Digital Image Forgery Detection Using Zernike Moment and Discrete Cosine Transform: A Comparison

Shilpa Hiremath[1], Sneha A[2], N Bhavya[3], Rachna Singh[4], Meenakshi Biradar[5]

[1]Assistant Professor, Dept. of Electronics and Communication Engineering, BMS Institute of Technology and Management, Bangalore, Karnataka, India
[2345]UG Students, Dept. of Electronics and Communication Engineering, BMS Institute of Technology and Management, Bangalore, Karnataka, India

Abstract – *There is a saying that -"A picture is worth a thousand words"- but nowadays images are easily tampered because of the availability of powerful image processing software and improvement of human-computer knowledge that makes image security a challenging problem. This trend of morphing indicates serious vulnerabilities and decreases the credibility of digital images. Morphing is a technology for transforming one image to another. An Image Morphing detection technique identifies hints of computerized altering in the complete absence of any form of digital watermark or signature. This paper presents the comparison of two algorithms- Zernike Moment and Discrete Cosine Transform (DCT) for digital image forgery detection. Both original and tampered images are tested using Zernike Moment and Discrete Cosine Transform. The performance of each algorithm is measured by evaluating parameters such as accuracy, precision, recall, and specificity. This comparison between the two techniques proves that Discrete Cosine Transform is more accurate in detecting the morphed regions.*

***Key Words*: Discrete Cosine Transform (DCT), Forgery Detection, Image Morphing, Performance Parameters, Zernike Moment.**

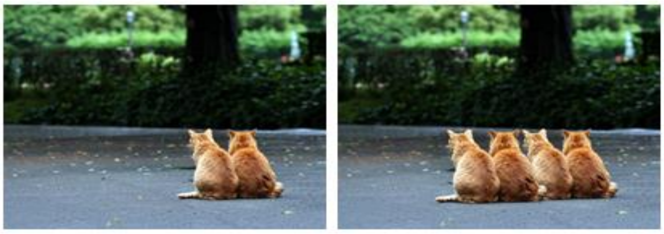
1. INTRODUCTION

Image forensics investigation is an emerging branch of image processing, which is aimed at obtaining quantitative confirmation on the origin and honesty of a digital image. One of the vital errands of image forensics is the discovery of picture manipulations. Tampering intends to meddle with something keeping in mind the end goal to cause harm or make unapproved changes. Pictures are dealt with as evidence in different situations and along these lines; picture altering is characterized as deliberate control of pictures for malicious purpose. Image tampering dates its origin to the earliest twentieth century when it was used for political propaganda. Image tampering is not a rare phenomenon and accordingly, the most recent decade stamped enormous improvements in the field of image forensics.

Image morphing is a process of generating an animated sequence of images from one image to another or making changes in the same image. Morphing is derived from the word "metamorphosis" and involves the image processing techniques of warping and cross-dissolving. Manipulation of digital images in different fields like an official courtroom and medical imaging create a serious issue. With quick advances in digital image processing software, there is a broad improvement of cutting-edge instruments and procedures for computerized picture imitation. This availability carried with it new difficulties concerning the trustworthiness and genuineness of digital documents, in particular, images. Advanced cameras and photo-editing programming bundles are utilized to make and alter computerized pictures effortlessly and manipulate it without leaving any obvious hints of having been modified.

As compared to the past, morphing is utilized vigorously today. Though the impact was at first a curiosity, today morphing effects are most often designed to be seamless and imperceptible to the stripped eye. This demands a reliable image forgery detection system. In spite of the fact that these manipulations are often not identified by the human eye, they do influence the statistics of the picture and in view of this; the detection of tampering is conceivable.

The most common type of image forgery is known as copy-move forgery. In copy-move forgery, a part of the image is copied and pasted somewhere else within the image. Detection techniques of copy-move forgery were developed to identify the copied regions and their pasted ones, however, detection may fluctuate in light of whether there has been any post-processing on the replicated part before pasting it to another part. Usually, attackers will do some operations such as rotation, filtering, JPEG compression, resizing and noise addition to the original part before pasting, and these operations make it difficult to detect copy-move forgery. Therefore, forgery detector should be robust to all such manipulations.



(a) Original Image (b) Tampered Image

Fig -1: Copy-move Forgery

2. LITERATURE REVIEW

Minati Mishra et al [1] proposed a comprehensive study of the brief history of image tampering and a state-of-the-art review of the tamper detection techniques [2][3].

Amandeep Kaur et al [4] presented a review of the various forgery basics and various types of digital image forgery and forgery detection techniques [5].

Resmi Sekhar [6] presents a paper on a survey on the recent developments in block-based methods and Key-point based methods.

