Received: June 19, 2023. Revised: August 6, 2023.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Image Copy-move Forgery Detection and Classification Using Golden Jackal Optimization Based Multi-Support Vector Machine

MR Archana[1] **Dayanand Jamkhandikar**[2] **Deepak N. Biradar**[1]*

[1]*Department of Computer Science, Gitam University, Rudraram, Hyderabad, India*
[2]*Department of Computer Science, Guru Nanak Dev Engineering College, Bidar, India*
* Corresponding author's Email: dbiradar@gitam.edu

Abstract: Protecting the data against forgery is an important concept and digital images are necessary for exhibiting information. Digital image forgeries are attaching extraordinary patterns to original images and it causes visual heterogeneousness. Image copy-move forgery is a challenging technique, that involves copying part of an image and then pasting the copied part into the same image. In this paper, the golden jackal optimization (GJO) is proposed for feature selection and multi-support vector machine (M-SVM) is proposed for effective classification. The GJO optimizes the feature selection process by iteratively searching for the most informative subset of features. By leveraging the exploration and exploitation of GJO, the algorithm efficiently explores the feature space, selecting relevant features that contribute to accurate forgery classification. This enhance the performance of MSVM by focusing on the most discriminative features. For this work, a dataset named as MICC-F2000 is examined which is managed by 2000 images in this 1300 are original and 700 are forged images. The result shows that the proposed GJO based MSVM model delivers the performance metrics like accuracy, sensitivity, specificity, precision, and MCC values about 99.47 %, 97.01%, 96.51%, 99.62%, and 96.39% respectively which ensures accurate forgery detection compared with existing methods such as SSDAE-GOA-SHO, ConvLSTM, CNN and dual branch CNN methods.

Keywords: Copy-move forgery, Digital image, MICC-F2000, M-SVM, Tampered images.

1. Introduction

Digital images are widely used all over the world and the bad quality effect of an image harms digital images [1]. There are several ways to improve the image quality increasing contrast, brightness, and saturation and also changing a coloured image into grayscale images [2]. Nowadays, people are using image editing tools like Inshot, Canva, Snapseed, PicsArt, Adobe Photoshop and other applications to easily manipulate images. These digitally manipulated images are the main sources to impact individuals and society by spreading misleading information [3]. The manipulated images are presented nowadays in different sectors such as cinemas, politics, press and the accessibility of these resources to share the information makes the dangerous image tampering [4]. The long-range accommodating method equivalence relationship on Instagram and Facebook there has an extensive development of the image data delivered in the last decade and these pictures are primary sources of fake news [5]. Copy move forgery is a challenging mechanism in which an image region is copied and pasted into other regions with a similar image to hide unwanted regions of an image [6].

The copied regions are selected from a textured portion of the image to be invisible from human sight. This type of forgery is popular because there is a chance that copied portion of an image has the same content, texture and features [7]. There are different traditional techniques for image forgery detection, which mostly include key-points-based and block-based feature extraction and matching techniques [8]. Deep learning-based techniques are introduced for overcoming these issues of digital image forgery [9]. The block-based detection technique splits the image into small overlaying or non-overlaying blocks and these blocks are always square and rectangular. The matched technique is applied for feature extraction based on which blocks are matched to determine the parallelism [10]. The key-point based technique extracts the features from the input images and these are analysed to identify similarities. This technique is used to effectively detect image forgeries under rotation [11]. Machine learning based forgery detection, specifically the Convolutional Neural Network (CNN) has been established because CNN shows good performance in the object detection field and is used to find the copy move portions [12]. The proposed GJO based M-SVM for feature selection in forgery classification, the advantages include enhanced feature selection, improved classification accuracy, reduce dimensionality and computational complexity, robustness to noisy features, faster convergence, improved efficiency and flexibility. These advantages collectively contribute to the development of accurate, efficient and reliable forgery classification systems. The major contribution of this research is mentioned as follows,

- Preprocessing is done by using the image denoising method and the image features are extracted by using Resnet-50 and GLCM models.
- The GJO is utilized for feature selection which gives efficient search capability, global search ability, robustness, versatility and fewer assumption.
- The MSVM is utilized to handle multi-class classification and robustness against outliers which ensures accurate classification and effectively handle forgeries.

The remaining work is organized as follows: Section 2 illustrates the Literature review. The architecture of the proposed model is presented in section 3. The experimental result of this proposed model on various datasets is illustrated in section 4. Section 5 describes the summary of this paper and lastly, this paper finishes with the references.

2. Literature review

Elaskily [13] developed a deep learning-based technique for the effective copy-move forgery detection (CMFD) model in virtual images. The developed technique is based on architecture of CNN model. The developed method has been evaluated on various datasets like MICC-F220, MICC-F2000, and MICC-F600. The CNN classification was applied to classify the candidate images into tampered and original images. The developed CMFD model obtains high accuracy compared to other models and it proves the robustness against a diversity of known attacks. The developed technique required huge time to detect forgery from the noisy images.

