# Performance Analysis of Image Forgery Detection using Transform Function and Machine Learning Algorithms

**Bokefode Shudhodhan Balbhim[1], Harsh Mathur[2]**

Department of Computer Science & Engineering[1,2]
Madhyanchal Professional University, Bhopal, India[1,2]
shudhodhan358@gmail.com[1], harshmathur786@gmail.com[2]

**Abstract**

The image forgery process deformed the reputation of digital multimedia data in the era of internet technology. The availability of image editing software promotes the activity of image forgery. The action of forgery rise Ransome demands from the legitimate use of social media. The increasing rate of multimedia temptation changes the authenticity of data. Image forgery detection is a vital challenge for research scholars in the current decade. The forgery detection detects the location of forgery in the image and ensures the authentication of the picture. This paper represents the study of image forgery detection based on transform methods and machine learning. The transform methods have been great potential in image processing and pattern recognition. The various derivates of transform methods estimate the image forgery. The variants of transform include discrete wavelet transform, DCT, FFT, SIFT and many more transform. The applied transform methods have certain limitations and the detection of forged image compromised. The machine learning algorithm increases the detection ratio of image forgery. The trends of machine learning algorithms focus on image forgery detection and improve the detection ratio. Machine learning provides various classification and clustering algorithms for image forgery detection. This paper analyzed the experimental performance of image forgery detection based on transform and machine learning algorithms. The analysis process uses MATLAB tools and a standard image forgery dataset for the detection ratio. The analysis of results suggests that the machine learning algorithm is very efficient instead of transform-based methods.

**Keywords: -** Image Forgery, DWT, ML, Feature, MATLAB, Detection

## I. Introduction

Image forgery detection plays a vital role in digital image forensic analysis. The outcomes of forensics depend on the detection ratio and authenticity of the detection process. The increasing rate of digital multimedia data face a problem of forgery and loses the integrity of the content. Forgery is promoted with image editing software such as adobe, photoshop, and many image editing software [1,2]. The process of image forgery declines the authentication of images available on multiple internet sources. The most common image forgery is copy and move. The copy and move are an easy way to image forgery. The standard image forgery process is image slicing, enhancement, and formation based on pixel swapping [3,4,5,6]. The rate of occurrence of forgery has increased to the point where the process can be classified in a variety of ways; all of these cases are classified into three categories based on the process of creating fake images, namely, image retouching, image slicing, and copy-move attack [7, 8]. Image forgery is the process of altering an image in order to conceal some meaningful or valuable information. Copy-move and cut-paste forgery are two common image manipulations. As a result, the scheme's development should provide an adequate response to the related issue of forgery formation. As a result, the detection process accurately identifies the formation of the forgery over the image while also verifying and resolving the issue through consistent changes to the image within the same patch [9,10]. The contribution of transform-based methods in image forgery detection is very high. The transform-based methods apply in terms of coefficient and feature components. DCT based image forgery detection scan the forged images coefficient wise and detect the location of forgery. The contribution of DCT based forgery detection is significantly less due to the partition of blocks of images. Feature-based image forgery detection is a new area of research in the current domain of forensics analysis. The digital image content has three low-level features: color, texture, and shape size. The texture is a major dominated feature component of digital images. The transform-based function is reach dominated function of texture extraction. The discrete wavelet transform (DWT) subgroup of the mother wavelet transform. The DWT function decomposes the digital images into multiple layers, and the detection process is performed [11]. The other transform functions include integer wavelet transform (IWT), wavelet packet transform (WPT) and other applications of transform function such as CSP, curvelet, share let, and contourlet transform. The application of transform methods estimates an excellent detection ratio but the major limitation on significant scale detection of forgery [12]. Despite various studies of transform-based image forgery detection, they suggest applying a machine learning approach for forgery detection in the case of digital images. Machine learning provides various algorithms for the detection of image forgery detection. The classification and clustering algorithms are applied for the formation of image patterns; pattern-based detection enhances the results of image forgery detection. The machine learning algorithm support vector machine is applied to detect a common pattern in the forged image. The support vector machine faces the problem of feature selection of forged images. For the selection of features applies a swarm intelligence-based optimization algorithm. This paper applies a particle swarm optimization algorithm to select features in image forgery detection [14,15]. The remaining paper discusses, as in section II—the existing work of image forgery detection. Section III discuss machine learning and particle swarm optimization. Section IV discusses the experimental analysis of transform-based methods. Furthermore, finally, conclude in section V.

## II. Existing Work

The incremental approach of image forgery detection enhances the detection ratio of the forged area of the image. In addition, the transform-based methods and swarm intelligence-based algorithms contribute more. Machine learning algorithm also enhances the performance of image forgery detection. The contribution of the authors describes here.

In this [1] author proposed the DCT coefficient was used to detect copy-move image counterfeiting The RGB image is first converted to grayscale using a typical image conversion technique. As a outcome, the grayscale image is divided into m 9 m pixel overlaying blocks, with m = 4.8. Every block uses zig-zag scanning to calculate 2D DCT coefficients and positions them into a feature vector.

In this [2] author proposed a robust technique for CMF identification and localization in digital images. For exposing forgeries in digital images, the technique extracts stationary wavelet transform (SWT) based features. The outcome of the experiments show that the proposed technique outperforms existing strategies in terms of true and false detection rates.

In this [3] author proposed a revolutionary feature-based CMFD approach. A modified SIFT-based detector is used to detect key-points. For equally distributing key-points throughout a picture, a novel key-point distribution approach is devised. Finally, for the CMFD scenario, an updated SIFT descriptor is used to describe key-points. To prove the efficacy, extensive experimental outcome is presented.

In this [4] author Using invariant quaternion exponent moments, they developed a new block-based robust copy–move forgery detection method (QEMs). To begin, a Gaussian low-pass filter is applied to the original tempered color image, and the filtered color image is partitioned into overlapping circular blocks. Outcome show that the newly presented approach is effective in detecting copy–paste forgeries under a variety of difficult situations, including noise addition, lossy compression, scaling, and rotation.