Harpreet Kaur et al [7] proposed use of discrete cosine transform with a combination of Sobel edge detection on an input image to detect copy-move forgery. The input image is first compressed then it is divided into 8*8 overlapping blocks and correlation is computed between blocks to extract the forged region. Edges of the forged region are detected by Sobel edge detection. Proposed method improves the detection time, precision, recall, and accuracy. Walaa M. Abd-Elhafiez et al [8] proposed a paper to explain the color image compression based on the DCT blocks. Mehdi Ghorbani et al [9] demonstrated the steps to perform DCT on an input image to detect the copy move forgery.

Junfeng He et al [10] proposed DQ Effect Analysis in Doctored JPEG Images.

S.Murali et al [11] proposed 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.

Nishmitha M R, Aravind Naik [12] proposed a paper helping us to understand the best method for image forgery detection is Discrete Cosine Transform against the other two alternative methods; Weber local descriptor, Histogram Oriented Gradient. DCT can be used to effectively detect copy-move forgery.

Naincy et al [13] proposed an enhancement of copy-move image forgery detection by implementing a hybrid of block-based method DCT (Discrete Cosine Transform) and key-point based method SIFT (Scale-Invariant Feature Transform).

Madhu et al [14] proposed a histogram-based totally method for quantization step estimation. The proposed technique also indicates its accuracy in other practical forensic situations which includes estimation of the secondary quantization table in a double-JPEG compressed photo stored in a lossless format, and JPEG compression identification.

Yujin Zhang et al [15] proposed local binary pattern operator to be used to model magnitude components of two-dimensional arrays obtained by applying multi-size block discrete cosine transform to test images. Then, all of the bins of histograms computed from local binary pattern codes are served as discriminative features for image-splicing detection.

Nilesh P Ghatol et al [16] proposed an approach which effectively detects the morphed image with the presence of demosaicing in a digital image. The algorithm validates two things: distinguishing original images from the manipulated ones and accurately localizing tampered image regions.

P. Bhaskara Rao et al [17] proposed feature extraction using Zernike moment algorithms [18] for a set of alphabets.

Rajeev et al [19] proposed a new approach for detecting copy-move forgery in digital images using statistical moments and two-dimensional discrete cosine transform. A sliding window was centered around every pixel of the input image. The DCT is applied to obtain the quantized coefficient matrix. The low dimensional features of the quantized coefficient matrix are arranged in a feature matrix F. The columns of F contain 4 - statistical features, i.e., mean Me, variance Var, third order moment skewness Sk and fourth order moment kurtosis Kr. In order to make similar windows adjacent, the feature matrix F is lexicographically sorted using radix sort. The proposed method has the lower dimension feature vector with lower computational complexity.

Seung-Jin Ryu et al [20] proposed the use of Zernike Moments for the detection of copy-move forgery that is algebraically invariant against rotation and also resilient to the intentional distortions such as additive white Gaussian noise, JPEG compression, and blurring.

3. DISCRETE COSINE TRANSFORM (DCT)

DCT is the most widely used transform in the image processing applications for feature extraction. DCT represents a sum of sinusoids of varying magnitudes and frequencies. The approach involves taking the transformation of an image as a whole and separating the relevant coefficients. The picture is divided into a 16x16 sliding window in which each 8x8 block is subjected to discrete cosine transform (DCT) to calculate the frequency components. The DCT of an image basically consists of three frequency components namely low, middle, high each containing some detail and information in an image. The higher frequency components contribute lesser to the image hence their values can be reduced to zero by quantization table (matrix) as shown below. This eliminates their effect on the compressed image. [21]

$$\begin{bmatrix} 313 & 56 & -27 & 18 & 78 & -60 & 27 & -27 \\ -38 & -27 & 13 & 44 & 32 & -1 & -24 & -10 \\ -20 & -17 & 10 & 33 & 21 & -6 & -16 & -9 \\ -10 & -8 & 9 & 17 & 9 & -10 & -13 & 1 \\ -6 & 1 & 6 & 4 & -3 & -7 & -5 & 5 \\ 2 & 3 & 0 & -3 & -7 & -4 & 0 & 3 \\ 4 & 4 & -1 & -2 & -9 & 0 & 2 & 4 \\ 3 & 1 & 0 & -4 & -2 & -1 & 3 & 1 \end{bmatrix} \div \begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix} =$$

8 x 8 DCT Terms Quantization table (Matrix)

$$\begin{bmatrix} 20 & 5 & -3 & 1 & 3 & -2 & 1 & 0 \\ -3 & -2 & 1 & 2 & 1 & 0 & 0 & 0 \\ -1 & -1 & 1 & 1 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Result

The DCT equations can be represented mathematically as,

$$y(k) = w(k) \sum_{n=1}^{N} x(n) \cos\left[\frac{\pi(2n-1)k-1}{2N}\right] \qquad k = 1,2,\ldots N$$

$$\text{Where } w(k) = \begin{cases} \sqrt{\frac{1}{N}} & if\ k = 1 \\ \sqrt{\frac{2}{N}} & 2 \le k \le N \end{cases},$$

where x,y is a matrix of row or column, N is the size of the matrix.