Gupta [14] implemented a deep learning-based technique on Stacked Sparse Denoising Autoencoder (SSDAE) model to detect and classify the images as fake or legitimate. The hidden layers bias and input the weight of the SSDAE model are enhanced by using spotted hyena optimizer (SHO) and grasshopper optimization algorithm (GOA). The hybrid model of SSDAE-GOA-SHO has been evaluated by using four datasets named CASIA 2.0, MICC-F220, MICC-F2000, MICC-F600. This developed method is used to solve the statistical analysis and runtime analysis by evaluating the performance. This model only recognizes the image forgeries with duplicate minimum places and the large block size decreases the computing complexity.

Elaskily [15] introduced a deep learning method of hybrid convolutional long short-term memory (ConvLSTM) and convolutional neural network (CNN) for copy-move forgery detection (CMFD) model. This developed model extracts the image features using a pooling layer, ConvLSTM layers and Convolutions layers then compares features and detects the forgery. The model has been evaluated by using four various datasets named MICC-F220, SATs-130, MICC-F2000 and MICC-F600. This developed method achieves high performance with stability and minimum processing time in testing and learning process. This model maximize the computational complexity and it has existence of various spatial data.

Koul [16] presented a deep learning-based technique for automatic copy-move forgery detection (CMFD) in images by using MICC-F2000 dataset. This developed method is used for classification and extracts the features from images by using convolutional neural network (CNN). By using CNN, automatically features are learned and shared to classifier. The feature extraction comprised in the training CNN that contains Conv layers with activation function, pooling, fully connected and classification layers. The advantage of this model has accuracy and speed are better than other models for detecting forged images. This developed model does not work for those images which contains a minimum forged region and it only works in JPEG images.

Goel [17] suggested a deep learning technique for image copy-move forgery detection (CMFD) by using MICC-F2000 dataset. This developed model applied a dual-branch convolutional neural network (CNN) to classify the images. The developed model contains dual branches that are implemented in

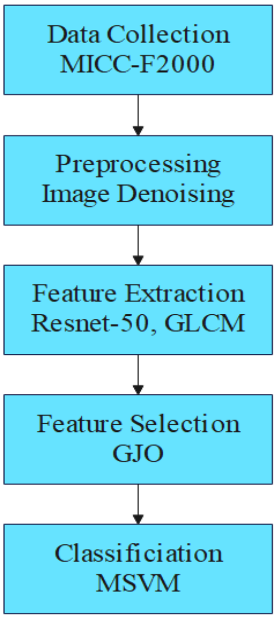

Figure. 1 Block diagram of the proposed method

various-size kernels for extracting features. This developed model is lightweight and achieves good accuracy in prediction and the computation time, performance scores are efficient compared to an existing model. This model cannot be utilized for over compressed images and also the comparison is limited to the classification stage.

These existing methods have various applications and also suffer from limitations. Hence, these limitations can be overcome in this manuscript by proposing GJO based MSVM methods.

3. Proposed method

The Machine learning based technique is proposed for image Copy-Move Forgery Detection (CMFD) and classification using MICC-F2000 dataset. The block diagram of the proposed method is shown in Fig. 1 which represents five different methods such as data collection, preprocessing, feature extraction, selection and classification.

3.1 Data collection

The machine learning based frameworks require a large dataset from training and testing of the model. Many datasets are available for detecting image forgery. This model uses the MICC-F2000 dataset [18] which is managed by 2000 images in this 1300 are original images and 700 are forged images. The image dimension is 2048×1536 pixels. After collecting the dataset, data are preprocessed by using the image denoising method.

3.2 Preprocessing

Preprocessing is done by using the image denoising method. When establishing the dataset, some noise points will be store on the left side of the image and it will affect the detection. Removing this noise can give better results in detection. In this paper, the Perona-Malik (P-M) equation is used to remove noise, which links the features of different regions of the image to diffusion. The diffusion coefficient in all directions is not constant but varies with the gradient modules of the image and it not only removes noise and also protects the edge from being smoothed. Edge detection is used to achieve forgery positioning and the edges are not smoothed to make the effect better. This is the main reason why the P-M equation is used. The Perona-Malik equation is shown in Eq. (1),

$$\frac{\partial u}{\partial t} = div\left(c(|\nabla u(x,y,t)|)\nabla u(x,y,t)\right) \qquad (1)$$

Where, $u_t = r(x,y,t)$ is an image obtained after a diffusion time t, div is the divergence operator, and ∇ is the gradient operator concerning the variable x and y. After the denoising process, the image can be used to extract the feature.

3.3 Feature extraction

In the dataset, the number of layers calculates how many features remain and that requires to be trained on. For this purpose, the Residual Network (Resnet-50) [19] and gray-level Co-Occurrence Matrix (GLCM) [20] are used for feature extraction. The residual network contains five stages. The input stage is the first stage, which contains only one convolutional layer with batch normalization and the initial feature map is generated by using the activation function. The remaining states have identity blocks and convolutional blocks. These two blocks contain a convolutional layer with activation functions and additional batch normalization. To increase the residuals of the convolutional blocks, the input layer has an extra bridge to the output layer. The residual block on Resnet-50 is represented in Eq. (2),

$$y = F(x, W + x) \qquad (2)$$

Where, x and y represent the input and output layer respectively, F function is represented by the residual map. Residual block on the Resnet-50 is accomplished when the input data are identical to the output data.

