TPM Vol. 32, No. S8, 2025
ISSN: 1972-6325
https://www.tpmap.org/



# DIGITAL IMAGE AUTHENTICATION: CHALLENGES AND STRATEGIES IN FRAUD DETECTION

DR. SHUDHODHAN BOKEFODE[1*], DR. RAMESH SHAHABADE[2], DR. KISHOR SAKURE[3], DR. ROHINI PALVE[4], DR. VARSHA BADADE[5], DR. JAYESH SARWADE[6]

[1,2,3,4,5]TERNA ENGINEERING COLLEGE, NERUL NAVI MUMBAI, MAHARASHTRA 400706, INDIA
[6]JSPM'S RAJARSHI SHAHU COLLEGE OF ENGINEERING, TATHAWADE, PIMPRI-CHINCHWAD, MAHARASHTRA 411033, INDIA
[1]EMAIL: shudhodhan358@gmail.com, ORCID ID: https://orcid.org/0000-0003-4144-0267

**Abstract**: Digital images must now be authenticated since they are a critical source of information in this day and age. A variety of free and for-profit image altering programmes have thrown into doubt the validity of picture contents due to the expanding accessibility of digital devices. There are several forging techniques available, both invasive and non-intrusive. Attackers carry out these activities with the intent of causing harm to persons and websites, as well as for financial gain, extortion, and other purposes. Image fraud detection is getting increasingly difficult to detect as image processing technology advances. Two common picture adjustment strategies are copy-move and cut- glue imitation. As a result, the creation of the plot ought to offer an adequate arrangement to the associated issue of frauds arrangement. Consequently, the detecting procedure demonstrates how the forgery was created over the image with accuracy, and then confirms and fixes the problem by making consistent modifications to the image within the same patch

**Keywords:** Digital forensics, discrete fractional wavelet transforms, Genetic algorithm, image forgery.

## INTRODUCTION

Users today share endless digital photographs not just on social networking sites, but also in news articles, insurance claims, courtrooms, and other places. The emergence of commercially accessible picture editing software has contributed significantly to the increase in our daily use of digital photographs. The doctored images can be used as a deception weapon to conceal the truth. Changed visuals in digital media (TV and newspapers, for example) may fool viewers since crucial elements may be replicated or disguised in the pictures. [1]. This demonstrates that photo fraud is a big problem, and as a result, digital image forensics specialists have lately begun to be concerned about it [2-5]. Numerous tamper detection methods have been reported in the literature, and they can be categorised as either active procedures or passive (blind) methods [6–8]. The simplicity of these technologies has simplified photo editing. Two methods for altering photographs are image forgeries and image steganography. Although image steganography and image forgeries both alter images, their techniques vary [9–11]. Picture steganography, advanced marks, and watermarking are cases of dynamic methods that include information to the first picture. Scientific investigation employments the inserted information to confirm the judgment of the picture substance by comparing it to the extricated information Active image processing approaches necessitate the use of specialized hardware and software [6-8].

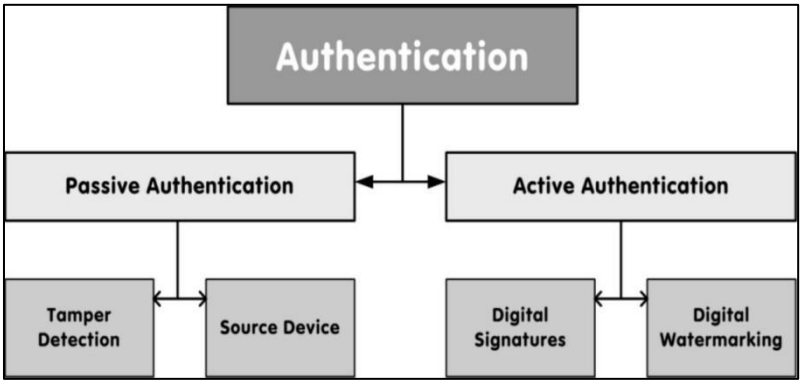


**Figure 1: Techniques for Authenticating Images.**

The results of digital image counterfeit detection methods can be divided into two categories: (a) original or manipulated (without localization); (b) identify the manipulated parts within the same image when the image was created [12]; This article presents a passive CMF detection technique for determining if an input image is legitimate or has been altered. We use both the Discrete Cosine Transform (DCT) and the Genetic Algorithm (GA) to accurately detect the CMF. The main reasons for using DCT are its improved spatial localization capabilities and spectral enhancement.

