International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi :https://doi.org/10.32628/IJSRSET

Digital Image Authenticity Verification System

Dr. Ch. Anusha*1, V. V. Brahma Chari*2, P. China Veeraiah*3

*1Associate Professor, Department of Computer Science Engineering, A.M Reddy Memorial College of Engineering and Technology, Andhra Pradesh, India

*2, 3Assistant Professor, Department of Computer Science Engineering, A.M Reddy Memorial College of Engineering and Technology, Andhra Pradesh, India

Article Info
Volume 9, Issue 1
Page Number 363-368

Publication Issue :
January-February-2022

Article History
Accepted : 05 Feb 2022
Published: 20 Feb 2022

ABSTRACT

In today's day today life digital images are available everywhere and it is very easy to manipulate these digital images by using powerful editing software. Now a day's many people add, crop or remove important features from an image without leaving any proof of fake images. There are many techniques used for forgery detection. One of the technique most commonly used is Copy-Move forgery in which coping a some part of image and pasting it into the same image in order to hide some data or part of an image and other most commonly used technique is staganalysis in which some message is hidden inside the image which is not easily possible to see with naked human eye. In this paper we search the problem of detecting the forgery and describe robust detection method. this method successfully detect the forged part even when the copied area is edited to combine it with the background of an image and even if the forged image is saved in the JPEG format.

Keyword — Digital image, Stenography, Copy-Move

I. INTRODUCTION

Now a days, digital images are widely used all over the world From newspapers to magazines, fashion industry, in medical field, science field, forensic labs etc. depends on digital images. Exchanging soft copy of various documents is a normal practice in these days. So there is a possibility of forgery while exchanging such type of documents. Forgery is manipulation of an image to achieve a specific result. Image Forgery is the process of making illegal changes of image information. Forgery may occur in every application which is using digital image because user can change it by using editing tools available in market.

Forgery detection techniques divided into two major categories: active and passive methods. Active method requires some prior information of an image hence such methods are not useful while handling images from unknown sources. this is biggest drawback of active method digital watermarking belongs to active method Passive method does not require any prior information of digital image. The method works purely by analyzing binary information of digital image without any external information. Copy-move forgery belongs to this method. Some examples of forgery is shown below.

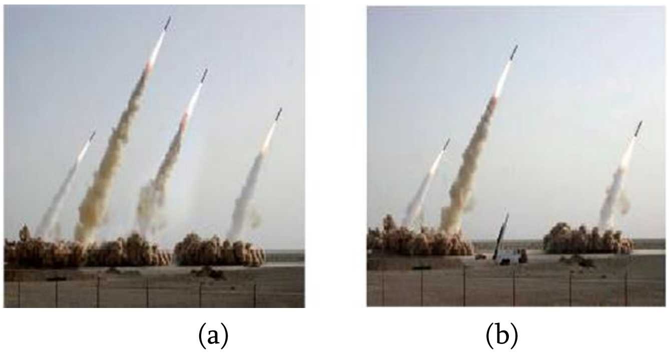


Fig 1. An example of copy-move forgery:(a) the forged image with four missiles & (b) the original image with three missiles.

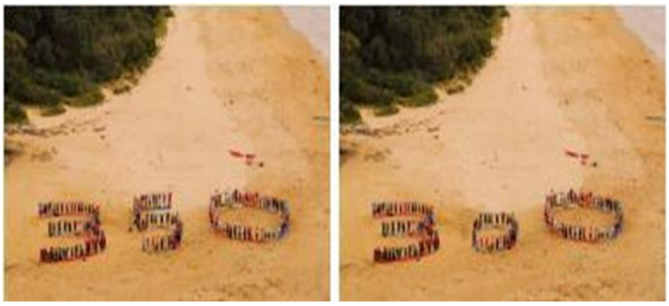


Fig. 2. Another example of typical copy-move forgery .Left : the original image. Right : the tempered image.

There are many techniques have been proposed to solve the problem of forgeryas given below:

[1] Bin YANG 1, Xingming SUN 2 proposed robust and more reliable forgery method for copy- move forgery detection based on DWT- FWHT. They uses DWT to reduce the size of image and expands the feature in the overlapping blocks by FWHT instead of the DCT. Their proposed method is weak in detecting images which have undergone the attack of transforming.

