Image Forgery Detection Using Dct And Quantization Matrix Techniques

Shiji Abraham, Anisha P Rodrigues, Roshan Fernandes

Abstract: ***In today's era the image has become useful for communication purpose. But due to the development of software and various techniques it is possible to change images in adding or removing essential feature from it without leaving a clue of real image. It is not easy for the common people to identify whether the image original or tampered. In order to avoid this problem, forgery detection came into existence. Detection of forgery refers to task of image processing to identify that the images are unique or tampered. Several techniques have been used in order to detect the forgeries from the forged image, but this issue has not yet solved. In order to solve these issues we have used Discrete Cosine Transformation (DCT) and quantization matrix techniques for identifying forged areas of image, where the quality of image is not reduced. The Discrete Cosine Transformation (DCT) is used in order for characterizing the overlapping blocks and quantization matrix is used to compress DCT values and gives both highly compressed and best decompressed image quality. Here we use block matching algorithm. This algorithm one of the most frequently used for detecting image which is duplicate. This proposed work also supports for different kinds of images such as JPEG, JPG or PNG of any size it can be either mxn or nxn.***

***Index Terms**: Forgery detection, image processing, tampered image, DCT based algorithm;*

I. INTRODUCTION

In today's world, digital image has become one of the important medium for communication. Millions of images and videos have been uploaded to the social media. And further this image are shared in sites to gain more attention and it also affects the social opinions of particular issues due to people having nature tendency of accepting things as seen by eyes. These days many image editing software has been developed, where one can change or modify the content of images. This process is called as image forgery or image tampering. Due to the content modification this has become a serious issue as it leads to some of the dangerous situations. Hence it is very much important to check the trustworthiness of image. Forgery detection method is an authentication method, which has an assumption that real image having some of the inheritance patterns that has a variety of imaging device or processing. Here these patterns are constant to real images and it can change after performing the operations of forgery. This identification of forged image has turn into a difficult, due of the highly developed and advanced tools for processing.1.1 Types of forgery detection

Digital forgery detection is used for detecting some of the significant features from image without ignoring the observable hint. There are different methods of forging an image, these methods are used to make forged images, and there are 2 different kinds of forgery detection. This is shown in Figure 1[1].

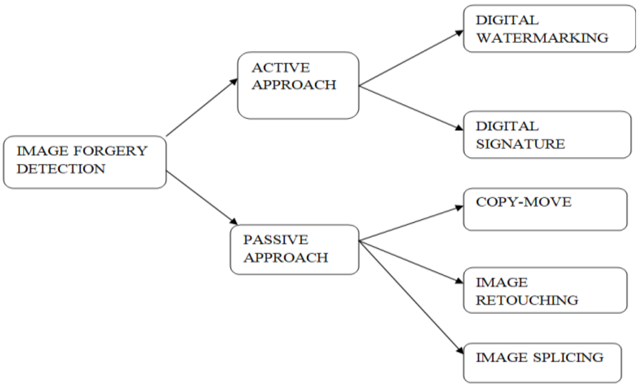


Fig1. Classification of forgery image

1.1.1 Active Approach

The active approach is used to perform pre-processing operation like watermark attachment and while generating digital image a signatures are used. The active approach again further classified into (i) digital watermarking and (ii) Digital signature.

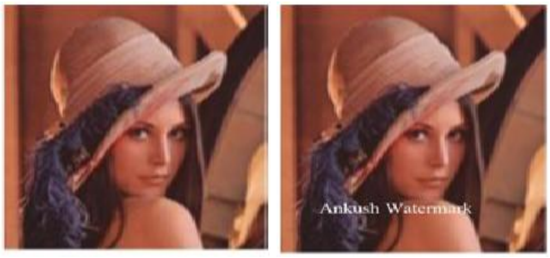
(i) Digital watermarking: This method is used for detecting tamped images. Watermarking techniques are of different types. Among that the checksum schema is used to add information into least significant bit of the pixel. Other method will add the linear sequence pixel onto the data pixel and recognize the watermark by spatial cross-correlation for the functions of order and the watermarked image. These watermarks are invisible watermarks. The visible watermark also exists, this kind of watermarks are used to identify the change in each pixel. The embedded watermarks are used during the creation of image. As mentioned in fig 2[2].

Revised Manuscript Received on August 30, 2019.
* Correspondence Author

Shiji Abraham*, Department of Computer Science and Engineering, NMAM Institute of Technology, Nitte, India.