In this [5] author proposed a fast and reliable method that can handle rotation, scaling, sheering, and reflection, among other geometric transformations The Scale Invariant Feature Transform is used in the CMFD design to extract key points and their descriptors from the image (SIFT). Outcome show that the discussed algorithm to state-of-the-art algorithms with established performance guarantees in their simulation.

In this [6] author compare the three approaches for copy-move forgery detection (CMFD) based on segmentation: Segmentation-Based Image CMFD, Adaptive Over segmentation and Feature Point Matching, and Multi-scale feature extraction and adaptive matching for CMFD. The outcomes show that each design performed admirably.

In this [7] author proposed a unique framework that uses a single left-hand radiograph to classify a person's gender and forecast their age. The accuracy of the Deep Convolutional Neural Network (DCNN) as a means of learning and predicting outcomes was 79.6% for gender classification and MAD 0.50 years and RMS 0.67 years for age classification.

In this [8] author proposed the grayscale image is then decomposed into four parts using a two-level Stationary Wavelet Transform (SWT), and the key-points are extracted from the approximation component of the decomposed image using the Scale Invariant Feature Transform (SIFT) algorithm. the discussed model has a 93 percent accuracy rate.

In this [10] author proposed the field of digital image forensics (DIF) has grown in importance as a means of checking the validity and integrity of digital information. This study gives a DIF literature review that includes active and passive methods as well as deep learning-based methods, and their work includes a large and up-to-date set of references synthesized in textual, tabular, and graphic form.

In this [11] author proposed the field of digital image forensics (DIF) has grown in importance as a means of ensuring the validity and integrity of digital information. This work gives a DIF literature review that includes active and passive methods, as well as deep learning-based methods, and their work includes a large and up-to-date set of references synthesized in textual, tabular, and graphic form.

In this [12] author proposed an efficient technique for detecting Copy Move Forgery in a digital picture The discussed approach uses the Scale Invariant Feature Transform (SIFT) and Fuzzy C-means (FCM) for clustering. The presented technique was tested utilizing both datasets, and on the MICC-220 data set, the average detection time was lowered by 14.67 percent compared to the existing standard SIFT-based algorithm.

In this [13] author proposed a method for detecting region duplication forgeries in digital photos that is quick and easy to use. The suggested technique divides the shift invariant stationary wavelet transform's approximation (LL) sub band into overlapping blocks of w*w sizes. Outcome compared to state-of-the-art techniques, revealing the prominence and efficacy of the discussed technique in terms of precision, recall, and F1 score for various block sizes.

In this [14] author proposed a copy-move forgery detection system based on multi-scale feature extraction and adaptive matching. The host image is first segmented into non-overlapping irregular shape patches in various scales. Then, to generate multi-scale features, the Scale Invariant Feature Transform is used to extract feature points from all patches.

In this [15] author proposed CMFD-Zernike is a fast and reliable technique for detecting copy-rotate-move fraud that uses wavelet decomposition and Zernike moments to locate duplicated regions. The outcome of the experiments show that the proposed technique is effective in detecting the faked region in copy-rotate-move forgery.

In this [16] author proposed highlighted how they divided a picture into texture and smooth parts to deal with them independently in order to overcome the problem of high computational complexity in block-based algorithms for copy-move forgery detection. Experimental outcome reveal that the presented method outperforms others and is resistant to JPEG compression, rotation, and scaling.

In this [17] author proposed Predefined Convolutional Filters Network (PCFNET) is a new framework that replaces the kernel in standard CNN's first layer convolution with certain learnable predefined filters. Outcome show that PCFNET has fewer learnable parameters in the first layer convolution, requiring less training data, and this effectiveness has been proven by CIFAR10/100 experimental.

In this [18] author proposed a new approach for detecting copy-move forgeries in replicated objects to create a sub-image, a bounding rectangle is formed around the detected object. For locating related objects, the Euclidian distance and correlation coefficient between feature vectors are calculated and employed.

In this [19] author use the Fourier Melling transform with log-polar mapping, as well as a color-based segmentation technique based on K-means clustering, to achieve invariance to all of the above types of assaults in digital image copy–move forgery detection. Their findings demonstrate the efficacy of the proposed strategy as well as its superiority over the present state of the art.

In this [20] author offers a copy-move forgery detection (CMFD) method based on circular blocks and discrete cosine transform (DCT) that uses fewer feature vectors than existing methods. The outcome shows fewer feature vectors, the computational complexity of the proposed method is lower than that of previous techniques.

In this [21] author Using the deep belief network (DBN) model, a novel approach of speech segregation for unlabeled stationary noisy audio signals has been developed. The approach described here effectively separates a music signal from noisy audio streams. The discussed method is put to the test on three datasets (TIMIT, MIR-1K, and Music Brains), and the outcome show that it is reliable for speech separation.

In this [22] author proposed a unique QCNN that always treats color triples as a whole to avoid information loss. To thoroughly mix the information of color channels, the original quaternion convolution process is described and developed. Outcome show that the proposed model is more efficient than a standard convolutional neural network and another QCNN with the same structure in color picture categorization and forensics.

In this [23] author proposed a method for detecting copy-move forgeries based on block processing and feature extraction from block transformations A Convolutional Neural Network (CNN) is also used to detect forgeries. The feature extraction is done with serial pairs of convolution and pooling layers, and then classification is done with and without transforms between the original and tampered images.

In this [24] author proposed a multimodal solution that takes care of both steps: forgery detection using deep neural networks (CNN) and part-based image retrieval. A deep neural network is used to accomplish classification and localization of the modified region. To extract essential characteristics from the complete image as well as the modified region, InceptionV3 is used.

