International Journal for Modern Trends in Science and Technology
Volume 11, Issue 06, pages 221-225
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol11issue06.html
DOI: https://doi.org/10.46501/ijmtst.26.v11.i06

Evaluation of Image Forgery Detection Techniques using DCT, DWT and QCD

Pooja S. Mali[1] | Dr. Mahesh S. Chavan[2]

[1]*Research Scholar Department of Electronics Engineering Kolhapur Institute of Technology's College of Engineering, Kolhapur Maharashtra, India. ppoojamali1051988@gmail.com*

[2]*Professor, Department of Electronics & Telecommunication Engineering, Kolhapur Institute of Technology's College of Engineering, Kolhapur, Maharashtra, India. chavan.mahesh@kitcoek.in*

To Cite this Article
Pooja S. Mali & Dr. Mahesh S. Chavan (2025). Evaluation of Image Forgery Detection Techniques using DCT, DWT and QCD. International Journal for Modern Trends in Science and Technology, 11(06), 221-225. https://doi.org/10.46501/ijmtst.26.v11.i06

Article Info
Received: 05 June 2025; Accepted: 28 June 2025.; Published: 29 June 2025.

KEYWORDS

Copy move forged detection (CMFD), DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), QCD (Quantization Coefficients Decomposition), SIFT (Scale – Invariant Feature Transform), Hu moments

ABSTRACT

Digital photographs are easily manipulated due to advancements in image processing tools, making it difficult to verify their authenticity. Copy and move type forgery, where a part of an image is duplicated and pasted in another location, reduces the image's dependability. A hybrid algorithm based on DWT and DCT is proposed to detect such cloned forgeries. In the proposed work we have used and hybrid algorithm which is based on DWT and DCT that is used to detect such kind of cloned forgery. The suggested technique reduces the dimensional representation of the image by first compressing it using DCT and then DWT. The compressed image above is then separated into overlapping chunks. After that, duplicate blocks are identified using a lexicographic technique. Compared to individual DCT or DWT, this method improves accuracy at the expense of a small increase in detection time. It decomposes the image through DCT and Hu moments features are extracted vector from a circle block for detection and localization of forged areas. The proposed technique dose precise detection and localization of all kinds of copy & move areas also if some kind of post processing operation has been carried out with image.

I. Introduction

Images are increasingly crucial in communication media, providing more information than words. With advanced technology, including camera gear, computer systems, and graphics software, digital photos are essential in sectors like media, defense, news, and medical examinations. Digital images can be easily edited using various cameras and software, making it difficult to distinguish between original and altered photos. Forgery in Copy & Move case is a type of digital

image fraud where a small block is copied and pasted to hide its contents. The human eye struggles to detect such forgeries, making detection crucial for preventing image fraud. Image forgery detection is crucial in forensic investigations and social media surveillance, allowing for the analysis of evidence for criminal and civil legal processes.

Copy & move type images require thorough search to identify copied and pasted elements, but this method is computationally complex and takes more time to discover. Two popular methods for detecting forgery are block-based and key point-based. Block-based splits images into sections, but can be ineffective for geometric adjustments, while key point-based detects duplicated areas.

Researchers use blocking tactics in DCT-based image detection to identify cloning forgeries. They use lexicographic sort and quantized DCT coefficients to identify duplicates. The Copy-Move detection method improves detection accuracy by focusing on the lowest level picture representation. The survey indicates that DCT and DWT are effective methods, but their localization accuracy is subpar. A hybrid model combining both improves accuracy.

(a) (b)

Figure 1 Copy & move type image Example (a) original image (b) forged image

a. Problem Statement

DWT approaches, often used in image forgery detection, offer advantages such as simplicity and feature vector size reduction, presenting opportunities for further development in performance and accuracy. The computational cost and durability of copy-move forgery detection are determined by parameters like quantization matrix, overlapping block size, and matching pixel occurrence threshold. We propose designing a hybrid model combining DCT and DWT for enhanced accuracy compared to traditional methods.

b. Objectives

Copy-move fraud detection aims to identify identical or similar parts of an image, enhancing accuracy, robustness, localization, performance, and reducing computational complexity.

c. **Motivation**

Image forgery, primarily for financial gain, is a significant issue in various fields, but detection applications can help preserve digital media integrity and increase viewers' confidence in misleading images.