- Use of smaller feature vectors reduces computational difficulty in tamper detection.
- Ability to successfully find many CMFs in digital images.
- Safe to post-processing assaults such as interpretation, obscuring, JPEG compression, color dithering, and brightness changes

The practise of forging documents has become so commonplace that it may be categorised in a number of ways; all of these instances are divided into three groups based on the method employed to create false documents, namely image retouching, picture splicing, and copy-move attack [6]. The act of changing an image to hide important or favourable information is known as picture forgery. Forgeries using cut-and-paste and copy-and-move are two common picture alteration methods. The ponder of assessing a picture that has experienced morphological adjustment as a result of the application of the related actuated instrument is known as Duplicate Move Imitation Location (CMFD). The CMFD is designed to be used with images when objects need to be copied from one place and moved to another inside the same image.

Pictures are adjusted utilizing different procedures such as obscuring, revolution, commotion era, scaling and compression [12]. Picture extortion has gotten to be simpler than ever with the improvement of mixed media innovation and preparing instruments. Despite its benefits, digital photography can ruin lives, relationships, and government efforts if left unregulated. This method can quickly improve the function of the aforementioned problem by reducing computational complexity through dimensionality reduction [3]. Planning should therefore provide a rational solution to the underlying problem of producing counterfeit goods. Since images on the same patch change frequently, the detection technique accurately detects the appearance of fakes across images, checks for problems, and corrects them [11]. In his second section of the study, you can learn about early efforts to become aware of changing situations. Section 4 describes the best way to find overlapping areas on photos. Section 5 describes the experiments performed to demonstrate the applicability of the strategy, and Section 7 summarizes the expected work and results.

## RELATED WORK

Mohammed Hazim, Alkawaz, and other individuals [13] Powerful editing tools are freely accessible, and image altering is simple, quick, and leaves no apparent traces. As a result, proving the authenticity of images is difficult since the human eye cannot tell the difference between the changed and original image. One of the most popular ways for copying and pasting elements of an image while altering with it is the copy-move technique. Simple Cosine The discrete cosine transforms (DCT) is capable of detecting changing regions. However, the block size of overlapping blocks affects performance in terms of accuracy (FP) and recall (FN). In their investigation, the researchers employed the DCT coefficient to identify copy-movie picture fraud. Mahmood, Toqeer, and colleagues [14] provide a trustworthy method for the localization and identification of CMF in digital images. In order to identify fraud, the method extracts SWT-based properties from digital photos. Due to SWT's superior localization skills in both the spectral and spatial domains, it is frequently employed. Due of its remarkable resistance to various changes. Yang, Bin, et al. [15] created many feature-based CMFD methods. Performance might be improved even further, though. Many of them encountered problems with poor key-point matching while working with mirror converted forgeries. Furthermore, numerous feature-based strategies may come up short to identify hardening in case the fashioning zone features a uniform surface. In this work, we propose an unused feature-based His CMFD strategy. An altered SIFT-based finder is utilized to discover the districts of intrigued. An extraordinary key point dissemination strategy was created to equitably disperse the key focuses over the picture. Finally, we use the new SIFT descriptor to describe key properties of CMFD scenarios. Numerous experimental results prove its effectiveness. Due to its exceptional robustness to multiple transformations, Yang, Bin et al. [15] developed a number of his feature-based CMFD techniques. However, performance can be even better. When dealing with mirrored fakes, many people run into the problem that the key points don't match well enough. Furthermore, many feature-based approaches may fail to detect tempering if the forging zone has a homogeneous texture. This article proposes his own feature-based CMFD approach. Locate critical points using a modified SIFT-based detector. Additionally, many feature-based techniques may fail to detect tempering if the forging zone has a uniform texture. In this work, we propose a modern feature-based His CMFD strategy. An adjusted SIFT-based locator is utilized to discover the districts of intrigued. An extraordinary key point dispersion strategy was created to equitably convey the key focuses over the picture. Finally, we use the new SIFT descriptor to describe key properties of CMFD scenarios. Numerous experimental results prove its effectiveness. Due to its exceptional robustness to multiple transformations, Yang, Bin et al. [15] developed a number of his feature-based CMFD techniques. However, performance can be even better. When dealing with mirrored fakes, many people run into the problem that the key points don't match well enough. Furthermore, many feature-based approaches may fail to detect tempering if the forging zone has a homogeneous texture. This article proposes his own feature-based CMFD