In this [25] author locate forged pixels; semantic segmentation is used to train these classed images using color pixel labels. GRIP, DVMM, CMFD, and BSDS300 datasets are used to test these techniques. The outcome show total accuracy was 0.98482, the average accuracy was 0.98581, the average IOU was 0.91148, the weighted IOU was 0.97193, and the average border F1 score was 0.86404.

In this [26] author proposed a multi-domain learning convolutional neural network (MDL-CNN) is described. They use the original and changed images to obtain the periodicity attribute. During the training phase, features of changed images taken from various datasets are fed into the neural network. The MDL-CNN method can greatly increase forensic performance, according to experimental outcome.

In this [27] author proposed embed the watermark, the host picture (shared/forwarded) is broken into equal-sized blocks, then each block is given a slant let transform. Three copies of the source information (user and app) are inserted during watermark embedding to ensure high dependability.

In this [28] author proposed a new IoT-enabled Optimal Deep Learning based Convolutional Neural Network (ODL-CNN) to aid in suspect identification. The IEHO technique was used to optimize the hyper parameters of the DL-CNN model. The ODL-CNN model outperformed the competition with a maximum average Peak Signal to Noise Ratio (PSNR) of 20.11dB, Average Structural Similarity (SSIM) of 0.64, and average accuracy of 90.10 percent, according to a rigorous simulation analysis.

In this [29] author proposed a novel deep learning-based architecture for more reliable and accurate periocular recognition that includes an attention model to highlight relevant regions in the periocular pictures Within a periocular image, the new architecture uses a multi-glance mechanism, in which portion of the intermediate components are configured to include focus on essential semantical regions, such as the eyebrow and eye.

In this [30] author proposed a convolutional neural network that is distinct from previous work in which researchers attempted to comprehend extracted features from each convolutional layer and detect various sorts of picture tampering using automatic feature learning. As the training data, they used CASIA v1.0, a public picture set containing authentic and splicing photographs, as well as its more reformed versions containing retouching and re-compressing images.

**III. Machine Learning and PSO**

This section describes the transform methods of image forgery detection, machine learning algorithm and particle swarm optimization.

Transform methods.

Transform methods have been great potential to image feature extraction as texture. For the detection of the image, forgery applied four transform methods, DCT, DWT, SIFT and WPT[21,22,23].

DCT

The discrete cosine transform covert the forged image into multiple coefficient such as 8 X 8, 16 X 16 blocks as the input processing of images. The formulation of DCT as

$$X_k = \frac{1}{2}(x_0 + (-1)^k x_{N-1}) + \sum_{n=1}^{N-2} x_n \cos\left[\frac{\pi}{N-1} nk\right] \qquad k = 0, \ldots, N-1.$$

The factor $x_0$ and $x_{N-1}$ terms by √2, and correspondingly multiply the $X_0$ and $X_{N-1}$ terms by 1/√2. This makes the DCT matrix, if one further multiplies by an overall scale factor of $\sqrt{2/(N-1)}$.

DWT

The wavelet transform is derived from mother wavelet transform for the scaling of transform for the signal data decomposition. In process of wavelet transform get a finer low frequency resolution. Wavelet transform applied long time windows, in order to get high frequency data. the processing of wavelet transform is superior than FFT and STFT for non-linear transient EEG signals.

Conder $f(x) \in L^2(R)$ relative to wavelet function $\psi(x) and\ scaling\ function\ \phi(x)$

The DWT defined as

$$W_\phi(j0,k) = \frac{1}{\sqrt{M}} \sum_x f(x)\phi_{j0,k}(x) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots. (1)$$

$$W_\psi(J,K) = \frac{2}{\sqrt{M}} \sum\nolimits_X f(x)\psi_{j,k}(x) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Now

$$f(x) = \frac{1}{M}\sum\nolimits_K W_\phi(j0,k)\phi_{j0,k}(x) + \frac{1}{\sqrt{M}}\sum_{J=J0}^{J-1}\sum\nolimits_K W_{\psi(J,K)}\psi_{J,K}(X) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots. (3)$$

In the value of M measure, the power of 2. The component of transform estimate M number of coefficients the maximum scale j-1 and minimum coefficient is 0, and detail coefficient define in equation 2.

SIFT

The SIFT algorithm was uses to extraction of multimedia information features. The SIFT algorithm was developed by Lowe. SIFT transform function finds the local -invariant features points. The multi-point feature points combined and generates features matrix[4].

Step 1 - Scale-Space Selection:

The scale-space approach is to define a scale parameter into the 2D image data processing model and get 2D image processing data at different scales by regular updating scale parameters. Then, the data is integrated to expand the required properties of 2D-image. The Gaussian convolution kernel is one of the linear kernels to summarize the scale transformation, and the scale-space kernel $f_{out}$ can be expressed mathematically as:

$$f_{out} = K_n * f_{in}$$

Where,
$K_n$ – kernel
$f_{in}$ - input signal
$*$ - convolution operation
Scale-space $S(x, y, \sigma)$ of image $I(x, y)$ is expressed mathematically as:

$$S(x, y, \sigma) = G(x, y, \sigma) * I(x, y)$$

$$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}}$$

Where,
$G(x, y, \sigma)$ - scale variable Gaussian function
$(x, y)$- spatial coordinates
$\sigma$ - scale-space factor (using image's smoothness)
A large value of $\sigma$ denotes a smooth image with feature's outline, while a small value of $\sigma$ introduce an abundant image with feature's described.

To detect the stable points considerable in the $scale - space$, Lowe discussed the DOG ($difference\ of\ Gaussian$) scale-space, defined mathematically as:

$$D(x, y, \sigma) = [G(x, y, k\sigma) - G(x, y, \sigma)] * I(x, y) = S(x, y, k\sigma) - S(x, y, \sigma)$$

Where,

$I(x, y)$ - input image

$k$ - multiple of 2 neighboring scale-spaces

$*$ - convolution operation.

To get the local maxima and minima of $D(x, y, \sigma)$, each point is compared with its $8 - neighbours$ in the used picture and $9 - neighbours$ in the scale below and above. Utilising the DOG scale-space image can be detected as feature points of all extreme points.