[2] Nathalie Diane Wandji1, Sun Xingming proposed an DCT algorithm that can detect copy move forgeries. They use the category of passive methods because it does not require any primary information of an image to perform operations. Also it can detect multiple copy- move forgeries in the same image and also it is relatively very powerful to some common distortions.

[3] Ashima Gupta1, Nisheeth Saxena2, S.K Vasistha3 proved that the use of DCT is better than using PCA for detecting copy-move attacks in highly textured images. They improve the detection rate and time of the copy-move attack proposed by their algorithm.

[4] Andrew D. Ker publish peper on "Steganalysis of LSB matching in gray scale images.They have given two ways to apply the histogram characteristic function diagnosis of stegnography. They produce more reliable detectors for LSB steganography in grayscale images.

[5] Fridrich et al. firstly, divided an image into overlapping blocks of equal size. The coefficient of each block was removed by discrete cosine transform. Finally, the duplicated regions were found by matching the quantized coefficients which had been simultaneously sorted.

[6] Popescu and Farid proposed a copy-move forgery detection method in which the authors extracted the coefficient by principal component analysis (PCA) instead of DCT.Therefore the dimensions of the coefficients extracted by PCA are relatively smaller than DCT. The weakness of this peper is that it cannot detect the rotating copy region of an image.

II. PROPOSED SYSTEM

An illegal modification or reproduction of an image information. In this paper, we used DCT algorithm for forgery detection. There is an approach that can detect tempered JPEG images and further locate the tempered parts, by observing the double quantization effect hidden among the DCT coefficients. The JPEG process is a widely used form of lossy image compression that only used by the DCT. The JPEG method is used for both Black & white and colour images. Our method detects duplicated forgery regions by dividing the image into 8*8 overlapping blocks and then we search for the matching region in the image. We show the potential of this method on capable forgeries and evaluate its strongness also.

III. CONCLUSION

In the study, the wireless sensor technology is combined with the human health monitoring terminal based on the Internet of Things to test the health-related indexes. The test results are analyzed. It is observed that the human health monitoring system of the Internet of Things is relatively stable and has functions such as an accurate collection of human health data, real-time monitoring and alarming, and evaluation of subjects. The subjects were assessed for temperature using the thermometer, which provides the temperature values of 36.4, 36.7, and 36.5 (°C), respec tively, demonstrating relatively accurate and stable testability. Similarly, the pulse rate monitoring module employing the ECG observes the test outcomes of 78, 78, and 79 (times/min), respectively, similar to the medical pulse meter results.

The human health monitoring system based on the Internet of Things designed in this study has completed collecting the user's blood pressure, pulse, body temperature, heart rate, physio logical information, and other vital sign data, which is suggested in practice. After long-term data collection, factors related to a potential risk prediction should be further explored in the future to expand the application of human health monitoring systems based on the Internet of Things. This will provide a scientific and effective basis for preventing and controlling chronic high-risk diseases in the near future.

A. BLOCK DIAGRAM

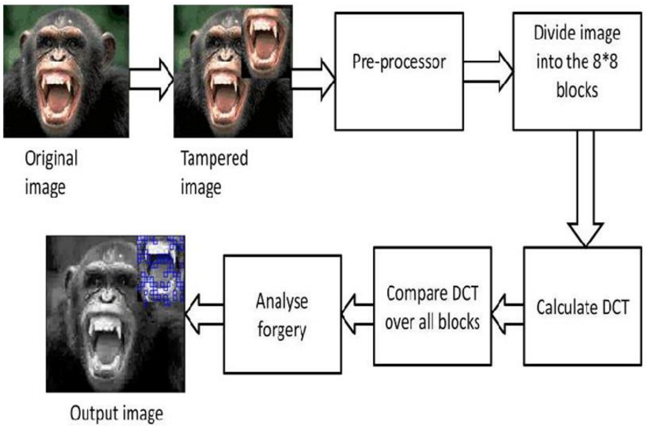


Fig 3 : Block diagram of DCT algorithm

B) WORKING OF DCT ALGORITHM:

1. Take tampered image as a input.
2. Divide input image into 8*8 block of pixels.
3. Apply DCT to each block of pixels.
4. After applying DCT each block is compressed through quantization.

The array of compressed blocks that form the image is stored in a drastic manner reduced amount of space.