approach. Locate critical points using a modified SIFT-based detector. The majority of image-fraud-detection tools cannot detect manipulated areas if noise is added or the area warped, rotated or scaled before overlay. Those thinking of this, here is a blueprint for an equally strong and effective venue doctrine against such photo-extortion. The image is initially left gray scale. The grayscale image is divided into four sub-bands using two-level stationary wavelet transform (SWT) method, and the salient points are recovered by scale-invariant feature transform based on Filter approach. Abstract: The aim of the paper is to examine image forgery detection by transform methods and machine learning. The method approach has always been promising in the case of an image or pattern recognition algorithm. Methods that derive by transforming the image forgery as per Bokefode Shudhodhan Balbhim, Harsh MathurPerformance[23] The transpose through which it can be got are transform like discrete wavelet transistion(DWT), Discrete Cosine Transform (DCT) , Fast Fourier(FFT) Singular Value Decomposition(SVD)), SIFT [20],[22], etc. The transform methods applied have limitation and the detection of forged image distorted. Used with machine learning algorithms, it increases the detection ratio of image forgery. Finally, we will also leverage the machine learning algorithms trends to find out more effective methods of image forgery detection and enhancing its rate of detection as well. There are a lot of classification and clustering algorithms in machine learning to ultilize for image forgery detection. In this paper, experimental evaluation of image forgery detection using transform and machine learning algorithms is discussed. a feature optimizing image forgery detection approach [9]. The proposed method used a glow worm optimization (GWO) algorithm and support vector machine to optimize the features. Shudhodhan Balbhim Bokefoe, Harsh Mathur: [24] The glow worm optimization algorithm was it optimized the lower content of feature (i._FOREACH LEVEL OF FEATURES D3> ALL) such as texture image and improved detection ration . Simulation of proposed algorithm carried out in MATLAB tools and tested Result on reputed copy-move database comofod_samll. The outcomes of the proposed algorithm evaluation say that the propped algorithms are efficient rather than SVM and CNN.

## DIGITAL IMAGE FORGERY DETECTION APPROACHES

### A. Active strategy

Active counterfeit detection systems [1][2] use digital watermarks or embedded signatures to verify or dispute the legitimacy of images. The main limitation of this technique is that encoded watermarks can only be used by persons with appropriate permissions to process images or recording devices.

### B. Passive strategy

Blind or indifferent tactics [3] Fakes are identified using statistical anomalies [4] that occur during the creation or modification of images or camera fingerprints. In differentiate to dynamic strategies, daze approaches don't require information of genuineness. Dazzle forensics he can classify based on six distinctive characteristics. [5] Geometric, physics-based, source camera identification-based, camera-based, format-based, pixel-based, and camera-based. The chart underneath appears the suggested prepare stream.

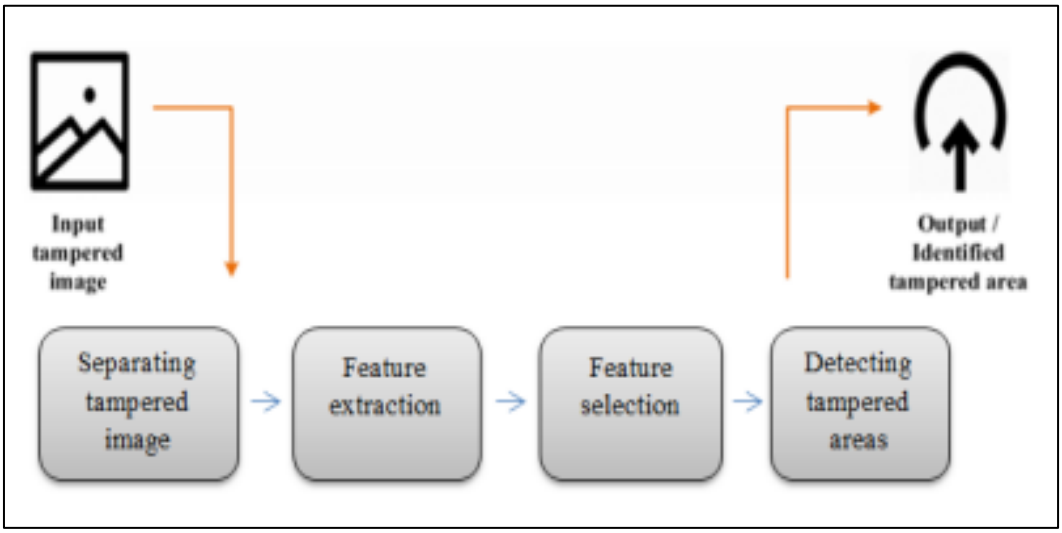


**Figure 2: The method for detecting image faking in action**

### Pixels Extracted

The method combines SLIC super pixel segmentation and VGGNet feature extraction for image analysis. SLIC segments the image into super pixels, which are then mapped to VGGNet's convolutional feature maps. Super pixel features are created by averaging pixel values within these regions. These features are utilized in detecting fake images, with enhancements made to address challenges in low-contrast regions and large image sizes, ultimately improving the accuracy of the detection process.