II. LITERATURE SURVEY

The technique of copy-move forgery detection has been the subject of research on a number of current systems, looking at unforeseen outcomes such feature correlation between replicated and original frames. These effects could show up as either frame insertion or replacement. This section offers a thorough analysis of the many Copy-Move Forgery Detection (CMFD) techniques currently in use.The authors introduces IKFR-T (Identical Key Feature Recognition and Tracing), a revolutionary technique for identifying digital photo copy & move frauds. The three main parts of the methodology—recursive localization, similarity testing, and feature extraction—are all optimized for better efficiency. The usefulness of IKFR-T is demonstrated by the results and discussions, which show that it performs better than current models. Evaluation criteria that highlight the methodology's dependability in identifying copy-move forgeries include, True Positive Rate also False Positive Rate and F1-Score [12].

CMF creates a new issue since it minimises the accuracy for picture's forgery detection. Comparable locations have been selected and pasted into CMFD. The suggested technique aids in the detection of picture forgeries and is based on the Equilibrium Optimization Algorithm (EOA), DWT, and DCT. The technique uses the EOA, DWT, and DCT to detect forgery regions, segment images, and detect features. At beginning the image is then has converted to gray scale. Then

transferred to the signal domain using a discrete cosine transform technique [13].

The primary objective of this work was to identify strategies to guarantee the identification of copy-move fraud in digital photos. This paper's primary focus was on identifying the forged items in the suspected image and reducing the feature length dimension. As a result, we used kernel PCA and DCT for feature extraction, considering the same items that were present in the fabricated image. This paper's primary focus was on identifying the forged items in the suspected image and reducing the feature length dimension [14].

In this paper, they have thoroughly examined the CMFD problem. The CMFD techniques have been grouped based on their detection paradigm, detection methodology and detection capability. Several detection paradigms and approaches has been examined and their pros and cons discussed.The CMFD is still an unsolved problem and a very difficult one. Due of numerous conflicting challenges, most CMFD approaches have not yet attained acceptable enough performance. As a result, more effort needs to be done to resolve several competing issues, and the CMFD problem requires extensive research and the use of a variety of deep learning techniques [15].

III. PROPOSED METHODOLOGY

In proposed system we are using block-based image forgery detection method. In this section, three techniques are discussed. The first one is DCT, DWT and proposed hybrid method combining DCT and DWT.

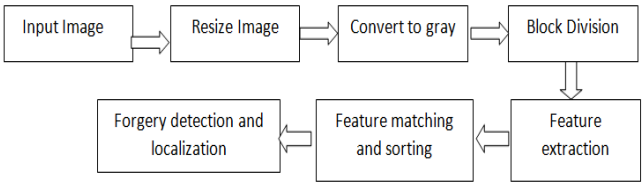

Figure 2 General block diagram of forgery detection method for block-based image

QCD - Quantization Coefficients Decomposition : To identify such copy-move forgeries, we offer an enhanced technique in our suggested system that is based on the DWT and DCT the hybrid method called Quantization Coefficients Decomposition (DCT-QCD). QCD is a DCT and DWT hybrid model Quantization is the process of decreasing the precision of an integer to minimize the number of bits required to store it.

Quantizers lower the precision of values to hold updated coefficients, reducing the number of bits needed for data compression. Scalar quantization and vector quantization are two types, with vector quantization being widely used for data compression due to its benefits. However, codebook design and vector search performance are challenges. Vector quantization is a signal processing method that models probability density functions using prototype vector distribution. It divides large data sets into groups, using centroid values for each. Density matching characteristics help determine high-dimensional data density.

Hu Moments Features: Hu Moments are a set of seven values calculated from image moments that are invariant to image transformations like translation, scale, and rotation. They are commonly used in image recognition and shape classification. While the seventh instant changes sign for a reflected picture, the first six moments remain constant across translation, scaling, and rotation. Since hu moments don't change when an object's size, position, or orientation in the image does, they can be used for shape matching.