The first coefficient in this matrix is known as the DC component, representing the average intensity of an image, while the rest are the AC coefficients corresponding to high-frequency components of an image. It is proved that high-frequency information by itself is insufficient for good forgery detection performance. The elimination of the high-frequency components also causes an image to be robust to scale variations which are required in Face Recognition (FR) systems. The top left entry referred to as the DC coefficient, stores the amplitude and the base frequency.

In DCT algorithm, the input image is a color image. It is converted to a grayscale image using the standard formula,

$$I = 0.299R + 0.587G + 0.114B.$$

RGB represents the three color components of RGB color model: Red, Green, and Blue. An image is divided into overlapping blocks for feature extraction. We can use DCT coefficients for feature extraction. DCT will compress all rows and columns of an image due to which blocking artifact is introduced in the compressed image [22]. Then, the image is divided into fixed size overlapping blocks of B*B pixels. Further, the coefficients of blocks are lexicographically sorted. After lexicographical sorting, similar blocks are detected and forged regions are found. Finally, robust retouching operations in an image are performed to declare the result as a morphed image or not. Then, performance parameters such as precision, recall, specificity, and accuracy are calculated.

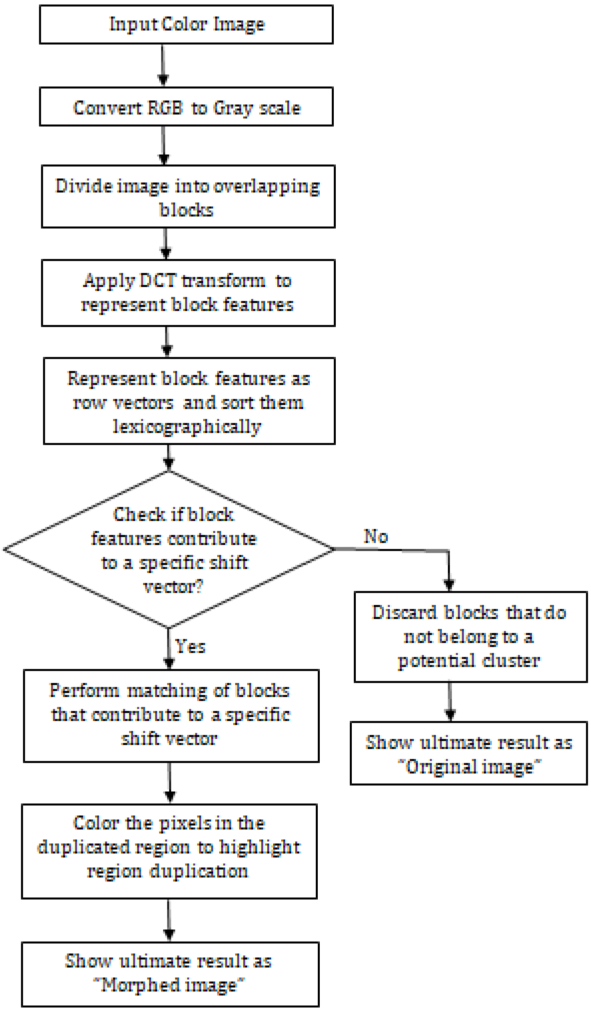

Input Color Image
Convert RGB to Gray scale
Divide image into overlapping blocks
Apply DCT transform to represent block features
Represent block features as row vectors and sort them lexicographically
Check if block features contribute to a specific shift vector?
No
Yes
Discard blocks that do not belong to a potential cluster
Show ultimate result as "Original image"
Perform matching of blocks that contribute to a specific shift vector
Color the pixels in the duplicated region to highlight region duplication
Show ultimate result as "Morphed image"

Chart -1: DCT algorithm flow chart

4. ZERNIKE MOMENT

The image f of size M x N is divided into overlapped sub-blocks of L x L to calculate Zernike moments. Each block is denoted as B_{ij}. [20]

$$B_{ij}(x,y) = f(x+j, y+i)\ ,$$
$$\text{where } x,y \in \{0,\ldots,L-1\},\ i \in \{0,\ldots,M-L\}, \text{and } j \in \{0,\ldots,N-L\}$$