Step 2 - feature points:

The goal at orientating the location of feature points precisely. A huge number of extreme points are got in this manner. But not all extreme points are feature points. Afterword's, a desired method is required to calculate some points.

Step 3 - feature point orientation assignment:

The goal is to summarize the SIFT features of rotation invariance. For scaling the smoothed image $I_L$, the central derivative of $I_L$ at each feature point can be considered. The scale and orientation at feature point $(x, y)$ can be considered by:

$$\begin{cases} \theta(x, y) = \tan^{-1} 2\, \{[I_L(x, y+1) - I_L(x, y-1)]/[I_L(x+1, y) - I_L(x-1, y)]\} \\ g(x, y) = \sqrt{[I_L(x+1, y) - I_L(x-1, y)]^2 + [I_L(x, y+1) - I_L(x, y-1)]^2} \end{cases}$$

Where,

$\theta(x, y)$ - orientation of the gradient

$g(x, y)$ -magnitude

With the use of gradient direction histogram graph, getting the gradient amplitude and direction, that direction of feature points can be determined. The highest peak visualizes the direction. In the gradient direction histogram, when another peak value equals 80% of the main peak's value, this direction should be set as the auxiliary direction of this feature point. The direction matching has been finished with the parameter, position, situation and recent step is to find the local picture descriptor of the feature points.

This completes all steps of the SIFT algorithm.

WPT

Wavelet packet transform function is useful transform function for lossless data encoding in image forgery detection. The value of transform H (Z) is always whole number and the part of image is lossless. For lossless coding it is necessary to make an invertible mapping from an integer image input to an integer wavelet representation. The lifting scheme is used to construct symmetric bi-orthogonal wavelet transforms starting from interpolating Deslauriers–Dubuc scaling functions. A family of (N, N) symmetric bi-orthogonal wavelets is derived, where N is the number of vanishing moments of the analysis high-pass filter and N is the number of vanishing moments of the synthesis high-pass filter. An instance of this family of transforms is the (4, 2) interpolating transform. The integer version of it, given in [7], is implemented in the first stage of our coding algorithm. In this case, the integer wavelet representation of a one dimensional signal $A^0(n)$ having N nonzero samples is given by

$$\forall n: D^{i+1}(n) = A^i\,(2n+1) - \left[\sum\nolimits_k pkA^i\big(2(n-k)\big) + \frac{1}{2}\right]$$

$$0 \le i < j, 0 \le n < 2^{-(i+1)}N$$

$$-2 \le k \le 1$$

$$\forall n: A^i(2n) = A^i\,(2n) + \left[\sum\nolimits_k ukAD^{i+1}(n-k) + \frac{1}{2}\right]$$

$$0 \le i < j, 0 \le n < 2^{-(i+1)}N$$

$$0 \le k \le 1$$

where[x] represents the integer part of x,j is the number of scales,$A^{i+1}(n)$ and $D^{i+1}(n)$ denote, respectively, the Approximation and the detail of the original signal calculated at the scales (i+1), 0≤ I <j. The integer part of transform function gives the better encoding

Machine Learning

Machine learning algorithms enhance the detection ratio of image forgery detection. The machine learning based algorithms such as support vector machine, decision tree, ensemble-based classifier and many more hybrid algorithm. This paper focus on support vector machine and feature selection based on particle swarm optimization.

SVM (Support vector machine) is machine learning algorithm derived by Vipin in 1990. The support vector machine applied in various filed of image classification and pattern recognition. The nature of support vector machine is linear, non-linear and sigmoid. The non-linear support vector machine mapping the feature data with respect to one plane to another plan. The separation of data plan is non-linear and decision factor correlate with margin function of support vector[31]. The hyperplane of equation is derived as

$$WD.xi + b \ge 1 \; if \; yi = 1$$

(4)

$$WD.xi + b \le \; -1 \; if \; yi = -1$$

Here W is weight vector, x is input vector yi label o class and b is bias.

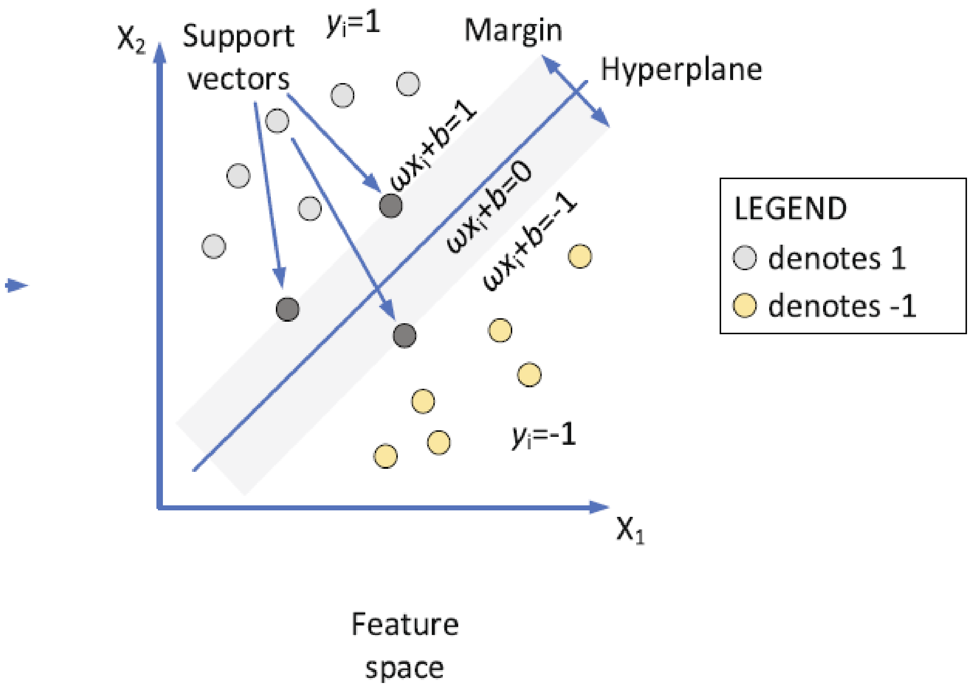


**Figure 1 process block diagram of support vector machine.**

The minimization formulation of support vector

$$Minimize\ \frac{1}{2}||w||2 + C\sum_{i=1}^{n} \varepsilon i\ , i = 1,2, \dots \dots, n$$

$$subject\ to\ y_i(w^T D.x1 + b) \geq 1 - \varepsilon 1$$

$$\varepsilon_i \geq 0\ i = 1,2, \dots \dots, n \dots \dots \dots \dots \dots \dots \dots \dots .(5)$$

Here C is constant, n is number of observation and $\varepsilon 1$ is slack variable.