Anisha P Rodrigues, Department of Computer Science and Engineering, NMAM Institute of Technology, Nitte, India.

Roshan Fernandes, Department of Computer Science and Engineering, NMAM Institute of Technology, Nitte, India.



(a) Original image (b) Watermarked image

Fig.2. Digital Watermarking

(ii) Digital signature: Digital signature is used to detect forged image or tampering. By indicating an authenticity of the digital document used to arrange the scheme in mathematical form is called digital signature. In the digital signature technique, it extracts the robust bit from the original signature. The picture is separated into 16X16 pixels. The K secrete key is used to produce matrices of N which is random with [0,1] invariant distributed interval. A filter called low pass filter that are adapted to every unsystematic matrix frequently to obtain 'N' smooth pattern which is unsymmetrical. The digital signature is generated through a system by placing process of signing in image which is digital [3]. The steps involved in image signing process are [4]:

1) The image is decomposed by using the parameterized wavelet feature.

2) SDS is extracted

3) Hash cryptographically extract SDS and generate signature of crypto by using sender key which is private of an image.

4) The associated crypto signature and its image are sent to receiver.

The working procedure is shown in figure 3[5].

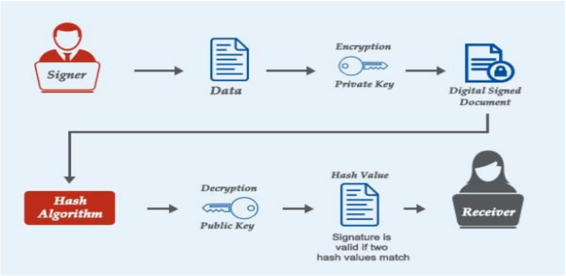


Fig.3. working procedure of digital signature

1.1.2 Passive Approach

The image which is real has some of the acquired characteristics that are originated by different image processing techniques. The pattern which is present in the real image is modified after the tamper operation. Here the image which is real is forgeried only when tampering of the image takes place. By detecting the pattern we can identify the source of digital image and obtain the authencity. By comparing with active method, passive method is found to be a new technology which does not have digital watermarking and digital signature. The techniques involved in passive approach are:

1. *Pixel based techniques*-are used for identifying statistical anomaly which is originated on each level of pixel.
2. *Format based techniques*-are correlation which is statistical originated by a particular freely compressed scheme.
3. *Camera based techniques*-this exploits artifacts which are originated from sensor, lenses of camera or at post processing of chip.
4. *Physically based techniques*- are used to detect anomalies in three dimensional interactions among objects which are physical, cameras, and lights.
5. *Geometric based techniques*-this will build the dimensions of world objects and there position related to camera [6].

The different types of passive approach in detection of forgery are:

(i) Copy move approach (ii) image splicing approach
(iii) Image retouching approach.

(i)*Copy move approach:* In this approach, a number of areas in image with any shape and size are copy-pasted to another area of same image, as illustrated in fig 4[7]. Since the area which is copied is generated from same image and the essential properties like texture, noise and color does not vary and it makes identification procedure difficult.

The copy move also has different types: (a) Block based method (b) key point based method.

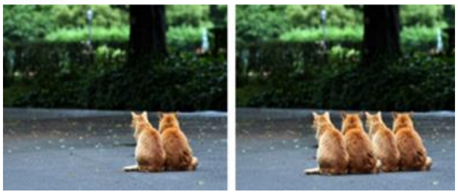
(a) Block based method: Input image can be divided into 2 image blocks i.e. regular and overlapping blocks. Then by mapping a block image pixel or change coefficient a tampered region is obtain. The block based method involves:

- Discrete cosine transformation (DCT) co-efficient of each block is matched for detecting the tamper regions.
- Principal component analysis (PCA) is used to reduce the size of features in block.
- Fourier-Mellin Transform (FMT) is used for the calculation of blocks.
- Each block and sub-block of Gray average result used as a block features.
- The block features are used by information entropy.

Apart from the mentioned procedure a feature of image calculation is very much essential to reach compression, scaling, rotation and complexity of time in forgery detection of an image is improvement. Hence key point based method was improved for identifying the forgery along with accurateness which is subjected to the scaling and rotation.

(b) Key-point based method: In the method based on key focuses only the features of image which is having more transformation. There are 2 key point methods:
(i) SIFT (scale invariant feature transform) (ii) SURF (Speeded Up Robust Features).

