# Image Content Forgery Detection Model Combining PSO and SVM in Electronic Data Forensics

Lingyu Liao, Yang Lei*
Department of Investigation, Fujian Police College, Fuzhou 350007, China
E-mail: fzleyan@163.com
*Corresponding author

**Keywords:** Support vector machines; Particle swarm optimization algorithm; Forgery detection; Image content; Electronic data forensics

**Received:** March 13, 2024

*With the rapid progress of information technology, the Internet is saturated with copious amounts of data and visuals. However, with the widespread availability of different image editing software, counterfeit image content arises periodically. To tackle image content forgery, the research is founded on the Gaussian mixture distribution similarity measure image forgery detection algorithm. The image classifier underwent training through encoding its underlying features and utilizing the encoded data as inputs for the support vector machine. Optimization of the support vector machine was performed simultaneously using the improved particle swarm optimization algorithm. The results indicated that the SVM-based image content forgery detection model, which employed improved particle swarm optimization, achieved a detection rate of 94.89% and processed the images in 22.06 milliseconds. In summary, the study of an image content forgery detection model that combines improved particle swarm optimization and support vector machine in electronic data forensics has resulted in a high detection accuracy.*

*Povzetek: Model za zaznavanje ponaredb slik združuje PSO in SVM za forenziko elektronskih podatkov. Uporablja izboljšani algoritma rojev delcev in podpornih vektorjev.*

## 1 Introduction

The replication and forgery of image content, whether it be movement, regional replication, or otherwise, has become a serious social problem due to the rapid development of information technology [1]. To combat this illegal behavior effectively, electronic forensics' use for evidence acquisition and parsing appears paramount. Electronic data forensics (EDF) refers to the entire process of acquiring, preserving, validating, verifying, interpreting, analyzing, archiving, and presenting evidence related to computer intrusion, sabotage, fraud, attack, and other criminal acts in a manner that adheres to legal norms [2]. The determination of the legal validity of electronic evidence needs to follow the principles of authenticity, completeness, and legality [3]. This is achieved through the use of computer hardware and software technology. In today's internet, a vast amount of information and images fill the network. Images, being one of the most intuitive forms of communication in people's daily lives, hold a crucial role [4]. However, with the widespread popularity of various image editing software, the phenomenon of forgery of image content copying and movement or region copying and forgery also frequently occurs. This illicit conduct deceives others through tampering, counterfeiting, or manufacturing false images, which constitutes a serious violation of intellectual property rights and may lead to criminal activities such as fraud, thereby causing significant harm to both society and individuals [5]. The use of image forgery technology may raise ethical concerns related to privacy and abuse, as it can violate personal privacy and damage personal image without consent. For instance, reconstructing or tampering with public photos using this technology may put individuals in unfavorable or awkward situations without their consent, which violates their privacy rights. Moreover, the misuse of image forgery technology may result in confusion or dissemination of misleading information. In fields such as social media and news, manipulated images can be utilized to disseminate false information, leading to public deception and erosion of social trust. The Gaussian mixture distribution similarity measure algorithm is an effective method for image content forgery detection (ICFD). It encodes the image's underlying features and uses them as inputs for classifier training in a support vector machine (SVM) to identify image region replication forgery [6]. SVM is a supervised learning model used in classification and regression analysis, which can play an important role in forgery detection of image content copying and movement [7]. Due to the continuous updating and iteration of information technology, new image encryption methods are constantly being developed. This further increases the difficulty of recognizing and detecting forged image content. One such method is the secret sharing encryption

method, which uses polarization-assisted secret sharing phase encoding to hide forged secret information in orthogonal polarization channels. This improves the difficulty of decryption [8]. The encryption method encodes each pixel for sub-pixel sharing and combines the dual encryption polarization key to reconstruct the target image. This increases the difficulty of detecting image content area duplication and forgery [9]. Against this background, this study aims to improve the accuracy of ICFD and effectively combat image content forgery. To achieve this, SVM is innovatively utilized to learn the features of real and fake images and identify the differences between them during the training process. At the same time, in order to improve the accuracy of forgery detection, the study also uses the improved particle swarm optimization (PSO) algorithm to optimize SVM parameters, in order to improve the accuracy of ICFD in EDF. The contribution of the research lies in applying Gaussian mixture model (GMM) to ICFD, proposing an image forgery detection algorithm that combines local feature aggregation description encoding of SVM and GMM to improve the accuracy of color feature extraction and classification. At the same time, the PSO algorithm is applied to optimize SVM parameters to solve the problem of selecting parameters for detecting content forgery in SVM images. The study is divided into four primary segments, and in the second segment, a thorough evaluation of the existing domestic and international research on SVM and ICFD technology is conducted. The third section details the development of an image content forgery detection by support vector machine (ICFD-SVM) model to enhance PSO optimization for EDF. The first section investigates ICFD-SVM using Gaussian Mixture Distribution Local Feature Aggregation Description Coding. The second section implements ICFD-SVM utilizing enhanced PSO optimization. The fourth section validates the optimized PSO ICFD-SVM model for EDF.