N-blocks of overlapped sub-blocks are obtained where N-blocks = (M-L+1) x (N-L+1). Then, the Zernike moments A_{ij} of a degree n are calculated from each block and vectorized. The total number of moments in the vector is given by,

$$N_{moments} = \sum_{i=0}^{n} \left(\left\lfloor \frac{i}{2} \right\rfloor + 1 \right)$$

Then, 'Z' is constructed which consists of a set of vectorized magnitude values of moments A_{ij} of all N-blocks. The set Z can be represented as shown below:

$$\mathbf{Z} = \begin{bmatrix} |\mathbf{A}_{00}| \\ \cdots \\ |\mathbf{A}_{(M-L)(N-L)}| \end{bmatrix}$$

The set **Z** is then lexicographically sorted since each element of **Z** is a vector. The sorted set is denoted as $\hat{Z}_p$.

$$\hat{Z}_p = (\hat{Z}_{1P}, \hat{Z}_{2P}, \hat{Z}_{3P}, \ldots\ldots\ldots\ldots\ldots\ldots, \hat{Z}_{(Nmoments-1)P}, \hat{Z}_{(Nmoments)P})$$

After the moments are calculated, each pair of moments in set $\hat{Z}_p$ will be compared using the Euclidian distance between the adjacent pair of $\hat{Z}_p$.

$$\hat{Z}_{P+1} = (\hat{Z}_{1P+1}, \hat{Z}_{2P+1}, \hat{Z}_{3P+1}, \ldots, \hat{Z}_{(Nmoments-1)P+1}, \hat{Z}_{(Nmoments)P+1})$$

If the Euclidean distance is lesser than the pre-defined threshold D1, then the pair of blocks is considered as a pair of candidates for forgery.

The condition for forgery: $\sqrt{\sum(Zp - Zp + 1)} < D_1$

However, the blocks that are near each other may have the similar characteristic of Zernike moments; the actual distance between each block is calculated as:

$$\sqrt{(i-k)^2 + (j-l)^2} < D_2$$

Where, $\hat{Z}_p = |A_{ij}|$ and $\hat{Z}_{P+1} = |A_{kl}|$. Finally, the investigated blocks are determined as duplicated or original.

5. PERFORMANCE PARAMETERS

To compare any two algorithms and determine the most effective approach, certain performance parameters are required. We use precision, accuracy, recall, and specificity parameters [7] which are defined as follows:

Precision: A precision rate is the ratio of a number of correctly detected images to the sum of correctly detected images plus false positive. It is also called positive predictive rate. If the value of precision is high it indicates less false positive. Precision represents the probability of truly detecting a forgery. Mathematically,

Precision = TP/ (TP+FP)

Accuracy: Accuracy is used to calculate the proportion of true positive and true negative in all evaluated cases. Higher the accuracy, higher will be the success rate of the algorithm. Accuracy is calculated by using below formula:

Accuracy = (TP+TN)/ (TP+FP+TN+FN)

Recall: A recall rate is the ratio of correctly detected images to the sum of correctly detected images plus false negative. If the value of recall is high it indicates less false negative. The recall represents the probability that a forged image has been detected; it may be either true or falsely forged. The recall is also called as a true positive rate (TPR) or sensitivity. Mathematically,

Recall = TP/ (TP+FN)

Specificity: Specificity measures the ability of a test to correctly exclude the condition (not detect the condition) when the condition is absent. Specificity can be calculated using the following formula:

Specificity = TN/ (TN+FP)

To calculate these performance parameters it is required to first obtain the values of the following evaluative measures.

The possible test results are as follows:

1. A true positive (TP) test result is one that detects the condition when the condition is present.
2. A true negative (TN) test result is one that does not detect the condition when the condition is absent.
3. A false positive (FP) test result is one that detects the condition when the condition is absent.
4. A false negative (FN) test result is one that does not detect the condition when the condition is present.

Considering the image level, some of the important measures are described below:

Evaluation Measures	Description
True Positive (TP)	A number of images that have been correctly detected as forged.
False Positive (FP)	A number of images that have been falsely detected as forged.
True Negative (TN)	A number of images that have been falsely missed but they are forged.
False Negative (FN)	A number of images that have been correctly missed but they are not forged.