The rule of decision function is

$$f(x) = \sum_{i=1}^{n} yi\alpha iK(xi, xj) + b \dots \dots \dots \dots \dots \dots .(6)$$

Feature optimization

The process of feature optimization applies particle swarm optimization. The particle swarm optimization inspired by the bird's fork stimulation. The process of particle swarm optimization reduces the unwanted features of forged image during the process of detection. The processing of PSO algorithm describe as

The processing of particle swarm optimization is based on acceleration function, constant factor, initial velocity, final velocity, and particle position. The processing of the algorithm describes here.

let the search space S- space and the position of particle is ith can be represented by S-space vector

xi=(xi1,xi2,xis,………………..,XiS). The velocity of vector represented as search space S as Vi=(Vi1,Vi2,……..Vis), now the position of particle after changes the position vector is Pi=(pi1,pi2,………,pis). The formation of new position of particle is

vis=Vis+C1a1(Pis-xis)+c2a2(Pgs-xis)…………………………..(7)

xis=xis+Vis s=1,……………s,………….S………………..(8)

where C1, C2 is constant and a1,a2 is acceleration coefficient towards global and local random number between[0,1].

Let the optimization coefficient K=c1+c2 and define as

$$k = \begin{cases} \dfrac{2x}{L(p) - 2 + \sqrt{x^2 - 4x}} & for\ X > 4 \dots \dots \dots \dots \dots \dots .(9) \\ & x, otherwsie \end{cases}$$

Where K is coefficient of optimization updated the position of particle as

Vis=K(vis+c1a1(Pis-xis)+c2a2(Pgs-xis))…………………….(10)

IV Experimental Analysis

Analysed the performance of existing algorithms of image forgery detection use MATLAB2012a software and reputed image forgery dataset forms this link http://www.vcl.fer.hr/comofod/download.html. The download image dataset are all size images such as 512 X 512 and 256 X256. The evaluation of results estimated in terms of PSNR in DB or FRR (false rejection ratio)[11,14,25].

Table: 1 shows that the PSNR and FRR with using DCT, DWT, SIFT and WPT techniques for the same and different images.

| Image | Method | PSNR In Db | FRR In % |
|---|---|---|---|
| Orange | DCT | 44.68 | 3.45 |
| | DWT | 46.52 | 2.76 |
| | SIFT | 49.75 | 3.89 |
| | WPT | 52.86 | 1.85 |
| BAT | DCT | 72.34 | 2.35 |
| | DWT | 75.52 | 3.45 |
| | SIFT | 78.15 | 2.68 |
| | WPT | 85.45 | 1.16 |
| CHAIR | DCT | 45.52 | 4.96 |
| | DWT | 49.67 | 3.85 |
| | SIFT | 53.85 | 3.61 |
| | WPT | 59.65 | 2.34 |
| HORSE | DCT | 31.54 | 3.56 |
| | DWT | 39.15 | 2.33 |
| | SIFT | 40.87 | 2.19 |
| | WPT | 45.69 | 1.45 |

Table:2 shows that the PSNR and FRR with using DWT-PSO, SIFT-PSO and WPT-PSO techniques for the same and different images.

| Image | Method | PSNR In Db | FRR In % |
|---|---|---|---|
| SHIP | DWT-PSO | 38.64 | 3.75 |
| | SIFT-PSO | 42.65 | 2.26 |
| | WPT-PSO | 46.89 | 1.75 |
| FUNGI | DWT-PSO | 70.93 | 3.48 |
| | SIFT-PSO | 72.15 | 2.95 |
| | WPT-PSO | 74.33 | 1.65 |
| AIRCRAFT | DWT-PSO | 39.46 | 4.01 |
| | SIFT-PSO | 42.73 | 3.95 |
| | WPT-PSO | 44.25 | 2.73 |
| HEN | DWT-PSO | 38.65 | 4.56 |
| | SIFT-PSO | 44.19 | 3.57 |
| | WPT-PSO | 49.56 | 2.34 |