IV. IMPLEMENTATION

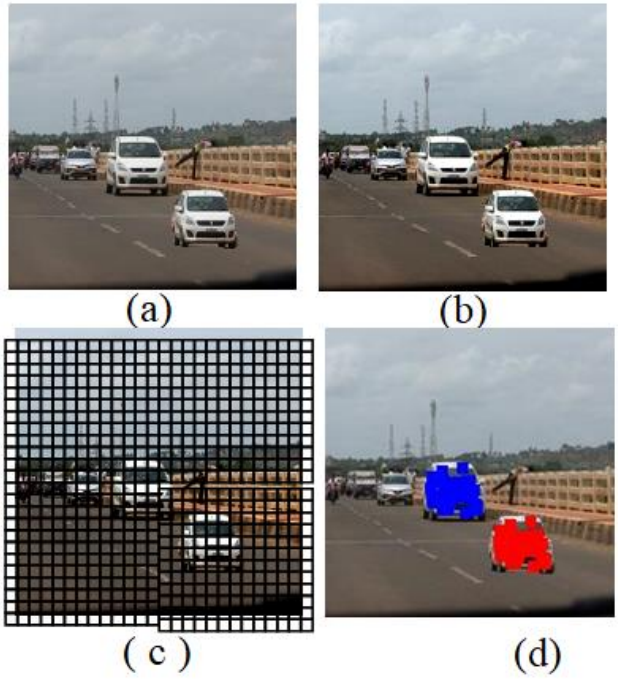

Figure 3 (a) original image (b) Quantized Image (c) block division (d) forged part marked with red colour

After applying DCT the image is divided into blocks of 8x8 ,From each block Hu moment features are extracted and stored. Each block was searched for a matching block; if one was found, it was marked blue, and if not, it

was marked red. As seen in figure 3, the original portions' pixels are marked in blue in the final localization of copy-move forging, while the copy-moved portions' pixels are marked in red. Depending on blue and red matching is predicted as forged or not forged.

QCD Implementation: QCD is a mixture of DWT and DCT; features are extracted from the input image after DCT has been applied. After application of DWT to the input image and extracting its features, the DCT and DWT features are concatenated, and block searching is carried out. The remaining localization is identical to DCT after that.

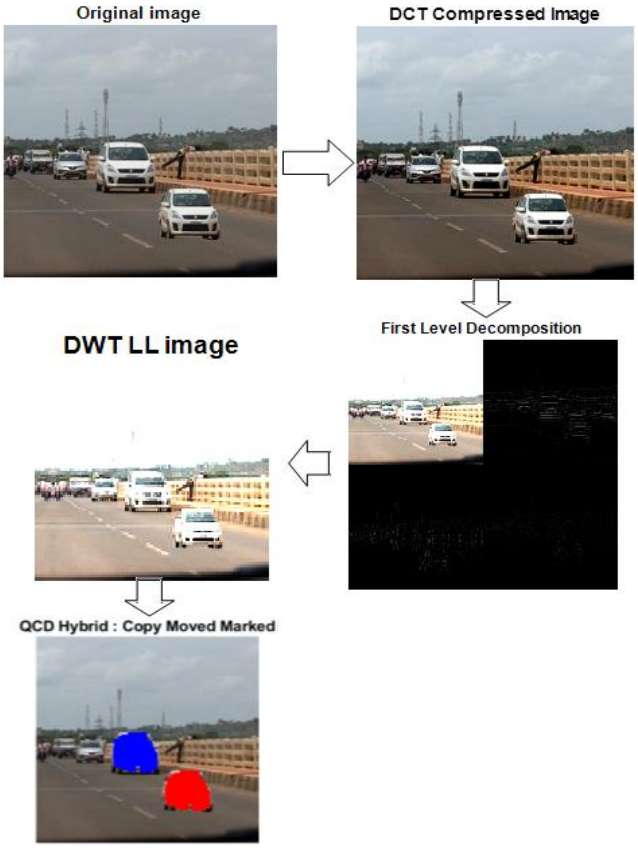

Figure 4 : Step wise results for QCD

V. RESULT & ANALYSIS

Table 1 Comparison of Performance Analysis DCT V/s DWT V/s QCD-proposed method

	DCT	DWT	QCD : DCT + DWT
Forged Detection Accuracy	87.50%	91.67%	95.83%
Average Localisation	37.38 %	47.10%	53.05%

Table 1 shows the comparison between Detection Accuracy of DCT , DWT and Proposed system i.e. QCD