Table -1: Evaluative measures and their description

It can be represented diagrammatically as follows. Here, the condition is "morphing" and the test is the "result obtained". If the condition is present then it means that the image has been morphed and if the condition is absent then it means that the image is original and has not been morphed. A test result is either "positive" or "negative", which may be "true" or "false". If the test is positive then it means that the image has been detected as a morphed image and if the test is negative then it means the image has been detected as original and not morphed.

		condition	
		present	absent
Test	positive	true positive	false positive
	negative	false negative	true negative

Table -2: Diagrammatic representation of possible test results

6. EXPERIMENTAL RESULTS

Discrete Cosine Transform (DCT) and Zernike Moment algorithms were both tested with 108 images each. Out of 108 images, 54 images were original (not tampered) and 54 images were morphed. When the input was an original image the possible results were True Positive (TP) and False Negative (FN). When the input was a morphed image the possible results were True Negative (TN) and False Positive (FP). The number of TP, FN, TN AND FP values for DCT and Zernike Moment was tabulated as shown below:

Images →	Morphed Images		Original Images	
Methods ↓	**TP**	**FN**	**TN**	**FP**
DCT	51	4	46	7
Zernike Moment	42	13	31	22

Table -3: Evaluative measures values

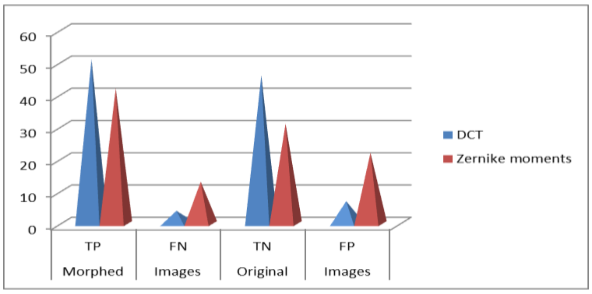


Chart -2: Graph showing evaluative measure values comparison

Using the above evaluative measures, the performance parameters were calculated and tabulated as shown below:

Parameters	**DCT**	**Zernike Moment**
Precision	87.93%	65.625%
Accuracy	89.81%	67.59%
Recall/Sensitivity/True Positive Rate (TPR)	92.73%	76.36%
Specificity/ True Negative Rate (TNR)	86.79%	58.49%

Table -4: Performance parameters values

Another parameter on which DCT and Zernike Moment can be compared is the detection time/ elapsed time. Elapsed time is the time taken to detect the presence of morphing in a specified digital input image. The elapsed time of DCT was found to be lesser than Zernike Moment.