- SIFT: It is used for extraction of image feature transfer of host in order to map duplicate or forged area detection
- SURF: It is used for the process of feature extraction.



(a) Original image (b) copy moved area

Fig.4. copy move image

(ii) *Image Splicing:* Image splicing is a technique, taking two different images and joining those two images to form a new single image as shown in figure 5[8]. Such a type of image does not reflect the reality, so spliced image must be executed carefully. Image splicing is harder to detect compared to copy move forgery because detecting the similar contours of object of same image is easier as they have the same texture, transactions, size etc, where in the case of image splicing dissimilar object are having dissimilar texture and image feature complexity. Hence it makes difficult to detect.

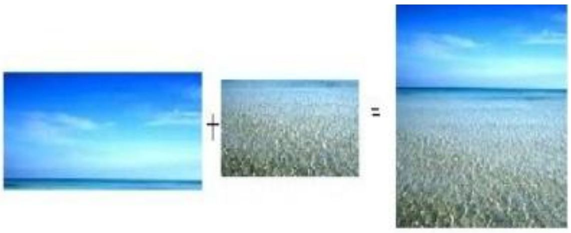


Fig.5. Image splicing

(iii) Image Retouching: In this method there is no addition of extra things or modify the image instead it can enhance the image or even reduce some features in the image. Image retouching is not much risky type connected with the different digitally forged image compared to the other methods. Figure 6 [9] shows the image retouching that consist of two images i.e. original image and image retouching.

(a) Original Image (b) Image retouching

Fig 6 Image Retouching

II. Related work

L. Li, et al. [10] introduced a technique forgery detection of copy move along with the rotation. In order to take out the features from blocks of circular, it is further used for block matching harmonic transformation performance. This technique used for the purpose of rotational and noisy figures.
H. C. Nguyen et al. [11] introduced a technique for forgery detection of copy move image using non block matching technique. This paper uses the exploiting correlation phase. The experiment result specifies the method is suitable for detecting a duplicate region of an image and robust to blurring and noise.
S. Kumar et al. [12] introduced a method known as copy moved forgery detection. This method uses discrete cosine transform (DCT) for the represent a feature for the overlapping block. It has successfully detected forgery from the image data set. In JPEG image Gaussian noise will be compressed and also results in giving less quantity of rotational and scaling and also shown robustness. Though robustness adjacent to operations of post process similar to shearing, flipping and the variations of local intensity may extended in this algorithm.
Z. Qu et al. [13] proposed an algorithm for detecting a splicing of image forgery along with visual cubes. Window detection is used and separated as sub-squares of nine. In order to distinguish obsession point a VAM (visual consideration model) method is used. After that a feature vector is used to extract a region which is spliced in the digital image
Yanjun Cao et al. [14] introduced a technique in order to forgery of copy move detection in images of digital. Here they made use of DCT for co-efficient identification of every block which is circular. Further, features from every circular block are extracted. In order to locate a related block pairs a searching operation is performed for mapping a duplicate region.
T. Ng et al. [15] and T.-T. Ng [16] improved the technique by using geometric invariant which is linear from one image and signature of CRF feature is extracted from the linear surface in irradiance of an image. T.-T. Ng [15] has developed an edge profile based in order to extract a signature of CRF from the one image. In the introduced technique the extraction method depends on edges and these edges must be wide and straight.
J. Zhang et al. [17] developed a method for detecting copy move forgeries of digital image. They applied DWT and the given image is separated as non-overlapping of four subimages and phase of correlation is adopt for computing the spatial offset among forgery of copy move regions. Then they apply matching algorithm among the pixels based on similarity for forged region detection. This method functions for highly compressed image and effective that is extremely lesser computation time compared to another method.
L. Kang et al. [18] introduced a method for copy move detection of forged digital image. Firstly images are classified into sub-blocks then they used enhanced SVD on each one of blocks. The matching of similarity is performed for every blocks which are based on sorting of lexicographical SV vectors. At the end a region of forged area of image is detected.
H. Shao et al. [19] introduced a technique based on expansion of polar phase and with limitation of band which is adaptive. Polar expansion based on Fourier transformation on windows pair which is overlapping to calculate and procedure with limitation is applied for adaptive band to get matrix of correlation which efficiently enhances peak. After analyzing the angle for rotation in forged area, a algorithm for searching in which executes a sense of seed filling for displaying the entire region which is duplicated. This approach is detecting area which is duplicated with robustness, large accuracy for rotation, illumination adjacement, blur and compression of JPEG.Andrea Costanzo et al. [20] have proposed a methodology to identify the image and find out a fake region of the forgery image.