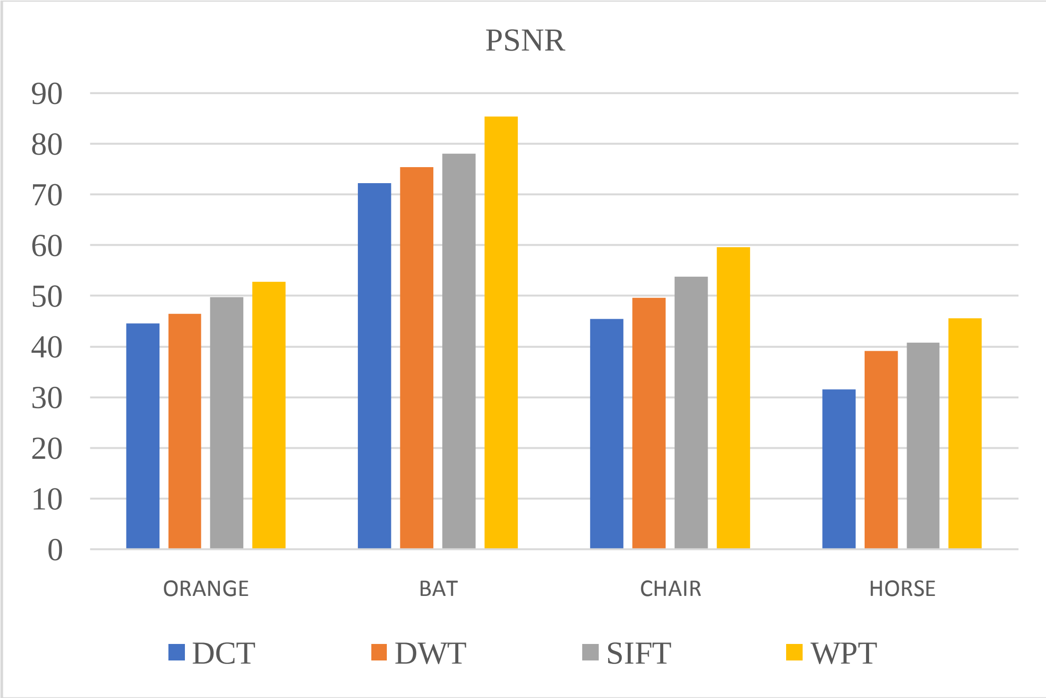


**Fig:2 Shows that comparative result of Image "Orange, Bat, Chair, Horse" with using DCT, DWT, SIFT, and WPT method and here our proposed algorithm shows that the better result in the form of higher PSNR than the existing method.**

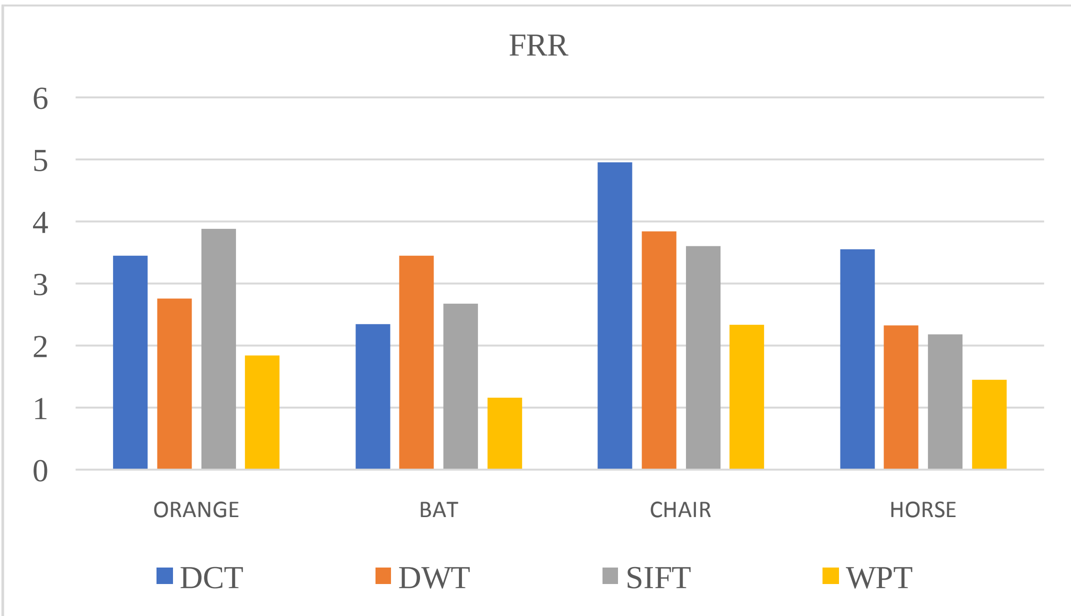


**Fig3: Shows that comparative result of Image "Orange, Bat, Chair, Horse" with using DCT, DWT, SIFT, and WPT method and here our proposed algorithm shows that the better result in the form of low FRR than the existing method.**

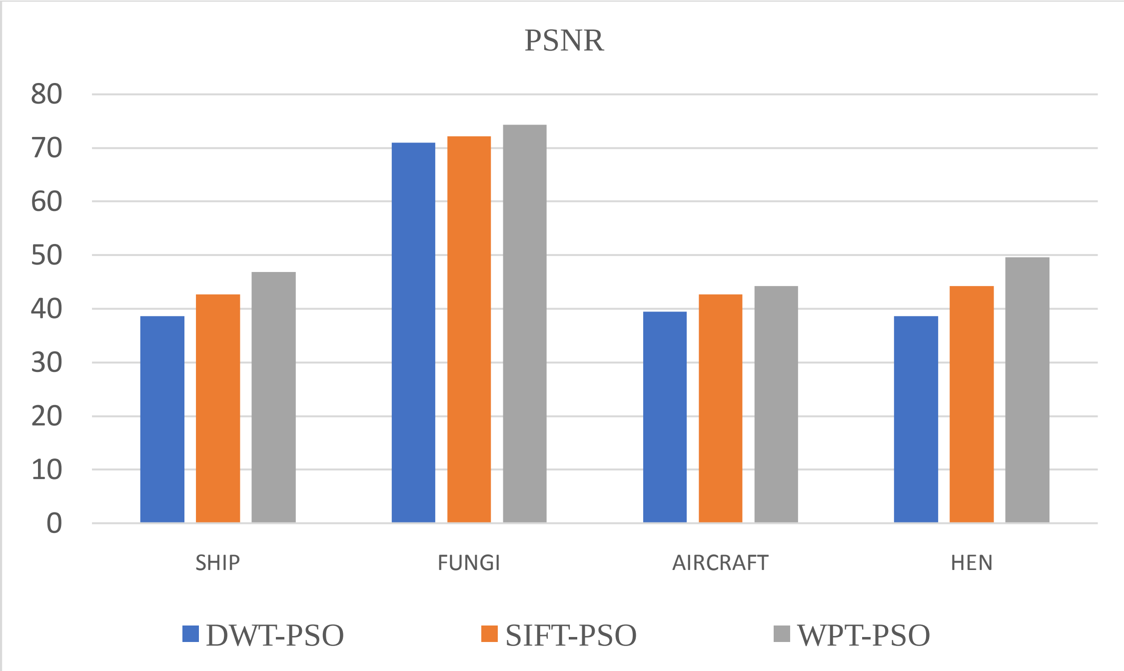


**Fig: 4 Shows that comparative result of Image "Ship, Fungi, Aircraft, Hen" with using DWT-PSO, SIFT-PSO, and WPT-PSO method and here our proposed algorithm shows that the better result in the form of higher PSNR than the existing method.**