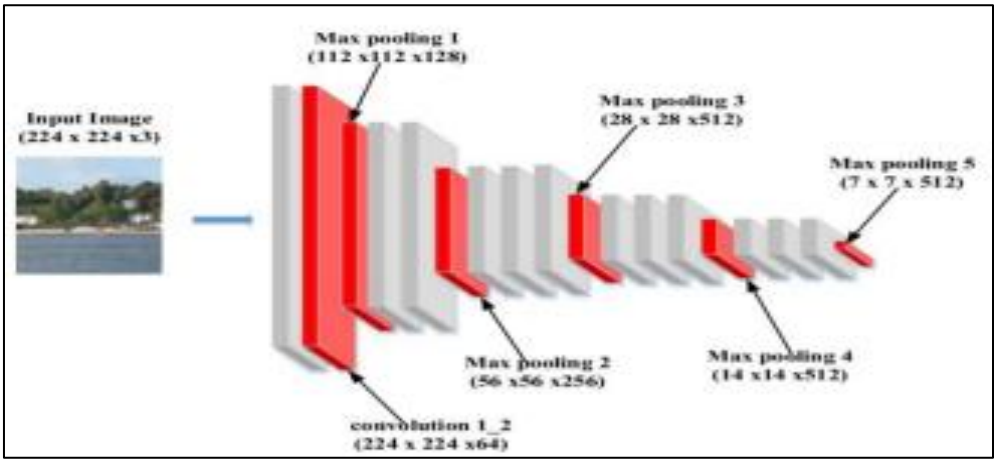


**Figure 3: Utilizing VGGNet to extract features**

**B. Extraction of Features from Segmented Pixels**

The method utilizes feature selection techniques including exponential, randomized, and sequential methods to maintain accurate classification with a smaller set of features. It employs a hill-climbing approach in the consecutive look algorithm for feature evaluation and selection. Modified algorithms such as sliding sequential methods and Successive Floating Forward Selection (SFFS) are used to address nested functionality, ensuring optimal feature subsets are chosen for improved classification accuracy.

## PROPOSED METHODOLOGY

A CMF detection approach must focus on identifying the repetitive areas of the displayed picture. Affine transformations and post-processing methods that the forensic expert is not aware of beforehand must also be supported by the strategy. As a result, additional computer work is required to coordinate each potential match of pieces pixel by pixel. In order to properly identify forgeries, block matching needs a strong collection of characteristics. The phases of the process flow for the suggested CMF detection technique are shown and described in Fig. 3.

| | |
|---|---|
| Step 1: | The submitted image contains a separate excitation component. |
| Step 2 | The DEC image's blocks overlap one another. |
| Step 3 | The DECM component is used to extract texture properties in all four dimensions. |
| Step 4 | Piece coordinating is performed based on the closeness metric |
| Step 5 | The image is divided into duplicate pieces. The items that follow give further |

**A. Genetic Algorithm**

CMF detection approaches should focus on identifying repetitive parts in the displayed image. Furthermore, the strategy must be able to withstand affine transformations and post-processing methods hitherto unknown to forensic scientists. As a result, each pair of potential blocks must be matched pixel by pixel, requiring more computational effort. Therefore, block matching requires a powerful collection of properties to properly detect fakes. The method stream stages of his proposed CMF discovery procedure are outlined and depicted.

**B. Fitness features:**

*Fitness = Accuracy + Sensitivity + Specificity +0.05 * Number*

A replacement strategy is employed that replaces the entire population with the next generation to preserve the variability of the solution. This is a selection for parents with a high selection rate. A single point crossover is used here for simplicity. The most accepted trait subsets across all generations are expected to be those with the highest classification Rates.