They had developed an algorithm which depends upon the concept of abnormal anomalies and identify the forgery regions.

Myna et al. [21] introduced a technique that uses a wavelet transform and log polar coordinates to identify and localize forgery of copy move. The use of transformation of wavelet into the input images that results in reduction of dimensionality and exhaustive search is taken place in order to recognize the blocks which are similar in mapping of an image to coordinates of log polar and critical correlation phase is used. The benefit of this technique is localization of duplicate region and reduced image size.

Cao et al. [22] improved the technique for detecting correlation of gamma for detecting the forgery of image. This method is based on histogram characteristics estimation which is calculated based on the patterns of features in peak gap. This feature is differentiated by histogram which is pre-computed for correlation of gamma in image detection. These results propose this method which is globally effective and modifications based on correlation that is local.

X. F. Li et al. [23] used a method for retouching based detection on filter of bi-Laplacian. These methods are used for block mapping based on KD tree for every block in an image. These method workings fine for images which is uncompressed and high resolution compressed images. So the accuracy is based on tampered region for compressing images at high level.

Yuan Rao et al [24] introduced a technique for detection of forgery in an image on the basis of deep learning technology, which make use of convolution neural networks (CNN) for learn hierarchical representation automatically from the RGB images color in input. CNN are applied specially for the splicing of an image and detection of copy move applications. In spite of strategy which is random, the starting layer network weight are initialized by 30 basic filters of high pass used in Spatial Rich Model (SRM) which is used for images steganalysis. It is very powerful in suppressing the consequence of the image and accelerates the network convergence. They conducted the experiments based on several datasets of public which illustrates the performance which is better.

Kang et al [25] introduced the utilization of SVD in order to recognize regions which are modified in images which are digital. The author used SVD for extraction of feature vector and decrease of dimensions. A sorting called Lexicographical sorting used for rows and column vector of identical blocks are recognized to find the forged region. The algorithm used here is more efficient and robust.

III. PROPOSED WORK

Steps involved in the proposed method:

1. Input image i.e. i1. If input image is colored then convert it to gray scale image i.e. i2=rgb2gray (i1).

2. Resize the image i2=imresize(i2, [128 128]).

3. Initialize null matrix for future use v=zero(64,1). Divide the image into 8x8 blocks/cells in overlapping manner i.e. Blocks2=cell(row/8, col/8) and subject each 8x8 cell as D=dctmtx(size(Block2(i,j),1). i=1:row-7 and j=1:col-7, where i is a row matrix and j is a column matrix.

4. Apply DCT to 8x8 matrix dct=D*Block2(i,j)*D.

5. Divide quantization matrix to element wise K=dct/Q75.

6. Convert each 8x8 to a linear row and create a new matrix with formed rows. v=horzcat(v,k1).

7. The first pixel location of the block corresponding to the row in ‘v’ is stored in‘s’.

8. The initial [0,0] null matrices declared are deleted. The 1st row is deleted. i.e L(1,:), add2(1,:). Next concatenate both i.e. L=[L,add2].

9. Lexicographically sort the row L1=sortrows(L).

10. Remove the concatenated location s2=[L1(:,end-1)L1(:,end-1)]. Delete the last 2 columns, since we stored the sorted location in s2.

11. Find the Euclidian distance i.e. shiftvector=zero(1,2), copy=zero(1,6). And segregate all the unique set of element in shiftvector.

12. Count the number of times each unique set of element occur in shift vector i.e. cnt=0, repetition=zero (row 3,1). The number of times “repetition” matrix i.e. repetition (i,1)=cnt.

13. Filter highly repeated Euclidian distance values i.e. threshold=repetition>400. And finally check the matrix with same distance.