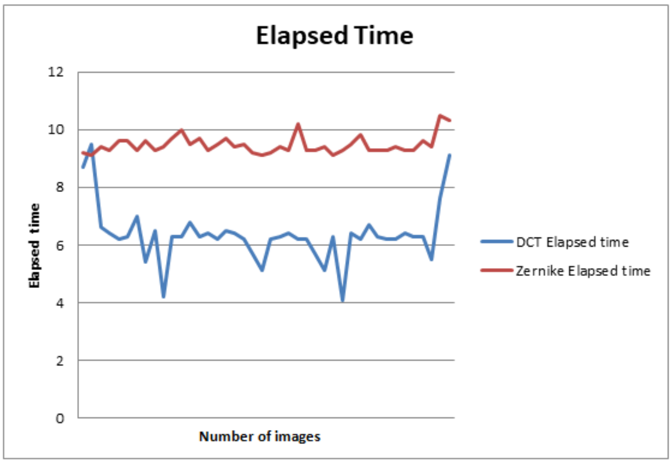


Chart -3: Graph showing elapsed time comparison

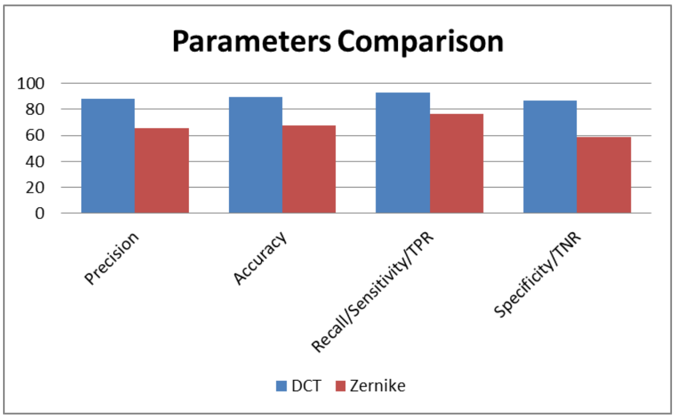
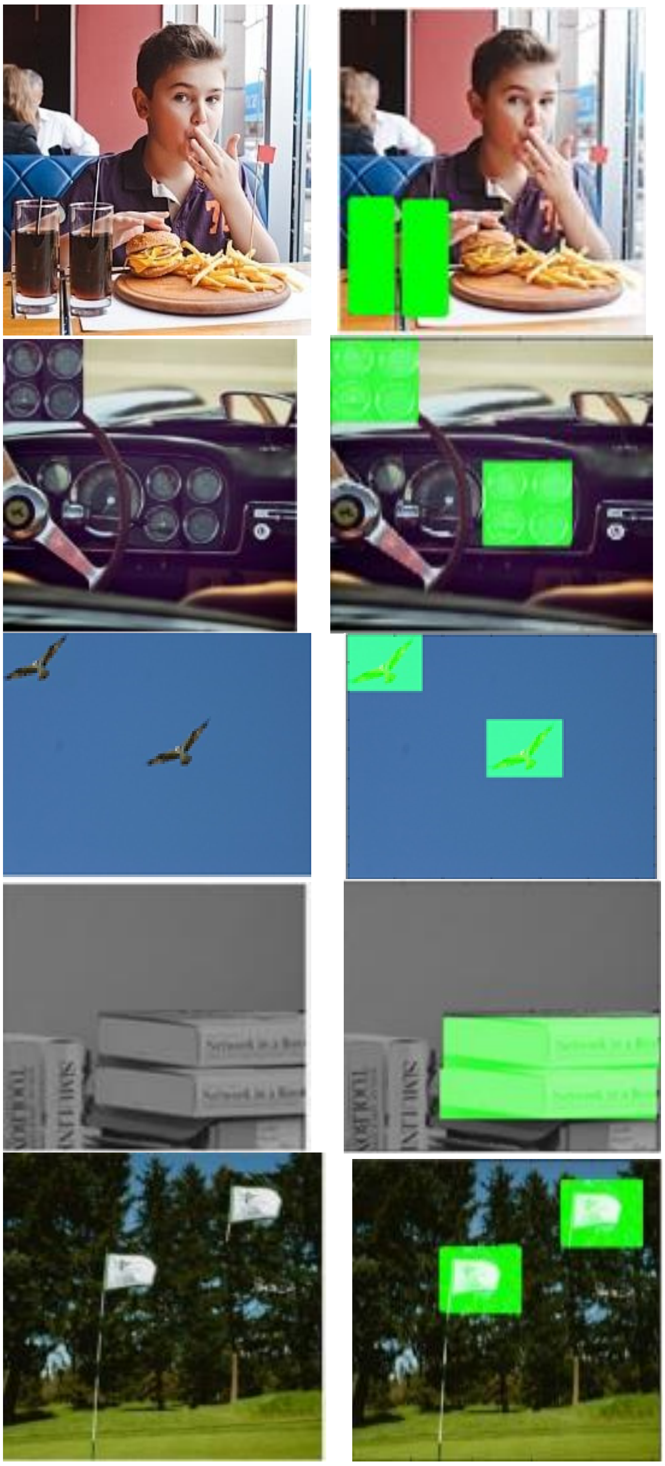


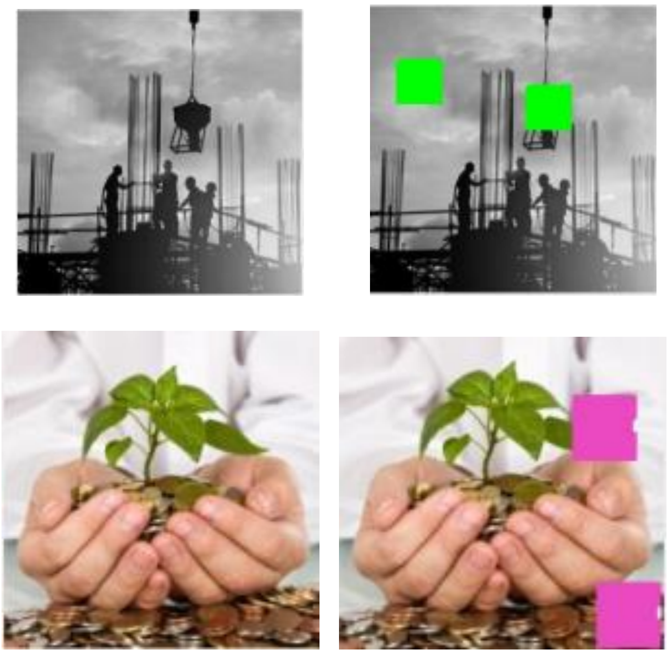
Chart -4: Graph showing performance parameter values comparison

RESULTS:



(a) Morphed Images (input) (b) Result Images (output)