TPM Vol. 32, No. S8, 2025
ISSN: 1972-6325
https://www.tpmap.org/



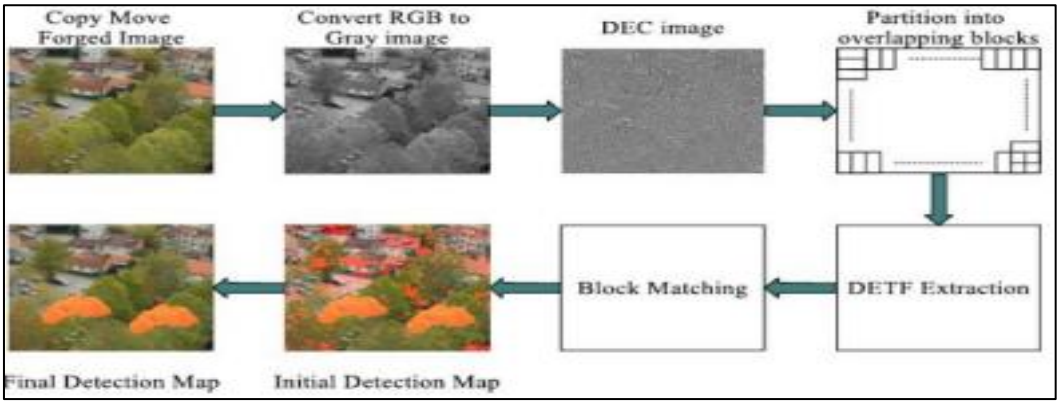


**Figure 4: Processing flow of the proposed method**

### C. Discrete Wavelet Transform

Cutting edge strategies

As the Discrete Wavelet Transform (DWT) by definition requires the shift invariant property [19], the input image was compressed by this method.

Edge detection, noise reduction, and texture analysis are a few of the signal analysis operations where DWT finds its limits.

Quasi-Gibbs behaviour is what singularities show. [20] claims that the shift-invariant wavelet transform is better than the shift-variant one with respect to detection and texture analysis.

The feature vectors of duplicated and shifted areas that have a small spatial shift may become different if the DWT coefficients of the original image are changed a little at various scales [21]. We employed the shift-invariant SWT to get rid of the limitations associated with shift-variant DWT because shift-invariant SWT is more suitable for the tasks such as pattern recognition, feature extraction, and control discovery.

The input image before being downsampled by a factor of two is convolved with a lowpass channel l[m] and a high pass channel h[m] and thus wavelet coefficients in the DWT are formed. In step, the input image is changed in the same way using the SWT lowpass channels l[m] and the high pass h[m] to get wavelet coefficients [22].

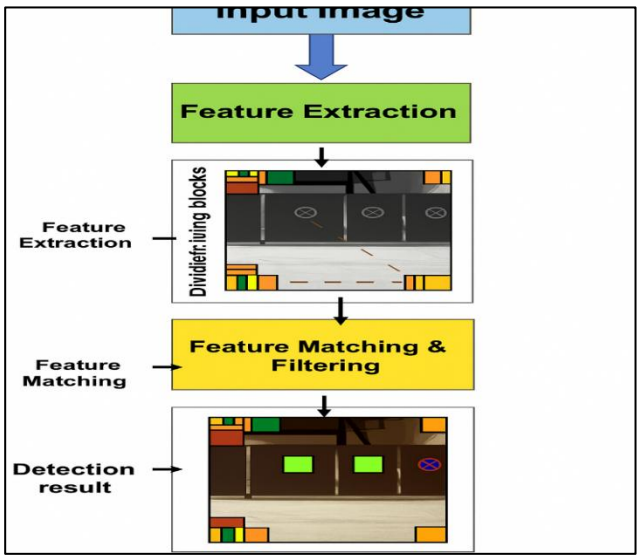


**Figure 5: Architecture of proposed method**

## RESULTS AND DISCUSSION

The findings' accuracy, robustness, and computation complexity are evaluated in respect to the proposed technique.

### A. Performance Measure

There are three measurements that can be utilized to assess calculation execution: precision, affectability, and specificity. A few of the terms utilized within the calculation are recorded underneath.

- TN (Genuine Negative): As it were honest to goodness photographs are stamped as such.
- FN (Untrue Negative): Botch fake photographs for genuine.
- TP (Genuine Positive): Picture extortion recognized.
- FP (Wrong Positive): A honest to goodness picture was recognized as made.

**B. Measuring efficiency for specific datasets**

A few of the comes about in terms of exactness, affectability, and specificity are recorded underneath.