14. Mark the copy moved region on binary image.

Steps involved in detecting copy move images:

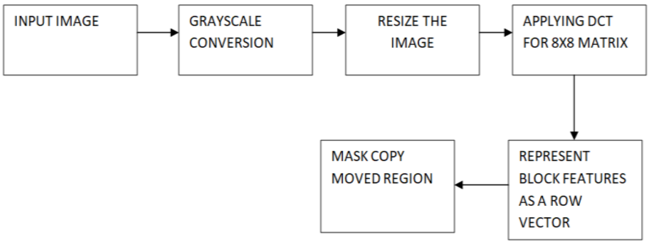


Fig.6. Flow Chart for forgery detection

1. *Input image:* The input images are taken of any size. The size must be either mxn or nxn. The image can be either colored or grayscale image.

2. *Gray Scale Conversion:* If the input image is colored image convert image to grayscale. Gray scaling of image is done because easier to deal with single color channel than multiple color channel.

3. *Resize the image:* In this step the image resizing is done. If the image is mxn then it is resized to nxn a square image. Resizing of image is done due to more size more the computational complexity.

4. *Apply DCT for 8x8 Matrix:* Apply DCT to every block and reshape 8x8 quantized co-efficient matrixes to a row vector by ordering DCT co-efficient in Zigzag order.

4.1. Calculations of DCT algorithm:

The DCT equation can be represented as follows where i,j is the entry of the DCT image.

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

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

In order to get a matrix form of equation (1), we can use the following equation

$$T_{i,j} = \begin{cases} \frac{1}{\sqrt{N}} & if\ i = 0 \\ \sqrt{\frac{2}{N}}\ \cos\left[\frac{(2j+1)i\pi}{2N}\right] & if\ i > 0 \end{cases}$$

The following standard matrix indicates 8x8 blocks

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

From the uppermost left side corner of an image we started with image pixel of 8X8 value is selected. The pixel value of DCT ranges from -128 to 127. Therefore 128 will get subtracted from each pixel value. The result will be stored in the alphabet 'H' after subtraction. By performing matrix multiplication the operation of DCT has successfully completed.

$$D = T * M * T'$$

4.2. Quantization:

The above given DCT values are used for compression using quantization. A specific quantization matrix is selected and varied according to the level of compressed image and the amount of image. The amount level of an image ranges from 1 to 100 where 1 indicates lower level image quality and higher quality compression and 100 indicates higher level image quality but lower quality compression. The matrix of quality level Q75 gives both highly compressed and best decompressed image quality.

$$Q75 = \begin{pmatrix} 8 & 6 & 5 & 8 & 12 & 20 & 26 & 31 & \\ 6 & 6 & 7 & 10 & 13 & 29 & 30 & 28 & \\ 7 & 9 & 11 & 15 & 26 & 44 & 40 & 31 & \\ 9 & 11 & 19 & 28 & 34 & 55 & 52 & 57 & 46 \\ 12 & 18 & 28 & 32 & 41 & 52 & 57 & 46 & \\ 25 & 32 & 39 & 44 & 52 & 61 & 60 & 52 & \\ 36 & 46 & 48 & 49 & 56 & 50 & 52 & 50 & \end{pmatrix}$$

The quantization is obtained by splitting each element present in matrix D by consequent pixel values in matrix of Q75 and values are round up that is closest to integers.

$$\mathbf{C_{i,j} = round\left(\frac{D_{i,j}}{Q_{i,j}}\right)}$$

5. Represent block features as row vector: The features of each block are indicated as a row vector and sorted them lexicographically. Segregate all the unique set of elements in a shift vector. And all the repeated values in the shift vector is stored in "repetition" matrix. In this experiment matrix there are 75x1 repetition matrixes.

6. Mask copy moved region: The quantized matrix is used for the last step of compression. In this method all the co-efficient are converted into binary stream with the help of encoder. Most of the coefficients will generate results zero after quantization as shown in fig 7. Mark the copy moved regions on a binary image.

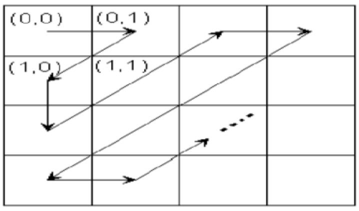
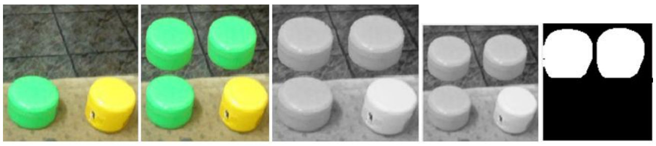


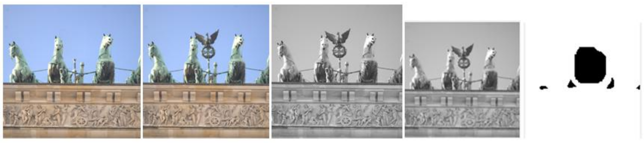
Fig .7.Representation forged region in binary image.