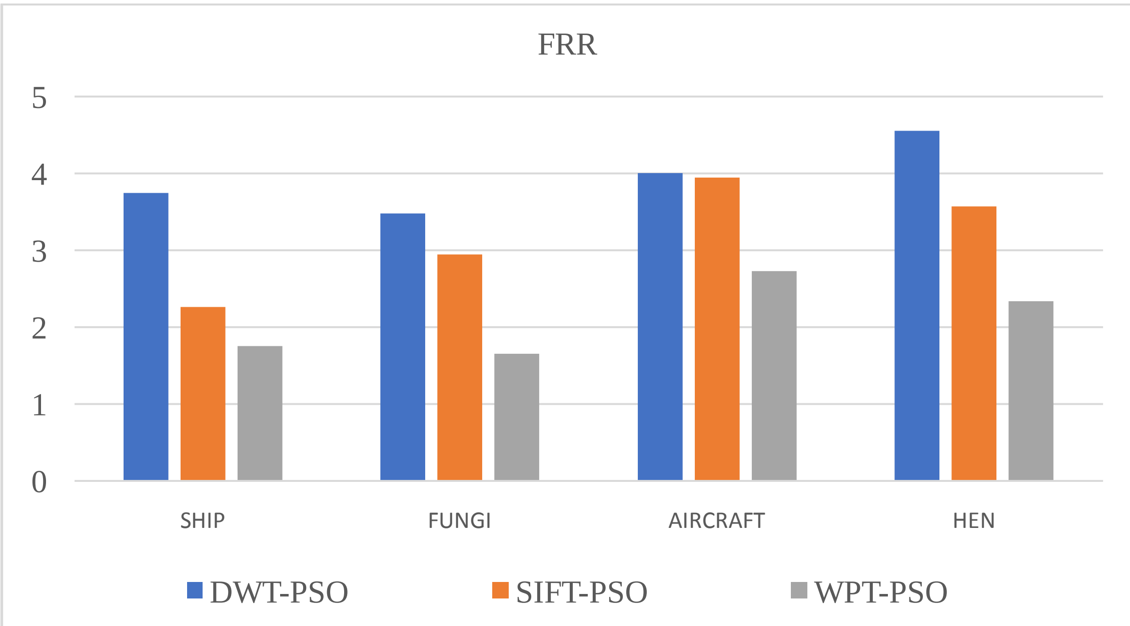


**Figure 5 Shows that comparative result of Image "Ship, Fungi, Aircraft, Hen" with using DWT-PSO, SIFT-PSO, and WPT-PSO method and here our proposed algorithm shows that the better result in the form of low FRR than the existing method.**

## V. Conclusion & Future Work

The role of image forgery detection is very high in digital image forensic. The study of different algorithms of image forgery detection based on transform function and machine learning enhance the performance of image forgery detection. The different types of transforms such as DCT, DWT, WPT and SIFT have different PSNR and false rejection ratios. The value of PSNR shows the level of deformation of the original image instead of the source image. Machine learning algorithms and particle swarm optimization also improve the detection ratio. The minimum value of FRR based on the optimization algorithm enhances forged image quality detection. DWT does not incorporate down sampling, so the image size is intact. The low-frequency component contains most of the information on which SIFT is applied to extract the features, and then matching is obtained between the feature descriptors to conclude that a given image is forged or not. The optimization algorithm has a higher matching rate, and it is robust to most of the attack and pre-processing techniques. Also, we have better performance parameter values on which we can conclude that it is feasible.