Comparison of Forgery Detection Accuracy

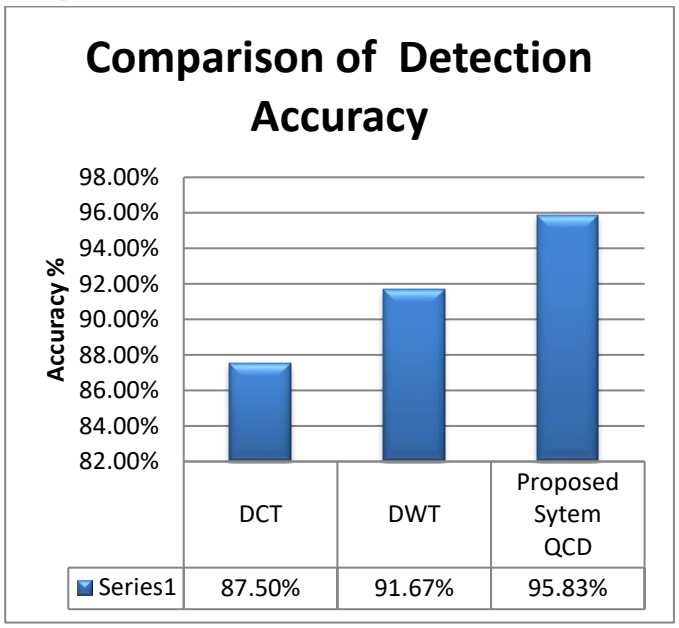

Figure 5 Graph showing Comparison of Detection Accuracy

For the chosen dataset, the accuracy of the DCT technique is 87.50%, the accuracy of the DWT is 91.67%, and the accuracy of the suggested approach is 95.83%, as the graph in Figure 5 illustrates. The graph comparison above demonstrates that the suggested system's accuracy surpasses that of the other two approaches.

Comparison of Forgery Localisation

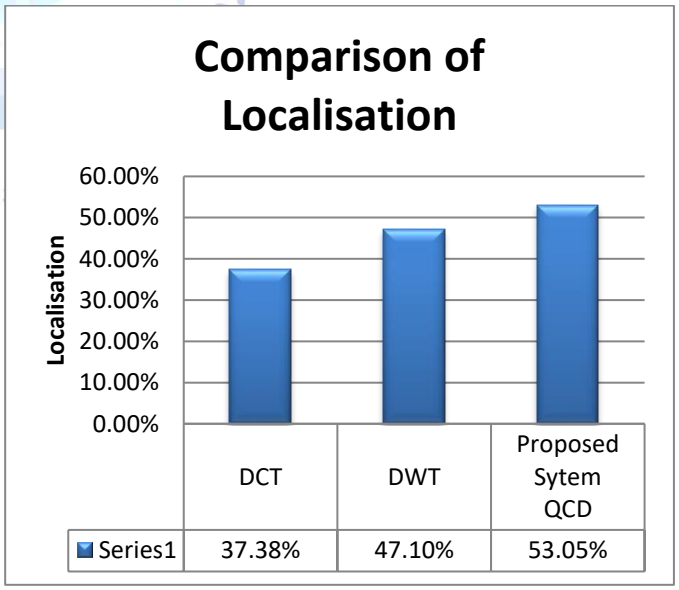

Figure 6 Comparison of Localisation

The graph in Figure 6 displays the localization of copy-move pixels for the chosen dataset; the localization obtained using the DCT approach was 37.38%, the localization obtained using the DWT method was 47.10%, and the localization obtained using the suggested method was 53.05%. The graph comparison

above demonstrates that the suggested system's localization outperforms the other two approaches.

VI. CONCLUSION

To detect digital image copy-move forgeries, this study proposes an improved method using DWT and DCT i.e. QCD. According to experimental results, the dimension of the features using the template is decreased or equaled when compared to the current related techniques, but the detection accuracy is still good. Additionally, a simple but crucial example is given using a toy image to assist students understand the influence of the primary algorithmic processes at the pixel level. We intend to remove the constraint on the location of pasted sections in the future and search for features that can withstand excessive compression, rotation, and rescaling.