Gray-level Co-Occurrence Matrix (GLCM) is a numerical method used as image feature extraction in second order and that considers the structural relationship between the pixels. The GLCM feature is examined based on region of interest (ROI) dimension by using a square matrix of the number of gray levels (N). GLCM obtained twenty-two texture-based features including contrast, energy, entropy, correlation, homogeneity, autocorrelation, inverse different movement (IDM), sum variance, dissimilarity, IDM normalization, maximum probability and more. A few of them are given in Eqs. (3) to (5), where, $p(i,j)$ is the element of normalized GLCM matrix and N is the number of gray levels.

$$\text{Contrast} = \sum_i \sum_j |i-j|^2 p(i,j) \tag{3}$$

The contrast is the intensity of the pixel and its neighbour over the image. Additionally, it also examines the number of local variations demonstrated in the image. This is calculated by the variance in brightness and colour of every object to the various objects with the same area.

$$\text{Energy} = \sum_{i,j} p(i,j)^2 \tag{4}$$

The energy calculates the pixel pair in degrees. It is the disorder calculation of an image and the highly corresponding pixels; the value of energy is high.

$$\text{Entropy} = \sum_{i=0}^{N_g-1} \sum_{j=0}^{N_g-1} p(i,j) \log\left(p(i,j)\right) \tag{5}$$

The entropy calculates the degree between pixel and randomness to the image and it is used to characterize the image texture. Entropy is inversely correlated to energy when a large grey level entropy is high. After the feature extraction, the image features are selected using an optimization process.

3.4 Feature selection

Feature selection is done by using golden jackal optimization (GJO). It is stimulated by the golden jackal's behaviour in pair of bond-hunting and it is shown by their choral howling. The golden jackal howling is examined as a certain type of engagement. The golden jackal with the choral howl, informs others of their position and communicates with others. Cooperative foraging is utilized by the golden jackal, which allows them to search for larger prey. The search space golden jackal population is represented in Eq. (6),

$$X_0 = LB + rand \times (UB - LB) \tag{6}$$

Where, LB and UB are the lower boundary and upper boundary respectively with $rand$ as a search space random number in the [0, 1] range. In the mimicking phase, the golden jackals hunting behaviour is displayed in the exploitation, exploration and transition phase from the exploitation and exploration phase.

In the exploration phase, golden jackals track their prey. However, the prey cannot continuously mark in some areas and is easy to lose. The prey strength is represented as Evading Energy E_v. Whenever the $|E_v|$ is higher than 1 at that time the prey has sufficient strength to escape. In this state, the exploration phase is occurring, and the global jackals hunting action is to select the male (X_{male}) as the leader and the female (X_{female}) as the adherent is represented in Eqs. (7) and (8),

$$X_M = X_{male} - E_v \left| X_{male} - \left(0.05 \times LF_D(\beta) \otimes X_{prey}\right) \right| \tag{7}$$

$$X_F = X_{female} - E_v \left| X_{female} - \left(0.05 \times LF_D(\beta) \otimes X_{prey}\right) \right| \tag{8}$$

Where, X_{prey} is the position of prey vector with the constant of 0.05, $\otimes$ is the element wise multiplication and the LF_D is the Levy flight. The movement of X_{male} and X_{female} are managed by the prey evading energy $E_v = E_{ld} \times E_0 . E_{ld}$ represents the decrease level of prey energy. $E_{ld} = 1.5 \times (1 - \frac{1}{T})$ is the linear decrement energy which reduces from 1.5 to 0 during the generation. E_0 is the initial prey energy that is equal to $2 \times rand - 1$ with the range of [0,1]. The mathematical representation of the Levy flight is shown in Eq. (9),

$$LF_D(\beta) = \left(\frac{U_D \cdot \sigma}{|V_D|^{\frac{1}{\beta}}}\right), \qquad \sigma = \left(\frac{\Gamma(1+\beta) \times \sin\left(\frac{\pi\beta}{2}\right)}{\Gamma\left(\frac{1+\beta}{2}\right) \times \beta \times 2^{\left(\frac{\beta-1}{2}\right)}}\right)^{\frac{1}{\beta}} \tag{9}$$

Where, the random numbers U_D and V_D is the normal distribution result to the standard deviations of U_D is σ and V_D is 1. The Levy flight parameter β is 1.5 and the Levy flight vector dimension is D.