**References**


1. Alkawaz, Mohammed Hazim, Ghazali Sulong, Tanzila Saba, and Amjad Rehman. "Detection of copy-move image forgery based on discrete cosine transform." Neural Computing and Applications 30, no. 1 (2018): 183-192.
2. Nagpal, Shruti, Maneet Singh, Richa Singh, and Mayank Vatsa. "Discriminative shared transform learning for sketch to image matching." Pattern Recognition 114 (2021): 107815.
3. Jindal, Neeru, and Kulbir Singh. "Digital Image Forensics-Gateway to Authenticity: Crafted with Observations, Trends and Forecasts." In Handbook of Multimedia Information Security: Techniques and Applications, pp. 681-701. Springer, Cham, 2019.
4. Zhang, Xiaoqing, Hongling Zhao, Shuo Zhang, and Runzhi Li. "A novel deep neural network model for multi-label chronic disease prediction." Frontiers in genetics 10 (2019): 351.
5. Wang, Shui-Hua, Chaosheng Tang, Junding Sun, Jingyuan Yang, Chenxi Huang, Preetha Phillips, and Yu-Dong Zhang. "Multiple sclerosis identification by 14-layer convolutional neural network with batch normalization, dropout, and stochastic pooling." Frontiers in neuroscience 12 (2018): 818.
6. Ye, Jingyu, Yuxi Shi, Guanshuo Xu, and Yun-Qing Shi. "A convolutional neural network-based seam carving detection scheme for uncompressed digital images." In International Workshop on Digital Watermarking, pp. 3-13. Springer, Cham, 2018.
7. Gupta, Surbhi, Neeraj Mohan, and Priyanka Kaushal. "Passive image forensics using universal techniques: a review." Artificial Intelligence Review (2021): 1-51.
8. Marouf, Muhammad, Raheel Siddiqi, Fatima Bashir, and Bilal Vohra. "Automated Hand X-Ray Based Gender Classification and Bone Age Assessment Using Convolutional Neural Network." In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), pp. 1-5. IEEE, 2020.
9. Abidin, ArfaBintiZainal, Hairudin Bin Abdul Majid, Azurah Binti A. Samah, and HaslinaBintiHashim. "Copy-move image forgery detection using deep learning methods: a review." In 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS), pp. 1-6. IEEE, 2019.
10. Wang, Xiang-yang, Yu-nan Liu, Huan Xu, Pei Wang, and Hong-ying Yang. "Robust copy–move forgery detection using quaternion exponent moments." Pattern Analysis and Applications 21, no. 2 (2018): 451-467.
11. Ferreira, William D., Cristiane BR Ferreira, Gelson da Cruz Júnior, and Fabrizzio Soares. "A review of digital image forensics." Computers & Electrical Engineering 85 (2020): 106685.
12. Lin, Xiang, Jian-Hua Li, Shi-Lin Wang, Feng Cheng, and Xiao-Sa Huang. "Recent advances in passive digital image security forensics: A brief review." Engineering 4, no. 1 (2018): 29-39.
13. Zhou, Yuanyuan, Ji Zhang, Jiao Huang, Kaifei Deng, Jianhua Zhang, Zhiqiang Qin, Zhenyuan Wang et al. "Digital whole-slide image analysis for automated diatom test in forensic cases of drowning using a convolutional neural network algorithm." Forensic science international 302 (2019): 109922.
14. Chen, Xu, Jianjun Li, Yanchao Zhang, Yu Lu, and Shaoyu Liu. "Automatic feature extraction in X-ray image based on deep learning approach for determination of bone age." Future Generation Computer Systems 110 (2020): 795-801.
15. Abiodun, Oludare Isaac, Aman Jantan, Abiodun Esther Omolara, Kemi Victoria Dada, NachaatAbdElatif Mohamed, and Humaira Arshad. "State-of-the-art in artificial neural network applications: A survey." Heliyon 4, no. 11 (2018): e00938.
16. Xiao, Bin, Yang Wei, Xiuli Bi, Weisheng Li, and Jianfeng Ma. "Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering." Information Sciences 511 (2020): 172-191.
17. Saravanakumar, R., N. Krishnaraj, S. Venkatraman, B. Sivakumar, S. Prasanna, and K. Shankar. "Hierarchical symbolic analysis and particle swarm optimization-based fault diagnosis model for rotating machineries with deep neural networks." Measurement 171 (2021): 108771.
18. Ma, Yangling, YixinLuo, and Zhouwang Yang. "PCFNet: Deep neural network with predefined convolutional filters." Neurocomputing 382 (2020): 32-39.
19. Ross, Arun, Sudipta Banerjee, and Anurag Chowdhury. "Security in smart cities: A brief review of digital forensic schemes for biometric data." Pattern Recognition Letters 138 (2020): 346-354.
20. Zhang, Jun, Yixin Liao, Xinshan Zhu, Hongquan Wang, and Jie Ding. "A deep learning approach in the discrete cosine transform domain to median filtering forensics." IEEE Signal Processing Letters 27 (2020): 276-280.
21. Qazi, Khurram Ashfaq, Tabassam Nawaz, Zahid Mehmood, Muhammad Rashid, and Hafiz Adnan Habib. "A hybrid technique for speech segregation and classification using a sophisticated deep neural network." PloS one 13, no. 3 (2018): e0194151.]
22. Yin, Qilin, Jinwei Wang, XiangyangLuo, JiangtaoZhai, Sunil Kr Jha, and Yun-Qing Shi. "Quaternion convolutional neural network for color image classification and forensics." IEEE Access 7 (2019): 20293-20301.

23. Al_Azrak, Faten Maher, Ahmed Sedik, Moawad I. Dessowky, Ghada M. El Banby, Ashraf AM Khalaf, Ahmed S. Elkorany, and Fathi E. Abd El-Samie. "An efficient method for image forgery detection based on trigonometric transforms and deep learning." Multimedia Tools and Applications 79, no. 25 (2020): 18221-18243.
24. Jabeen, Saira, Usman Ghani Khan, Razi Iqbal, Mithun Mukherjee, and Jaime Lloret. "A deep multimodal system for provenance filtering with universal forgery detection and localization." Multimedia Tools and Applications 80, no. 11 (2021): 17025-17044.
25. Jindal, Neeru. "Copy move and splicing forgery detection using deep convolution neural network, and semantic segmentation." Multimedia Tools and Applications 80, no. 3 (2021): 3571-3599.
26. Yang, Bin, Zhenyu Li, and Tao Zhang. "A real-time image forensics scheme based on multi-domain learning." Journal of Real-Time Image Processing 17, no. 1 (2020): 29-40.
27. Sinhal, Rishi, Irshad Ahmad Ansari, and Deepak Kumar Jain. "Real-time watermark reconstruction for the identification of source information based on deep neural network." Journal of Real-Time Image Processing 17, no. 6 (2020): 2077-2095.
28. Elhoseny, Mohamed, Mahmoud Mohamed Selim, and K. Shankar. "Optimal deep learning-based convolution neural network for digital forensics face sketch synthesis in internet of things (IoT)." International Journal of Machine Learning and Cybernetics (2020): 1-12.
29. Zhao, Zijing, and Ajay Kumar. "Improving periocular recognition by explicit attention to critical regions in deep neural network." IEEE Transactions on Information Forensics and Security 13, no. 12 (2018): 2937-2952.
30. Huang, Na, Jingsha He, and Nafei Zhu. "A novel method for detecting image forgery based on convolutional neural network." In 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), pp. 1702-1705. IEEE, 2018.
31. Karampidis, Konstantinos, ErginaKavallieratou, and GiorgosPapadourakis. "A review of image steganalysis techniques for digital forensics." Journal of information security and applications 40 (2018): 217-235.