Fig -2: True Positive Results

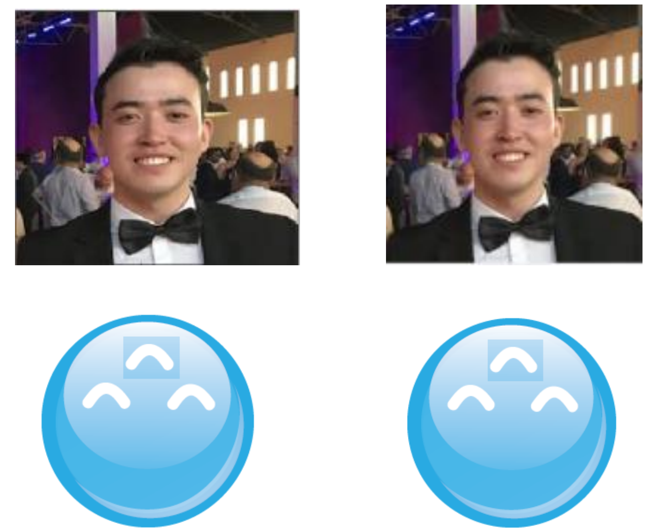


(a) Original Images (input) (b) Result Images (output)

Fig -3: False Positive Results

(a) Original Images (input) (b) Result Images (output)

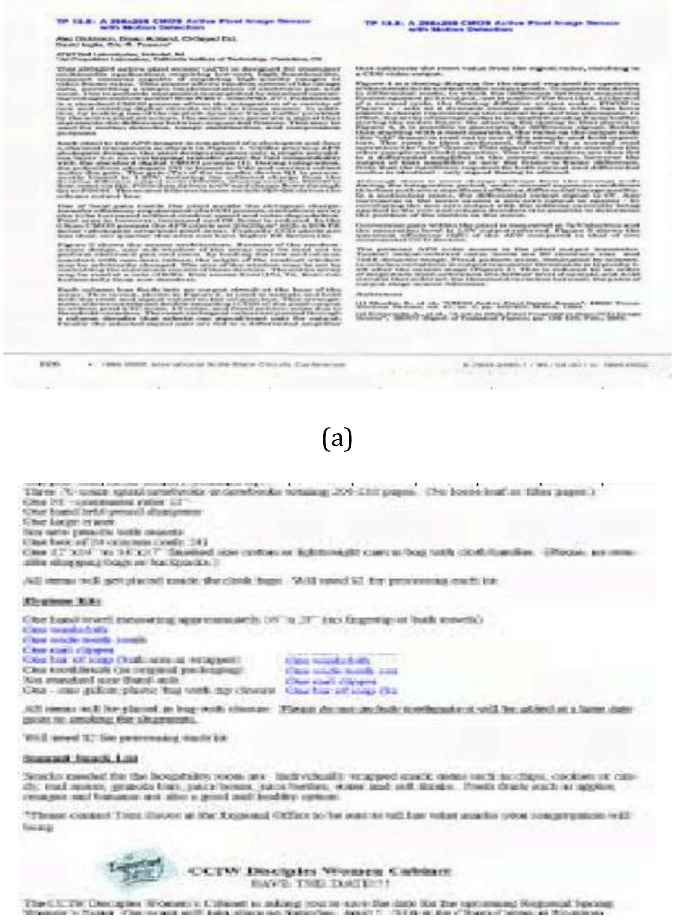
Fig -4: True Negative Results



(a) Morphed Images (input) (b) Result Images (output)

Fig -5: False Negative Results

When images of documents were given as test inputs, copy move forgery was detected and highlighted (blue) as shown below.



TP 13.8: A 256x256 CMOS Active Pixel Image Sensor with Motion Detection

[illegible]

(a)

[illegible]

CCTW Disciples Women Cabinet
SAVE THE DATE!!

[illegible]

(b)

Fig -6: Document Image Results

7. CONCLUSION AND FUTURE SCOPE

This paper involves use of DCT and Zernike moments for Copy move forgery detection with an aim to resolve the issues in the detection process. From the measure of performance parameters, it is confirmed that Discrete Cosine Transform is a more effective approach to detect copy move image forgery. The algorithms show robustness in accurately detecting the location of single or multiple, small or large forged regions of regular or irregular shapes. The future scope of this project is that DCT can be used in combination with other transforms such as Discrete Wavelet Transform (DWT) or DyWT to increase the accuracy of detection. The work can be extended to make the detection more robust to various types of attacks like noise addition, blur addition, compression, scaling, rotation, compression, and the combination of rotation plus scaling. The work can also be extended to locate copy move forgeries in videos.

REFERENCES

[1] Minati Mishra, Dr. M. C. Adhikary," Digital Image Tamper Detection Techniques -A Comprehensive Study", International Journal of Computer Science and Business Informatics, Vol. 2, No. 1. June 2013.