In the exploitation phase, the golden jackal pair surrounds the prey and chase them and the evading energy E_v is weak. This demonstrates that the $|E_v|$ is lower than 1 and at the time the exploitation happens. The golden jackal achieves in enclose the prey and charge the prey until it lifeless. The behaviour of pair hunting golden jackal's male (X_{male}) and female (X_{female}) is represented in below Eqs. (10) and (11),

$$X_M = X_{male} - E_v\left|(0.05 \times LF_D(\beta) \otimes X_{male}) - X_{prey}\right| \quad (10)$$

$$X_F = X_{female} - E_v\left|\left(0.05 \times LF_D(\beta) \otimes X_{female}\right) - X_{prey}\right| \quad (11)$$

Where, X_{prey} is the position of prey vector, the X_{male} and X_{female} is represented in Eq. (7) and Eq. (8), the male (X_{male}) and female (X_{female}) position is determined by the constant as 0.05, the Levy Flight $LF_D(\beta)$ vector D represents in Eq. (9). This is the variations of the golden jackal exploitation movement matched to the exploration. The Levy Flight $LF_D(\beta)$ and the constant value of 0.05 is applied for eliminating the local optima idleness. However, considering the golden jackal approach, the exploitation of prey evading energy E_v the operator performs similarly as in the exploration phase.

The Joint Opposite Selection (JOS) is used for improving the Golden Jackal Optimization performance. This JOS is a combination of Dynamic Opposite (DO) and the Selection Leading Opposition (SLO). The effectiveness of this algorithm is evaluated in terms of computational complexity. The complexity of JOS is represented in Eqs. (12) to (14),

$$O(SLO) = O(NP \times T \times D_c) \quad (12)$$

Where, the NP is the various number of golden jackals, T is the number of highest iterations and D_c is the close distance dimension.

$$O(DO) = O(NP \times J_r \times T \times D) \quad (13)$$

Where, the NP is the various number of golden jackals, J_r is the rate of the jump, T is the highest iterations and D is the dimension. The efficiency of computational complexity for GJO-JOS is represented in Eq. (14):

$$O(GJO - JOS) = O(NP \times T\left(2 + D_c + D(T + J_r)\right) \quad (14)$$

The memory requirement of this algorithm is determined by using the variable and parameter size. The GJO-JOS memory size is $k \times (NP \times D)$.

3.1.4. Fitness function

The fitness function is used for solving the imbalance issues in optimization algorithms and the frequently used fitness function is weighted average classification accuracy (avg) for classifying the imbalanced data. However, this fitness function is mandatory to give the weight but the assurance of weight is specific. To commonly treat the majority and minority class the weight w= 0.5 is used. In imbalanced data classification, the Area Under Curve (AUC) is a significant measure and is also used in the fitness function. In common, GJO with AUC as a fitness function consumes a large training time and gives better performance in evaluation. The AUC is represented in Eqs. (15) and (16),

$$AUC_F = \sum_{I=1}^{N-1} \frac{1}{2} * (FPR_{i+1} - FPR_i)(TPR_{i+1} - TPR_i) \quad (15)$$

Where N is the threshold number, FPR_i and TPR_i are the ith threshold of the false positive rate and true positive rate respectively.

$$AUC_w = \frac{\sum_{i\in Min}\sum_{j\in Maj} I_{wmw}(P_i,P_j)}{|Min|*|Maj|} \quad (16)$$

The mathematical form of $I_{wmw}\left(P_i, P_j\right)$ is represented in Eq. (17),

$$I_{wmw}\left(P_i, P_j\right) = \begin{cases} 1, & P_i > P_j \ and \ P_i \geq 0 \\ 0, & otherwise \end{cases} \quad (17)$$

The P_i and P_j represents the output values taking an instance of i and j from the minority class and majority class as input respectively. $|Min|$ and $|Maj|$ illustrate the number of minority class and majority class instances respectively.

3.5 Classification

After selecting features from a featured image, the multi-support vector machine (M-SVM) [21] is applied for classifying the images as original and forged images. In the forgery detection process, the classification is the final stage and it is a supervised learning method. In this method, the target variable is known and a sufficient number of values are given whereas unsupervised learning has observed only a limited number of data and the target variable is not known. Support vector machine (SVM) is a part of supervised machine learning techniques that has larger classification efficiency while matched to various classification models. But the implementation of the SVM is limited because of the need for high training time for larger data. The SVM integrated with feature selection techniques acquire reduced dimension data. The M-SVM classification is involved in classifying the original and forged

Received: June 19, 2023. Revised: August 6, 2023.

Table 1. Represents the various classifiers with actual features for the MICC-F2000 dataset

Methods	Accuracy (%)	Sensitivity (%)	Specificity (%)	Precision (%)	MCC (%)
KNN	86.40	86.75	87.13	89.74	88.67
RF	89.0	88.91	89.53	91.86	90.46
DT	92.03	92.84	93.01	94.87	93.90
MSVM	94.87	95.01	94.58	95.49	94.31

Table 2. Represents the various classifiers with optimized features for the MICC-F2000 dataset

Methods	Accuracy (%)	Sensitivity (%)	Specificity (%)	Precision (%)	MCC (%)
KNN	87.01	88.41	88.57	91.27	92.01
RF	90.72	91.32	91.76	92.41	92.31
DT	93.67	93.91	94.32	95.01	94.33
MSVM	99.47	97.01	96.51	99.62	96.39