IV. RESULTS



a. Original Image b. Forged Image c. Gray scale Image d. Resized Image e. Forged Image

Fig.8. Detection of forged Can



. Original Image b. Forged Image c. Gray scale Image d. Resized Image e. Forged Image

Fig.9. Detection of forged horse horn and flag.

In fig 8a is the original image and fig 8b is the forged image. In 9.a is the original image and 9.b is the forged image, here there are 2 forged areas, one is horse horn and another one is flag. Both these images are gray scaled and further it is resized to nxn image. Finally the dark portion indicates the forged image.

Table 1:

Dataset Number	Image Name	Time Taken For Execution(seconds)
Set 1	Can	46.31
Set 2	Horse	45.26
Set 3	Building	46.62
Set 4	Stage	49.38
Set 5	Insect	45.52
Set 6	Flowers	44.41
Set 7	Tree	45.85
Set 8	Kitten	46.42
Set 9	Jet	45.9
Set 10	Chickens	48.04

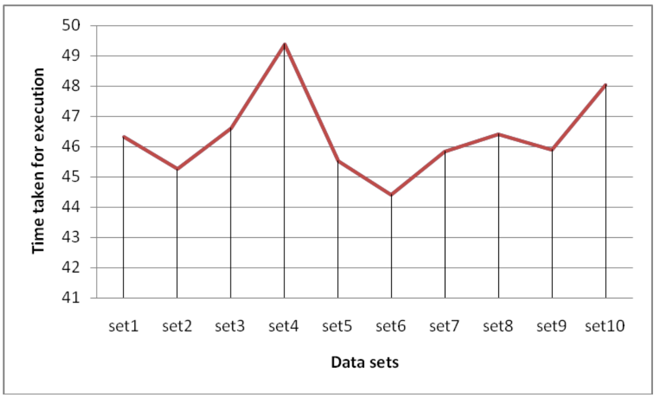


Fig.10. Time Graph

V. CONCLUSION

In advanced technology, digital editing process contains many tools for editing the image without leaving any traces to the human eye. In order to overcome this problem, a forgery detection of an image came into existence. There are two different techniques used for forgery detection called as active and passive approach. Active approach makes use of digital watermarking and digital signature for forgery detection of image but passive approach doesn't make use of these two methods but it will directly consider an image for forgery detection. Thus passive approach is more efficient than active approach. Passive approach does not depend on the data which is hidden in order to detect the forged image, but this uses statistics or image content in order to verify its genuineness. In our proposed work it is able to identify the forged areas of images with the help of Discrete Cosine Transformation (DCT) and quantization matrix techniques. A DCT is used overlapping block characterization and quantization matrix is used for compression of DCT values and gives highly compressed and best decomposed image quality. Here a block matching algorithm is help for identifying forged images. This proposed work supported for all the kind of images such as JPEG, JPG or PNG of any size it can be either mxn or nxn. And also gives the time taken for execution of each images.