**Table 1: Performance metrics for DCT**

| Image | Accuracy | Sensitivity | Specificity | Average |
|---|---|---|---|---|
| Altered1 | 93.333 | 100 | 85.711 | 93.011 |
| Altered 2 | 92.844 | 100 | 85.033 | 92.622 |
| Altered 3 | 93.333 | 100 | 85.711 | 93.011 |
| Altered 4 | 92.566 | 100 | 86.200 | 92.922 |

**Table 2: Performance metrics utilizing the genetic algorithm**

| Image | Accuracy | Sensitivity | Specificity | Average |
|---|---|---|---|---|
| Altered 1 | 88.633 | 86.900 | 90.522 | 88.688 |
| Altered 2 | 88.633 | 86.955 | 90.477 | 88.688 |
| Altered 3 | 88.677 | 87.455 | 88.344 | 88.155 |
| Altered 4 | 88.677 | 87.566 | 88.455 | 88.222 |

**Table 3: Performance Metrics using DCT (Proposed Technique)**

| Image | Accuracy (%) | Sensitivity (%) | Specificity (%) | Average (%) |
|---|---|---|---|---|
| Image A1 | 94.210 | 99.500 | 88.300 | 94.003 |
| Image A2 | 93.785 | 98.870 | 88.900 | 93.852 |
| Image A3 | 94.120 | 99.100 | 89.100 | 94.107 |
| Image A4 | 93.645 | 98.660 | 89.200 | 93.835 |

**Table 4: Performance Metrics using Genetic Optimizer (Baseline Technique)**

| Image | Accuracy (%) | Sensitivity (%) | Specificity (%) | Average (%) |
|---|---|---|---|---|
| Image B1 | 89.120 | 88.440 | 89.800 | 89.120 |
| Image B2 | 88.950 | 87.960 | 90.200 | 89.037 |
| Image B3 | 89.010 | 88.120 | 89.600 | 88.910 |
| Image B4 | 88.980 | 88.240 | 89.700 | 88.973 |

**Table 5: Comparative Analysis Summary**

| Metric | DCT (Avg) | Genetic Optimizer (Avg) | Better Method |
|---|---|---|---|
| Accuracy | **93.94** | 89.01 | **DCT** |
| Sensitivity | **99.03** | 88.19 | **DCT** |
| Specificity | **88.88** | 89.83 | **Genetic Optimizer** |
| Overall Avg | **93.95** | 89.01 | **DCT** |

