Workshop*, Cleveland, OH, USA, Aug. 2003, pp. 5-8.

[7] Zhou Wang, Alan C. Bovik, Hamid R. Sheikh and Eero P. Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity," *IEEE Trans. Image Process., vol. 13*, no. 4, Apr. 2004, pp. 1–14.