[2] Gayatri Dakhode, P Kumar Chourey," Forensic Technique for Detection of Image Forgery", International Journal of Advanced Engineering Research and Science (IJAERS), Vol-4, Issue-1, Jan- 2017.

[3] Abhishek Kashyap, Rajesh Singh Parmar, Megha Agarwal, Hariom Gupta,"An Evaluation of Digital Image Forgery Detection Approaches". March 2017.

[4] Amandeep Kaur, Jyoti Rani: " Digital Image Forgery and Techniques of Forgery Detection: A brief review", International Journal of Technical Research & Science, Volume 1 Issue 4, July 2016.

[5] C.Rajalakshmi, Dr.M.Germanus Alex, "STUDY OF IMAGE TAMPERING AND REVIEW OF TAMPERING DETECTION TECHNIQUES", International Journal of Advanced Research in Computer Science, Volume 8, July – August 2017.

[6] Resmi Sekhar, Chithra A.S: "Recent Block-based Methods of Copy-Move Forgery Detection in Digital Images", International Journal of Computer Applications Volume 89 – No 8, March 2014.

[7] Harpreet Kaur, Sheenam Malhotra: "Improving Copy-Move Forgery Detection Time by Using DCT, Correlation and SOBEL Edge Detector", International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 5 Issue I, January 2017.

[8] Walaa M. Abd-Elhafiez, Wajeb Gharibi:"Color Image Compression Algorithm Based on the DCT Blocks ".

[9] Mehdi Ghorbani, Mohammad Firouzmand, Ahmad Faraahi,"DWT-DCT (QCD) Based Copy-move Image Forgery Detection ". January 2012.

[10] Junfeng He, ZhouchenLin, Lifeng Wang, and Xiaoou Tang: "Detecting Doctored JPEG Images via DCT Coefficient Analysis", Springer-Verlag Berlin Heidelberg 2006, Part III, 2006.

[11] S Murali, Govindraj B Chittapur, Prabhakara H.S, Basavaraj S Anami:" Comparison and analysis of photo image forgery detection techniques", International Journal on Computational Sciences & Applications (IJCSA) Vo2, No.6, December 2012.

[12] Nishmitha M R, Aravind Naik:" Comparison of three-technique of image forgery detection", International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) Volume 14 Issue 2, April 2015.

[13] Naincy, Ashok Kumar Bathla: "AN ENHANCEMENT OF COPY MOVE FORGERY DETECTION IN DIGITAL IMAGES USING HYBRID TECHNIQUE ", 2nd International Conference on Science, Technology and Management, September 2015.

[14] Madhu, Jitender Kurmi: "A New Copy-Move Image Forgery Detection Based on DCT", International Journal of Advanced Research in Computer Science. Volume 8, No. 5, May-June 2017.

[15] Yujin Zhang, Chenglin Zhao, Yiming Pi, Shenghong Li, Shilin Wang,"Image-splicing forgery detection based on local binary patterns of DCT coefficients", John Wiley & Sons, Ltd 2013.

[16] Nilesh P Ghatol, Rahul Paigude, Aniket Shirke," Image Morphing Detection by Locating Tampered Pixels with Demosaicing Algorithms", International Journal of Computer Applications (0975 – 8887) Volume 66– No.8, March 2013.

[17] P. Bhaskara Rao, D.Vara Prasad, Pavan Kumar: "Feature Extraction Using Zernike Moments ", International Journal of Latest Trends in Engineering and Technology (IJLTET). Vol. 2 Issue 2 March 2013.

[18] J. H. Salverda," Comparison of different wavefront reconstruction methods With Zernike polynomials", Delft University of Technology.

[19] Rajeev Kaushik, Rakesh Kumar Bajaj, Jimson Mathew: "On Image Forgery Detection Using Two Dimensional Discrete Cosine Transform and Statistical Moments", in 4th International Conference on Eco-friendly Computing and Communication Systems, 2015; 130 – 136.

[20] Seung-Jin Ryu, Min-Jeong Lee, and Heung-Kyu Lee, “Detection of Copy-Rotate-Move Forgery using Zernike Moments”.

[21] Varsha Sharma, Swati Jha, Dr. Rajendra Kumar Bharti, “Image Forgery and it’s Detection Technique: A Review”, International Research Journal of Engineering and Technology (IRJET), Vo3, No.3, March-2016.

[22] Reshma R. Chaudhari, Nutan C. Malekar, Meena B. Vallakari, Kushal Suvarna, “DCT based Forgery Detection Technique in Digital Images”, International Journal of Computer Applications.