REFERENCES

1. Jiming Zheng and Liping Chang .2014."Detection of Region-duplication Forgery in Image Based on Key Points' Binary Descriptors", Journal of Information & Computational Science, vol. 11, no. 11, pp. 3959-3966, Jul, 2014.
2. https://www.slideshare.net/ankushkr007/digital-watermarking-15450118.
3. Bravo-Solorio S, Nandi AK. Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics. Signal Processing. 2011; 91(8):1759-70.
4. Doke KK, Patil SM. Digital signature scheme for image. International Journal of Computer Applications. 2012; 49(16):1-6.
5. https://comodosslstore.com/blog/what-is-digital-signature-how-does-it-work.html.
6. Hany Farid: "Image Forgery Detection", IEEE Signal Processing Magazine, pp. 16-25, March 2009
7. M. D. Ansaria, S. P. Ghreraa and V. Tyagi .2014. "PixelBased Image Forgery Detection: A Review". IETE Journal of Education.
8. M. P. Gomase and M. N. Wankhade .2014. "Advanced Digital Image Forgery Detection: A Review". International Conference on Advances in Engineering & Technology (ICAET), pp. 80-83.
9. S. Kumar, J. Desai and S. Mukherjee, "A fast DCT based method for copy move forgery detection," IEEE Second International Conference on Image Information Processing (ICIIP), 2013, Shimla, 2013, pp. 649-654.
10. L. Li, S. Li and J. Wang, "Copy-move forgery detection based on PHT," World Congress on Information and
11. Communication Technologies (WICT), pp. 1061-1065, Trivandrum, 2012.
12. H. C. Nguyen and S. Katzenbeisser, "Detection of Copy-move Forgery in Digital Images Using Radon Transformation and Phase Correlation," Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), Piraeus, 2012, pp. 134-137.
13. S. Kumar, J. Desai and S. Mukherjee, "A fast DCT based method for copy move forgery detection," IEEE Second International Conference on Image Information Processing (ICIIP), 2013, Shimla, 2013, pp. 649-654.
14. Z. Qu, and G. Qiu, "Detect digital image splicing with visual cues," Lect. Notes Comput. Sci., Vol. 5806, pp. 247-326, Jan. 2009.
15. Yanjun Cao, T. Gao, and Qunting Yang, "A robust detection algorithm forcopy-move forgery in digital images," Forensic Int.,Vol.214,pp.33-43, 2012.
16. T. Ng and M. Tsui, "Camera response function signature for digital forensics - part I: theory and data selection", Proc. IEEE workshop on information forensics and security, (2009), pp. 156–160.
17. T.-T. Ng, "Camera response function signature for digital forensics – part II: signature extraction", Proc. IEEE workshop on information forensics and security, (2009), pp. 161–5.
18. J. Zhang, Z. Feng, and Y. Su, "A new approach for detecting copy-move forgery in digital images," IEEE International Conference on Communication Systems, China, 2008, pp. 362-366.
19. L. Kang, and X.-P. Cheng, "Copy-move forgery detection in digital image," 3rd IEEE International Congress on Image and Signal Processing (CISP 2010), 2010, pp. 2419-2421.
20. H. Shao, T. Yu, M. Xu and W. Cui, "Image region duplication detection based on circular window expansion and phase correlation", Forensic Science International, vol. 222, (2012), pp. 71–82.
21. Andrea Costanzo, Irene Amerini, Roberto Caldelli, Mauro Barni, "Forensic Analysis Of Sift Keypoint Removal And Injection", Ieee Transactions On Information Forensics And Security, Vol. 9, No. 9, September 2014.
22. A. Myna, M. Venkateshmurthy and C. Patil, "Detection of region duplication forgery in digital images using wavelets and log-polar mapping", Proc. of the International conference on computational intelligence and multimedia applications ICCIMA, (2007), pp. 371–7.
23. G. Cao, Y. Zhao and R. Ni, "Forensic estimation of gamma correction in digital images", Proc. 17th IEEE Int. Conf. on Image Processing, (ICIP'2010), (2010), pp. 2097–2100.
24. X. F. Li, X. J. Shen and H. P. Chen, "Blind identification algorithm for the retouched images based on biLaplacian", Comput. Appl., vol. 31, (2011), pp. 239–242.
25. Yuan Rao and Jiangqun Ni,"A Deep Learning Approach to Detection of Splicing and Copy-Move Forgeries in Images",IEEE'2016.
26. X. Kang, and S. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in International Conference on Computer Science and Software Engineering, 2008, Vol. 3,pp.926-30.
27. A.C. Popescu, H. Farid, "Exposing Digital Forgeries By Detecting Duplicated Image Regions," Tech. Rep. TR2004-515, Dartmouth College, 2004.

Authors Profile

Shiji Abraham BE in Computer Science and Engineering. Pursuing MTech in Computer Science and Engineering at NMAM Institute of Technology, Nitte, Karkala, India. Her area of interests includes Image processing and Machine Learning. Research work carried out in Image forgery detection using DCT and Quantization Matrix.

Anisha P Rodrigues Working as Assistant Professor in the Department of Computer Science and Engineering at NMAM Institute of Technology, Nitte, Karkala, India. Her research interests include Natural Language Processing, Machine Learning, and Big Data Analytics.
She is a member of ISTE.

Roshan Fernandes is currently working as the Associate Professor in the department of Computer Science and Engineering at NMAM Institute of Technology, Nitte, Karkala, India. His area of interests includes Machine Learning, Mobile Web Services and Semantic Analysis.
He is a member of ISTE.