The accuracy of the DWT is 91.67%, the DCT method is 87.50%, and the suggested system, or QCD, is 95.83%. DCT, DWT, and QCD localization percentages are 37.38%, 47.10%, and 53.05%, respectively. The performance of the suggested approach is superior to that of the other methods, according to the results

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Irene Amerini and Lamberto Ballan," A SIFT Based Forensic Method for Copy Move Attack Detection and Transformation Recovery." IEEE transactions on information forensics and security, vol .6, no.3 September 2011

[2] Tiziano Bianchi and Alessandro piva," Image Forgery Localization via Block-Grained Analysis of JPEG Artifacts." IEEE transactions on information forensics and security, vol.7, no.3, June 2012

[3] Guo-Shiang Lin, Min-Kuan Chang and You-Lin Chen," A passive -Blind Forgery Detection Scheme Based on Content-Adaptive Quantization Table Estimation." IEEE transactions on circuits and systems for Video technology, vol 21, no.4, April 2011

[4] Er. Sajida Khan and Er. Arun Kulkarni," An Efficient Method for Detection of Copy-Move forgery using Discrete Wavelet Transform." International journal on computer science and engineering vol.02, no.05,2010,1801-1806

[5] Matthew C. Stamm and K.J. Ray Liu," Forensic Detection of Image Manipulation using Statistical Intrinsic Fingerprint." IEEE transaction on information forensics and security, vol.5, no.3, September 2010.

[6] B.L. Shivakumar and Dr.S. Santosh Baboo," Detecting Copy-Move forgery in digital Images: A survey and analysis of current methods Global journal of computer science and Technology vol.10 issue 7 Ver 1.0 September 2010.

[7] Alian C. Popescu and Hany Farid," Exposing Digital Forgeries by Detecting Traces of Resampling". IEEE transactions on signal processing, vol.53, no.2, February 2005

[8] Huazhu Fu and Xiaochun," Forgery Authentication in Extreme Wide angle Lens using distortion cue and Fake Saliency Map." IEEE transactions on information forensics and security, Vol .7, no.4, august 2012.

[9] M.K Bashar and N. Ohnishi," Exploring Duplicated Regions in Natural Images"2010 IEEE.

[10] Zhang Ting and Wang Rang-ding," Copy -Move Forgery Detection based on SVD in digital Image". 978-1-4244-4131-0/09/2009 IEEE

[11] Jie Hu, Huaxiong Zhang and Qiang Gao," An Improved Lexicographical Sort algorithm of Copy Move Forgery Detection." 2011 Second international Conference on Networking and Distributed Computing.

[12] Mohan D N, Dr Santosh Kumar Yadav, "Efficient Copy-Move Forgery Detection through Identical Key feature Recognition and Tracing", International Journal of Novel Research and Development, IJNRD | Volume 9, Issue 5 May 2024.

[13] Ehsan AMIRI, Ahmad MOSALLANEJ, Amir SHEIKHAHMADI, "Copy-Move forgery detection using EOA, DWT and DCT", Pamukkale University Journal of Engineering Sciences – 2023.

[14] Mr. Jaynesh Desai, Dr. Sanjay Buch, "A Depth Analysis on Forgery Detection in Case of Copy-Move Image Forgery", Saarth E-Journal of Research, Vol.8 No.19 Jan-Feb-Mar 2023

[15] Ibrahim A. Zedan, Mona M. Soliman, Khaled M. Elsayed, Hoda M. Onsi , "Copy Move Forgery Detection Techniques", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 12, No. 7, 2021

[16] Esteban Alejandro Armas Vega, Edgar Gonza´ lez Fernandez, "Copy-move forgery detection technique based on discrete cosine transform blocks features", Article in Neural Computing and Applications · May 2021

[17] Muthana S. Mahdi and Saad N. Alsaad, "Detection of Copy-Move Forgery in Digital Image Based on SIFT Features and Automatic Matching Thresholds", Springer Nature Switzerland AG 2020, M. I. Khalaf et al. (Eds.): ACRIT 2019, CCIS 1174, pp. 17–31, 2020.

[18] Zaid Nidhal Khudhair, Dr. Farhan Mohamed, Karrar A. Kadhim, "A Review on Copy-Move Image Forgery Detection Techniques", Journal of Physics: Conference Series 2021

[19] Avleen kour, Dr. Vibhakar mansotra , "Copy-Move Forgery Detection using Discrete Wavelet Transform (DWT) Method" , International Research Journal of Engineering and Technology (IRJET) , Volume: 06 Issue: 07 | July 2019

[20] Suvarna G. Upase , Sunil V. Kuntawar , "Copy-Move Detection of Image Forgery by using DWT and SIFT Methodologies" , International Journal of Computer Applications (0975 – 8887) Volume 148 – No.7, August 2016.