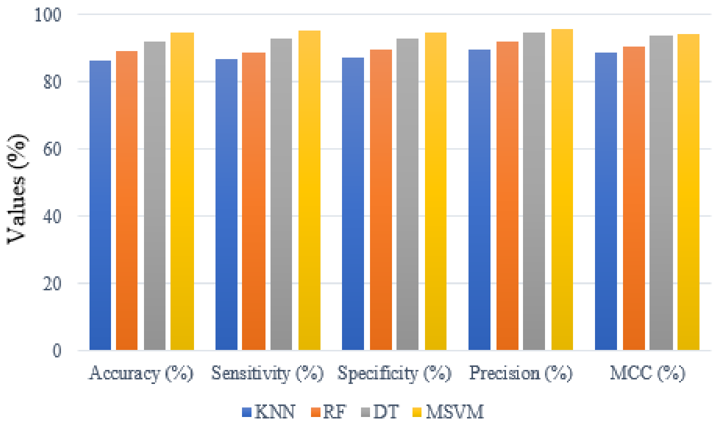

Figure. 2 Represents the performance of MICC-F2000 image classification with actual features

images. The proposed M-SVM method has the advantage of effective analysis of the non-linear relationship of the processes and the features of the data parallel to provide efficient classification. The forgery image detection is done by utilizing a systematic basis of M-SVM classifier by involving a basic procedure that considers two phases such as training and testing phase.

4. Result

In this paper, the proposed model is replicated using M-SVM with the system requirements. The parameters like accuracy, sensitivity, specificity, precision and MCC are used to evaluate the performance of this model. The mathematical representation of these parameters is shown in Eqs. (18) to (22),

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \times 100 \quad (18)$$

$$Sensitivity = \frac{TP}{FN+TP} \times 100 \quad (19)$$

$$Specificity = \frac{TN}{FP+TN} \times 100 \quad (20)$$

$$Precision = \frac{TP}{TP+FP} \times 100 \quad (21)$$

$$MCC = \frac{TP\times TN-FP\times FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}} \times 10 \quad (22)$$

Where, TP, FP, TN and FN represents the True Positive, False Positive, True Negative and False Negative respectively.

4.1 Quantitative analysis

This section shows the quantitative analysis of M-SVM model without augmentation in accuracy, sensitivity, specificity, precision and MCC are shown in Table 1 to 4 respectively. Table 1 and 2 illustrates the quantitative analysis of various classifiers with actual and optimized features by employing the MICC-F2000 dataset. Table 3 illustrate the quantitative analysis of various optimization by employing the MICC-F2000 dataset. Table 4 illustrates the performance analysis of K-fold validation on MICC-F2000 dataset. Figure 5 illustrates the graphical representation of the performance analysis of k-fold validation on MICC-F2000 dataset.

As shown in Fig. 2 the performance measure of classifiers on MICC-F2000 dataset with actual features. The accuracy, specificity, sensitivity, precision and MCC of the decision tree (DT),

Table 3. Represents the various optimization for the MICC-F2000 dataset

Methods	Accuracy (%)	Sensitivity (%)	Specificity (%)	Precision (%)	MCC (%)
PSO	91.29	91.40	91.35	91.79	92.09
GWO	91.54	91.38	91.48	91.78	92.65
ABC	93.21	93.98	94.06	94.21	94.52
GJO	99.47	97.01	96.51	99.62	96.39

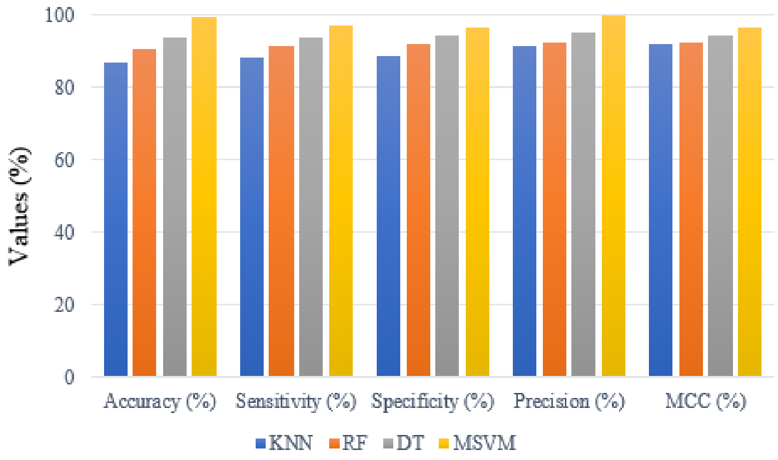

Figure. 3 Represents the performance of MICC-F2000 image classification with optimized features