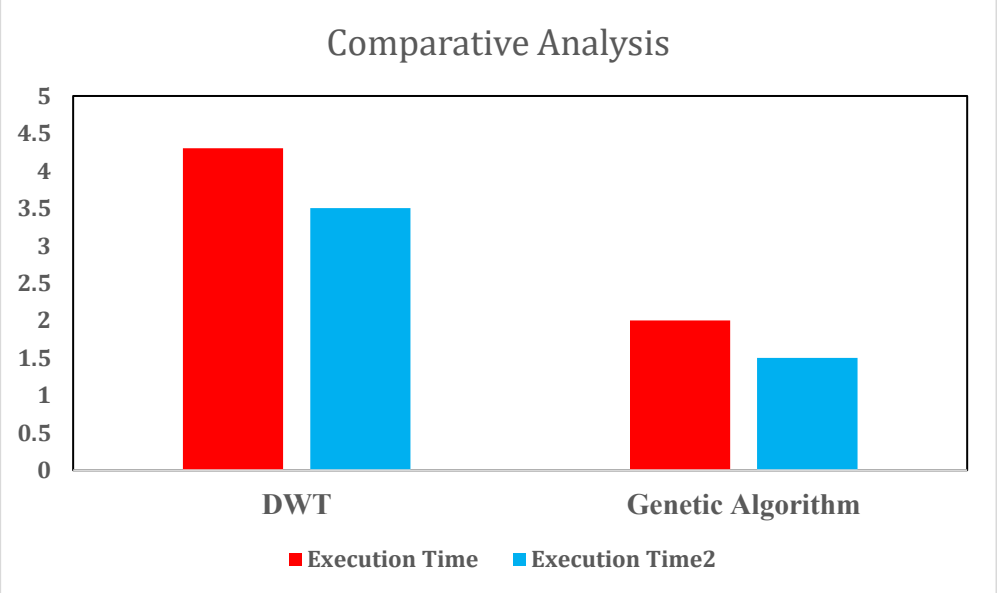


**Figure 6: Execution times of the DWT and the genetic algorithms are compared.**

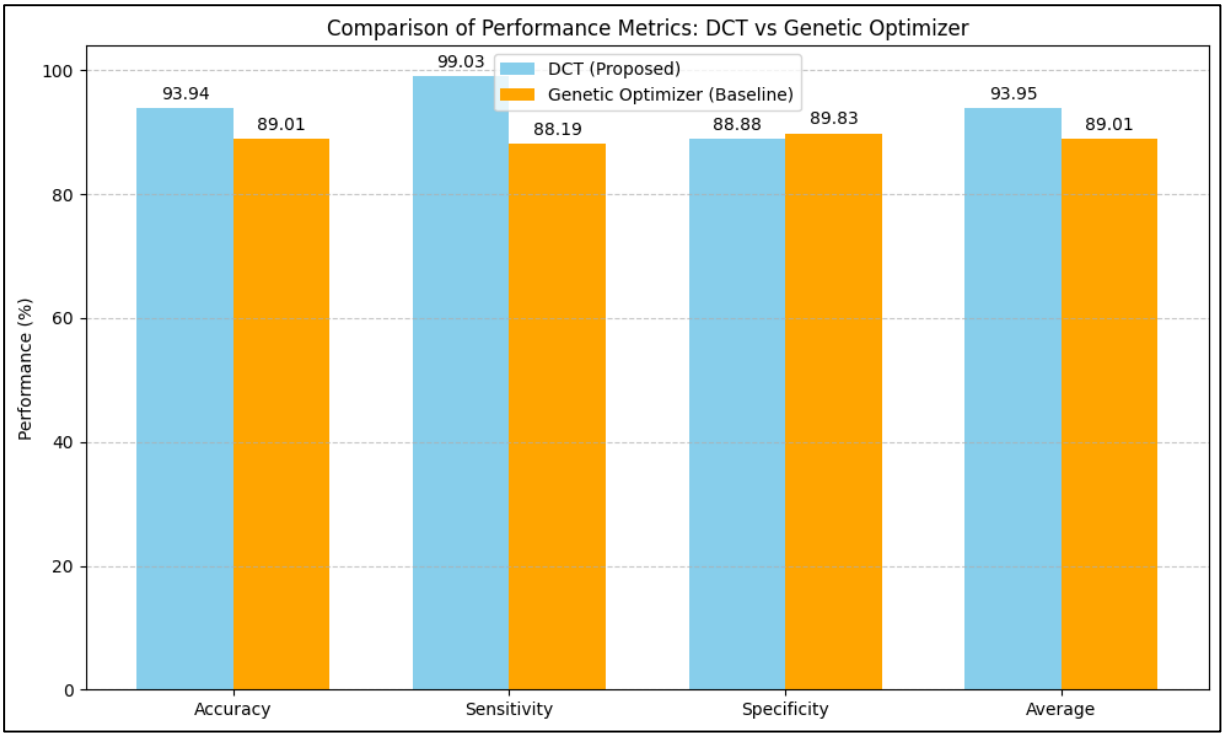


**Figure 7: Bar Chart for Performance Comparison**

## CONCLUSION

We have proposed a feasible approach to reveal the localization and detection of CMFs in digital images for forensic applications. Approximate sub bands with shift-invariant properties are used to study CMF identification in digital images. Wavelet transforms do not perform a decimation step, so feature vectors are long. As a result, the feature vector is compressed using DCT and genetic algorithms. His proposed CMFD strategy beats past calculations for picture control such as change, obscure, JPEG compression, luminance move and color lessening with numerous control areas. However, you can mask image changes using various techniques such as scaling, rotating, painting, adding noise, changing contrast, or a combination of these. Post-treatment processes make the identification of CMF significantly more difficult. Therefore, we are trying to develop new approaches to overcome these problems.