C) CALCULATIONS OF DCT ALGORITHM:

The DCT Equations:

The DCT equation represents the I,Jth entry of the DCT of an image.

$$D(i,j) = \frac{1}{\sqrt{2N}} C(i)C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} p(x,y) \cos\left[\frac{(2x+1)i\pi}{2N}\right] \cos\left[\frac{(2y+1)j\pi}{2N}\right]$$

$$C(u) = \left\{ \begin{array}{ll} \frac{1}{\sqrt{2}} & \text{if } u = 0 \\ 1 & \text{if } u > 0 \end{array} \right\}$$

…..(1)

To get the matrix form of equation (1), we will use the following equations.

For an 8*8 block it results in following standard matrix

$$T = \begin{bmatrix} .3536 & .3536 & .3536 & .3536 & .3536 & .3536 & .3536 & .3536 \\ .4904 & .4157 & .2778 & .0975 & -.0975 & -.2778 & -.4157 & -.4904 \\ .4619 & .1913 & -.1913 & -.4619 & -.4619 & -.1913 & .1913 & .4619 \\ .4157 & -.0975 & -.4904 & -.2778 & .2778 & .4904 & .0975 & -.4157 \\ .3536 & -.3536 & -.3536 & .3536 & .3536 & -.3536 & -.3536 & .3536 \\ .2778 & -.4904 & .0975 & .4157 & -.4157 & -.0975 & .4904 & -.2778 \\ .1913 & .4619 & .4619 & .1913 & .1913 & .4619 & .4619 & .1913 \\ .0975 & -.2778 & .4157 & -.4904 & .4904 & -.4157 & .2778 & -.0975 \end{bmatrix}$$

Firstly, we start with 8*8 block of image pixel values that is selected from very uppermost left side corner of an image. For DCT, pixel values ranging from -128 to 127.Therefore from each pixel values of 8*8 blocks 128 gets substracted. After substraction, this result is stored into some alphabet lets say M. Now, we perform the DCT which is completed successfully by matrix multiplication.

D=T*M*T’

D) QUANTIZATION

Now, above DCT matrix is ready for compression by quantization. In this step, by selecting a specific quantization matrices it is possible to vary the levels of image compression and quality of an image.The image quality levels ranging from 1 to 100 where 1 gives lower image quality and higher compression while 100 gives better quality but lower compression. The quality level Q50 matrix gives both high compression and best decompression image quality.

$$Q_{50} = \begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

For quantization, it is obtained by dividing each element in D matrix by corresponding pixel values in the Q50 matix and round up to the nearest integer value.

E) CODING:

The quantized matrix C is now used for final step of compression.In this step all coefficients of C are converted into binary stream by using encoder.After quantization most of the coefficients results into zero.JPEG encode this Quantized coefficients in the zig-zag mannar as shown in figure3.

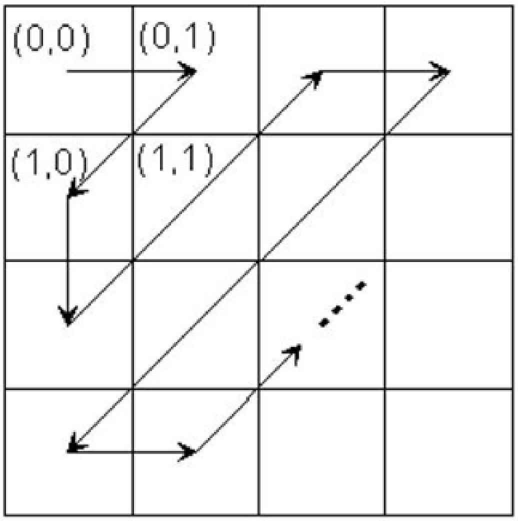


Fig.4. Process of Coding

F) DE-COMPRESSION:

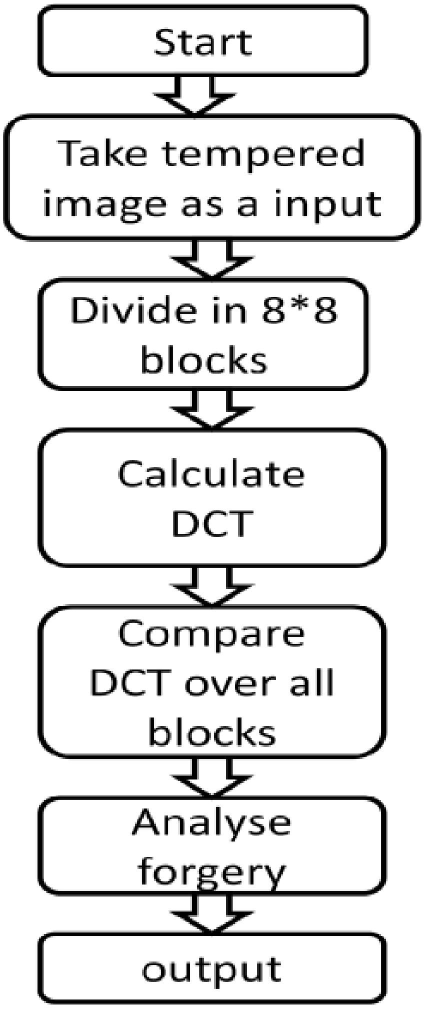
Decompression is exactly opposite process of compression.Original image is obtained by decoding the bit stream of quantised matrix C and multiplied by quantization matrix Q50

R(I,j)= Q(I,j) * c(I,j)

For IDCT, 128 is added to each element of matrix R which is rounded.Formula is given below.

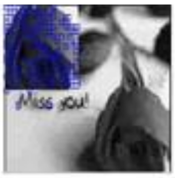
N=round(T’ * R * T) + 128

FLOWCHART OF DCT:



ORIGINAL IMAGE

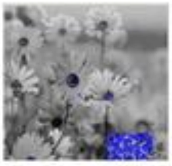
FORGE IMAGE



OUTPUT IMAGE

ORIGINAL IMAGE

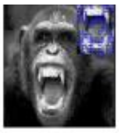
FORGE IMAGE



OUTPUT IMAGE

ORIGINAL IMAGE

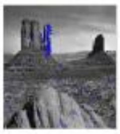
FORGE IMAGE



OUTPUT IMAGE

ORIGINAL IMAGE

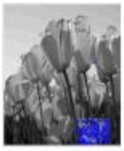
FORGE IMAGE



OUTPUT IMAGE

ORIGINAL IMAGE

FORGE IMAGE



OUTPUT IMAGE

IV. CONCLUSION

Copy-move forgery is one of the most commonly used forgery technique. In this we use a stongest method to detect the tempered region in an image. We have taken some test on the algorithm against forge images from the internet. From this algorithm, we get improvements in the detection rate and the detection time of copy move attack on images. For highly textured images DCT is better than any other forgery detection algorithms. By using wavelet transform, we can improve the efficiency of algorithm. For future work, we will improve the accuracy of algorithm and try to perform this process on video clips.

V. REFERENCES

[1]. Tao Jing Xinghua li, Feifei Zhang, Image Tamper Detection Algorithm Based on Radon and fourier-Mellin Transform”,pp 212-215 IEEE2010

[2]. Sarah A. Summers, Sarah C. Wahl “Multimedia Security and Forensic Authentication of Digital images,

"http://cs.uccs.edu/~cs525/studentproj/proj52006/sasummer/doc/cs525projsummersWahl.doc".

[3]. J. Fridrich, D. Soukal, and J. Lukas, "Detection of Copy-Move Forgery in Digital Images", in Proceedings of Digital Forensic Research Workshop, August 2003.

[4]. A. C. Popescu and H. Farid, "Exposing Digital Forgeriesby Detecting Duplicated Image Regions," Technical Report, TR2004-515, Department of Computer Science, Dartmouth College, pp. 758-767, 2006.

[5]. X. Kang and S. Wei, "Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensics," International Conference on Computer Science and Software Engineering, pp. 926-930,2008

[6]. B. Mahdian and S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants.," Elsevier Forensic Science International, vol. 171, no. 2-3, pp. 180-189 Sep. 2007..

[7]. S. jin Ryu, M.-jeong Lee, and H.-kyu Lee, "Detection of Copy-Rotate- Move Forgery Using Zernike Moments," IH , LNCS 6387, vol. 1, pp. 51-65, 2010.

Cite this Article

Dr. Ch. Anusha, V. V. Brahma Chari, P. China Veeraiah, "Digital Image Authenticity Verification System", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 1, pp. 363-368, January-February 2022.
Journal URL : https://ijsrset.com/IJSRSET2292108