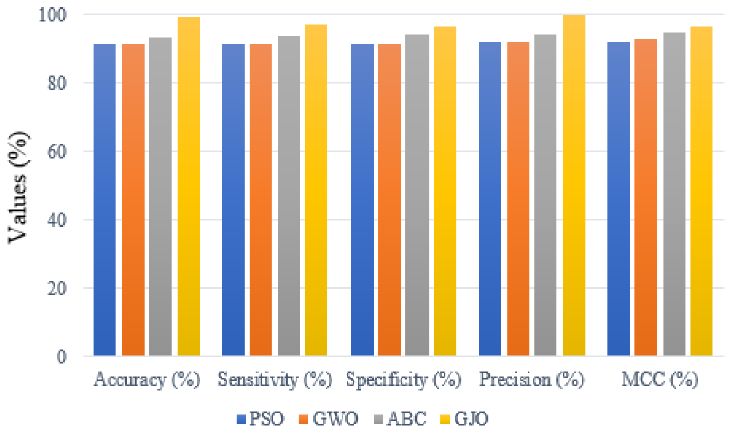

Figure. 4 Represents the performance of MSVM with optimization on MICC-F2000 dataset

reinforcement learning (RF) and K-nearest neighbour (KNN) are measured and matched with this proposed MSVM model. The obtained result shows that the proposed MSVM model achieves better results by using performance metrics like accuracy, specificity, sensitivity, precision, and MCC values of about 94.87%, 94.58%, 95.01%, 95.49% and 94.31% respectively while considering feature selection compared to other classifiers.

As shown in Fig. 3 the performance measure of classifiers on MICC-F2000 dataset with actual features are compared to those optimized features. The accuracy, specificity, sensitivity, precision and MCC of Decision Tree (DT), Reinforcement Learning (RF) and K-Nearest Neighbor (KNN) are measured and matched with the proposed MSVM. The obtained result shows that the proposed MSVM model achieves better results by using performance metrics such as accuracy, specificity, sensitivity, precision and MCC values of about 99.47%, 96.51%, 97.01%, 99.62% and 96.39% respectively while considering optimized features compared to other classifiers.

As shown in Table 3 and Fig. 4 describes the performance of MSVM using various optimization methods like grey wolf optimization (GWO), artificial bee colony (ABC), particle swarm optimization (PSO) and golden jackal optimization (GJO). The obtained result shows that the proposed GJO achieves better results by using performance metrics such as accuracy, specificity, sensitivity, precision and MCC values of about 99.47%, 96.51%,

Table 4. Represents the performance analysis of K-fold validation on MICC-F2000 dataset

K-fold Scores	Accuracy (%)	Sensitivity (%)	Specificity (%)	Precision (%)	MCC (%)
4-fold	92.10	93.05	92.36	93.08	92.75
5-fold	99.47	97.01	96.51	99.62	96.39
7-fold	93.03	93.42	93.58	93.74	93.16
9-fold	93.40	94.64	94.04	94.38	93.89
10-fold	94.41	94.95	94.79	95.03	94.27

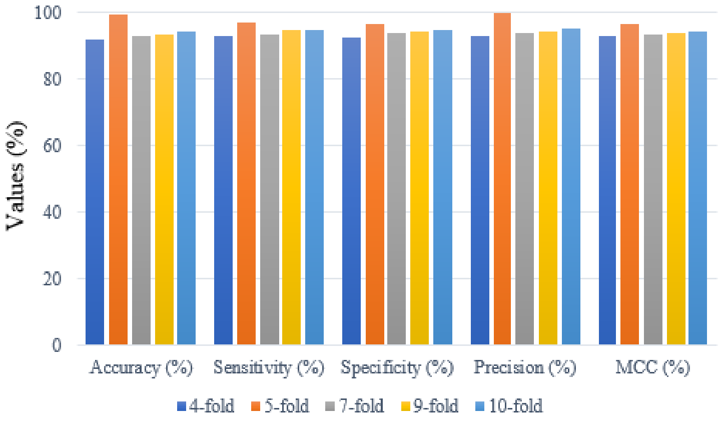

Figure. 5 Represents the performance of K-fold validation on MICC-F2000 dataset

97.01%, 99.62% and 96.39% respectively while considering feature selection compared to another optimization algorithm.

4.2 Comparative analysis

This section demonstrates the comparative analysis of MSVM classifier with performance metrics like Accuracy and Precision as shown in Table 5. Existing research such as [13, 14, 15, 16, 17] are used for evaluating the ability of this classifier. This proposed method is trained, tested, and validated using MICC-F220, MICC-F600, MICC-F2000 and CASIA 2.0 dataset. The accuracy was improved to 99.47% and the precision of 99.62%. The existing values are taken at 25 iterations then the FNR value becomes zero at 35th iteration. To achieve better performance the experiments are performed in same environment with 25 iterations. The proposed GJO was evaluated for efficient classification by using the MSVM technique by overcoming overfitting problems and dataset classification.