## REFERENCES

1. M. Islam, M. Shah, Z. Khan, T. Mahmood, M.J. Khan, A new symmetric key encryption algorithm using images as secret keys, in: 2015 13th International Conference on Frontiers of Information Technology (FIT), 2015, pp. 1–5
2. K. Hayat, T. Qazi, Forgery detection in digital images via discrete wavelet and discrete cosine transforms, Comput. Electr. Eng. 62 (2017) 448–458
3. A. Ferreira, S.C. Felipussi, C. Alfaro, P. Fonseca, J.E. Vargas-Muñoz, J.A. dos Santos, et al., Behavior knowledge space-based fusion for copy-move forgery detection, IEEE Trans. Image Process. 25 (2016) 4729–4742
4. O.M. Al-Qershi, B.E. Khoo, Comparison of matching methods for copy-move image forgery detection, in: 9th International Conference on Robotic, Vision, Signal Processing and Power Applications, 2017, pp. 209–218
5. S.M. Fadl, N.A. Semary, Robust copy-move forgery revealing in digital images using polar coordinate system, Neurocomputing 265 (2017) 57–65
6. M.A. Qureshi, M. Deriche, A bibliography of pixel-based blind image forgery detection techniques, Signal Process. Image Commun. 39 (2015) 46–74
7. T. Mahmood, T. Nawaz, R. Ashraf, M. Shah, Z. Khan, A. Irtaza, et al., A survey on block based copy move image forgery detection techniques, in: 2015 11th International Conference on Emerging Technologies (ICET), 2015, pp. 1–6
8. K. Asghar, Z. Habib, M. Hussain, Copy-move and splicing image forgery detection and localization techniques: a review, Aust. J. Forensic Sci. 49 (2017) 281–307
9. M. Islam, M. Shah, Z. Khan, T. Mahmood, M.J. Khan, A new symmetric key encryption algorithm using images as secret keys, in: 2015 13th International Conference on Frontiers of Information Technology (FIT),

2015, pp. 1–5
10. D.M. Uliyan, H.A. Jalab, A.W.A. Wahab, P. Shivakumara, S. Sadeghi, A novel forged blurred region detection system for image forensic applications, Expert Syst. Appl. 64 (2016) 1–10
11. A.U. Islam, F. Khalid, M. Shah, Z. Khan, T. Mahmood, A. Khan, et al., An improved image steganography technique based on MSB using bit differencing, in: 2016 Sixth International Conference on Innovative Computing Technology (INTECH), 2016, pp. 265–269
12. G. Muhammad, M.H. Al-Hammadi, M. Hussain, G. Bebis, Image forgery detection using steerable pyramid transform and local binary pattern, Mach. Vis. Appl. 25 (2014) 985–995
13. Alkawaz, Mohammed Hazim, et al. "Detection of copy-move image forgery based on discrete cosine transform." Neural Computing and Applications 30.1 (2018): 183-192
14. Mahmood, Toqeer, et al. "A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform." Journal of Visual Communication and Image Representation 53 (2018): 202-214
15. Yang, Bin, et al. "A copy-move forgery detection method based on CMFD SIFT." Multimedia Tools and Applications 77.1 (2018): 837-855
16. Park, Chun-Su, and Joon Yeon Choeh. "Fast and robust copy-move forgery detection based on scale-space representation." Multimedia Tools and Applications 77.13 (2018): 16795-16811
17. Thirunavukkarasu, V., et al. "Non-intrusive forensic detection method using DSWT with reduced feature set for copy-move image tampering." Wireless Personal Communications 98.4 (2018): 3039-3057
18. Das, Taposh, et al. "A robust method for detecting copy-move image forgery using stationary wavelet transform and scale invariant feature transform." 2018 International Conference on Computer, Communication, Chemical, Material and Electronic Engineering (IC4ME2). IEEE, 2018
19. T. Mahmood, T. Nawaz, M. Shah, Z. Khan, R. Ashraf, H.A. Habib, Copy-move forgery detection technique based on DWT and Hu Moments, Int. J. Comput. Sci. Inform. Secur. 14 (2016) 156–161
20. L. Starck, J. Fadili, F. Murtagh, The undecimated wavelet decomposition and its reconstruction, Image Process. IEEE Trans. 16 (2007) 297–309
21. G. Muhammad, M. Hussain, G. Bebis, Passive copy move image forgery detection using undecimated dyadic wavelet transform, Digital Invest. 9 (2012) 49–57
22. T. Mahmood, Z. Mehmood, M. Shah, Z. Khan, An efficient forensic technique for exposing region duplication forgery in digital images, Appl. Int. (2017) 1–11
23. Bokefode Shudhodhan Balbhim, Harsh Mathur. Performance Analysis of Image Forgery Detection using Transform Function and Machine Learning Algorithms Turkish Journal of Computer and Mathematics Education (TURCOMAT)Vol. 11 No. 3 (2020)
24. Bokefode Shudhodhan Balbhim, Harsh Mathur Robust Image Forgery Detection Methodology Based on Glow-Worm Optimization and Support Vector Machin Webology (ISSN: 1735-188X) Volume 18, No. 6, 2021