4.2.1. Discussion

This section illustrates the proposed method advantages and existing methods limitations. The existing model has some limitations such as, the deep CMFD using CNN [13] model required huge time to detect forgery from the noisy images. The SSDAE-GOA-SHO [14] model only recognizes the image forgeries with duplicate minimum places and the large block size decreases the computing complexity. The ConvLSTM [15] model maximize the computational complexity and it has existence of various spatial data. The CNN [16] model does not work for those images which contains a minimum forged region and it only works in JPEG images. The dual branch CNN [17] model cannot be utilized for over compressed images and also the comparison is limited to the classification stage. The proposed GJO based MSVM model overcome these limitations. The GJO optimizes the feature selection process by iteratively searching for the most informative subset of features. By leveraging the exploration and exploitation of GJO, the algorithm efficiently explores the feature space, selecting relevant features that contribute to accurate forgery classification. This enhance the performance of MSVM by focusing on the most discriminative features. By combining MSVM with GJO for feature selection in forgery classification, the proposed model obtains better result in terms of accuracy and precision values about 99.47% and 99.62% respectively.

5. Summary

The image copy-move forgery is a challenging mechanism in which an image region is copied within itself to achieve one specific goal. In this paper, a new golden jackal optimization (GJO) based multi-support vector machine (M-SVM) model is proposed for effective forgery detection and it classifies the

Table 5. Comparative analysis of proposed method with existing methods

Technique	Dataset	Accuracy (%)	Precision (%)
Deep CMFD using CNN [13]	MICC-F220	96.15	N/A
	MICC-F600	94.11	N/A
	MICC-F2000	95.1	N/A
SSDAE-GOA-SHO [14]	MICC-F220	97.45	98.75
	MICC-F600	98.92	88.45
	MICC-F2000	99.12	99.25
	CASIA 2.0	98.02	96.03
ConvLSTM [15]	MICC-F220	93.9	N/A
	MICC-F600	86.3	N/A
	MICC-F2000	96.6	N/A
CNN [16]	MICC-F2000	97.5	97
Dual branch CNN [17]	MICC-F2000	96	89
Proposed GJO based MSVM	MICC-F220	98.25	96.87
	MICC-F600	99.42	93.98
	MICC-F2000	99.47	99.62
	CASIA 2.0	98.99	97.92

images as original and forgery. The image features are extracted by using Resnet-50 and Gray-Level Co-Occurrence Matrix (GLCM). Resnet-50 consisting five stages for extract the features and GLCM is used to extract the image features in second order and that considers the structural relationship between the pixels. Feature selection is done by using golden jackal optimization (GJO). It is stimulated by the behaviour of golden jackals in pair bond-hunting. The proposed GJO based M-SVM method delivers the performance metrics like accuracy, specificity, sensitivity, precision, and MCC values about 99.47%, 97.01%, 96.51%, 99.62%, and 96.39% respectively which ensures accurate forgery detection compared with state-of-art methods. The obtained result shows that the proposed model achieves better result on MICC-F2000 dataset which consists of 2000 images in this 1300 are original and 700 are forged images. The future work includes hyperparameter tuning in optimization algorithms for improving the performance of the model.

Notations

Notation	Description
div	Divergence operator
∇	Gradient operator
$u_t = r(x, y, t)$	Image obtained after a diffusion time t
x	Input layer
y	Output layer
F	Residual map
$p(i, j)$	Element of normalized GLCM matrix
N	Number of gray levels
LB	Lower boundary
UB	Upper boundary
$rand$	Search space random number
E_v	Evading energy
X_{prey}	Position of prey vector
X_{male}	Golden jackal male
X_{female}	Golden jackal female
$\otimes$	Element wise multiplication
LF_D	Levy flight
E_{ld}	Linear decrement energy
E_0	Initial prey
U_D and V_D	Random numbers in levy flights
σ	Standard deviation
β	Levy flight parameter
D	Levy flight vector dimension
NP	Number of jackals
T	Number of maximum iterations
D_c	Close distance dimension
J_r	Jumping rate
FPR_i	False positive rate at ith threshold
TPR_i	True positive rate at ith threshold
P_i	Output value of a program P taking instance i from the minority class as input
P_j	Output value of a program P taking instance j from the majority class as input
$\|Min\|$	Number of minority class instances
$\|Max\|$	Number of majority class instances
TP	True positive
FP	False positive
TN	True negative
FN	False negative

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

All authors contributed to the study's conception and design. Material preparation, data collection, and analysis were performed by all three authors. The first draft of the manuscript was written by Archana, and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

References

[1] M. A. Basset, G. Manogaran, A. E. Fakhry, and I. E. Henawy, "2-Levels of clustering strategy to detect and locate copy-move forgery in digital images", *Multimedia Tools and Applications*, Vol. 79, Nos. 7-8, pp. 5419-5437, 2020.

[2] S. Krishnamurthy, K.A. Neelegowda, and B.G. Prasad, "IFLNET: Image Forgery Localization Using Dual Attention Network", *International Journal of Intelligent Engineering & Systems*, Vol. 15, No. 6, pp. 166-178, 2022, doi: 10.22266/ijies2022.1231.17.

[3] K. D. Kadam, S. Ahirrao, and K. Kotecha, "Efficient approach towards detection and identification of copy move and image splicing forgeries using mask R-CNN with MobileNet V1", *Computational Intelligence and Neuroscience*, Vol. 2022, p. 6845326, 2022.

[4] E. A. A. Vega, E. G. Fernández, A. L. S. Orozco, and L. J. G. Villalba, "Copy-move forgery detection technique based on discrete cosine transform blocks features", *Neural Computing and Applications*, Vol. 33, No. 10, pp. 4713-4727, 2021.

[5] S. Dhivya, J. Sangeetha, and B. Sudhakar, "Copy-move forgery detection using SURF feature extraction and SVM supervised learning technique", *Soft Computing*, Vol. 24, No. 19, pp. 14429-14440, 2020.

[6] A. Badr, A. Youssif, and M. Wafi, "A Robust Copy-Move Forgery Detection in Digital Image Forensics Using SURF", In: *Proc. of 2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, Beirut, Lebanon, pp. 1-6, 2020.

[7] A. Pourkashani, A. Shahbahrami, and A. Akoushideh, "Copy-move forgery detection using convolutional neural network and K-mean clustering", *International Journal of Electrical and Computer Engineering*, Vol. 11, No. 3, pp. 2604-2612, 2021.

[8] A. F. H. Sewan, and M. S. M. Altaei, "Forged Copy-Move Recognition Using Convolutional Neural Network", *Al-Nahrain Journal of Science*, Vol. 24, No. 1, pp. 45-56, 2021.

[9] P. Selvaraj and M. Karuppiah, "Enhanced copy–paste forgery detection in digital images using scale-invariant feature transform", *IET Image Processing*, Vol. 14, No. 3, pp. 462-471, 2020.

[10] P. Niyishaka and C. Bhagvati, "Copy-move forgery detection using image blobs and BRISK feature", *Multimedia Tools and Applications*, Vol. 79, Nos. 35-36, pp. 26045-26059, 2020.

[11] S. I. Lee, J. Y. Park, and I. K. Eom, "CNN-Based Copy-Move Forgery Detection Using Rotation-Invariant Wavelet Feature", *IEEE Access*, Vol. 10, pp. 106217-106229, 2022.

[12] M. T. Abdullah and N. H. M. Ali, "DeepFake Detection Improvement for Images Based on a Proposed Method for Local Binary Pattern of the Multiple-Channel Color Space", *International Journal of Intelligent Engineering & Systems*, Vol. 16, No. 3, pp. 92-104, 2023, doi: 10.22266/ijies2023.0630.07.

[13] M. A. Elaskily, H. A. Elnemr, A. Sedik, M. M. Dessouky, G. M. E. Banby, O. A. Elshakankiry, A. A. M. Khalaf, H. K. Aslan, O. S. Faragallah, and F. E. A. E. Samie, "A novel deep learning framework for copy-moveforgery detection in images", *Multimedia Tools and Applications*, Vol. 79, Nos. 27-28, pp. 19167-19192, 2020.

[14] R. Gupta, P. Singh, T. Alam, and S. Agarwal, "A deep neural network with hybrid spotted hyena optimizer and grasshopper optimization algorithm for copy move forgery detection", *Multimedia Tools and Applications*, 2022.

[15] M. A. Elaskily, M. H. Alkinani, A. Sedik, and M. M. Dessouky, "Deep learning based algorithm (ConvLSTM) for copy move forgery detection", *Journal of Intelligent & Fuzzy Systems*, Vol. 40, No. 3, pp. 4385-4405, 2021.

[16] S. Koul, M. Kumar, S. S. Khurana, F. Mushtaq, and K. Kumar, "An efficient approach for copy-move image forgery detection using convolution neural network", *Multimedia Tools and Applications*, Vol. 81, No. 8, pp. 11259-11277, 2022.

[17] N. Goel, S. Kaur, and R. Bala, "Dual branch convolutional neural network for copy move forgery detection", *IET Image Processing*, Vol. 15, No. 3, pp. 656-665, 2021.

[18] Dataset link: http://lci.micc.unifi.it/labd/2015/01/copy-move-forgery-detection-and-localization/.

[19] D. C. R. Novitasari, R. Hendradi, Y. Farida, R. E. Putra, R. Nariswari, R. A. Saputra, and R. D. N. Setyowati, "Effective Hybrid Convolutional-Modified Extreme Learning Machine in Early Stage Diabetic Retinopathy", *International Journal of Intelligent Engineering & Systems*,

Vol. 16, No. 2, pp. 401-413, 2023, doi: 10.22266/ijies2023.0430.32.

[20] A. Muntasa and M. Yusuf, “Multi Distance and Angle Models of the Gray Level Co-occurrence Matrix (GLCM) to Extract the Acute Lymphoblastic Leukemia (ALL) Images”, *International Journal of Intelligent Engineering & Systems*, Vol. 14, No. 6, pp. 357-368, 2021, doi: 10.22266/ijies2021.1231.32.

[21] B. B. Rudra, and G. Murtugudde, “Hybrid Feature Selection with Parallel Multi-Class Support Vector Machine for Land Use Classification”, *International Journal of Intelligent Engineering & Systems*, Vol. 15, No. 1, pp. 85-94, 2022, doi: 10.22266/ijies2022.0228.09.