## 2 Related works

ICFD technology is a crucial approach to guarantee the authenticity and integrity of images. It has attracted considerable attention from experts and scholars and has yielded fruitful findings through extensive research. To solve the issues of facial manipulation techniques in digital media forensics, Chen S and other researchers proposed a new method for face forgery detection through local relation learning, which utilizes a multi-scale patch similarity module for measuring the similarity between local area features. The findings shown that the approach, with robustness and interpretability, regularly outperforms the state-of-the-art methods in commonly used benchmark tests [10]. In order to address the impact of forged fingerprints in biometric-based security systems, Baskar M and other scholars proposed a region-centered detail propagation measurement-based method to detect forged fingerprints, which utilizes a multistage Gabor filter to remove the noise points, and then converts the enhanced image into a number of integral images. The results indicated that the method effectively improved the accuracy of forged fingerprint detection [11]. To design an effective method that can accurately detect in-depth forged images or videos, the research team of Arunkumar P M proposed to utilize deep learning techniques and introduced a fuzzy Fisher face model with capsule biplots to detect different types of fake images or videos. The results showed that the method achieved 89.32% accuracy in the dataset [12].

SVM plays an important role in ICFD techniques. To analyze negative and positive classes in movie review texts, Styawati S's research team used SVM in combination with Firefly algorithm to successfully construct a SVM-based sentiment classification model. This model is based on an optimized combination of 9 parameters. The results showed that the model achieved up to 89% accuracy in sentiment classification, demonstrating its excellent performance [13]. Muthukrishnan et al. proposed a machine learning method for modeling and simulating heat exchangers in order to conduct virtual analysis of the performance of manufactured products before manufacturing simulation. This method simulated and analyzed heat exchangers, allowing engineers to analyze their performance before manufacturing. The results showed that this method is feasible [14]. Aldino A and other researchers proposed using SVM algorithm to classify specific data on the platform in order to classify specific standards. Then, they divided the data into two label categories and rated and tested the label data. The results showed that the classification accuracy of SVM reached 97% [15]. The summary table of related work is shown in Table 1.

Table 1: Summary of related work

| Author | Technology | Method | Result | The gap in the current state-of-the-art (SOTA) methods |
|---|---|---|---|---|
| Chen S et al. [10] | Facial forgery detection based on local relationship learning | Using a multi-scale patch similarity module to measure the similarity between local region features | Robustness and interpretability in benchmark testing | Not universal |

| | | | | |
|---|---|---|---|---|
| Baskar M et al. [11] | Measurement method based on regional center detail propagation | Using multi-level Gabor filters to remove noise points, and then converting the enhanced image into several integrated images | Effectively improving the accuracy of counterfeit fingerprint detection | Low generalization ability |
| Arunkumar P M et al. [12] | Fuzzy Fisher face model detection method | Utilizing deep learning techniques and introducing a fuzzy Fisher face model with capsule dual images | The accuracy in the dataset reached 89.32% | Not universal |
| Styawati S et al. [13] | SVM based sentiment classification model | A sentiment classification model based on SVM was constructed by combining support vector machine and Firefly algorithm. | The highest accuracy in sentiment classification is 89% | Not universal |
| Muthukrishnan S et al. [14] | Machine learning methods for modeling and simulation of heat exchangers | Simulate and analyze heat exchangers using machine learning before manufacturing simulation | Feasible | Low accuracy |
| Aldino A A et al. [15] | A specific standard classification method based on support vector machine algorithm | Using support vector machine algorithm to classify specific data on the platform, and then dividing it into two label categories | The classification accuracy reached 97%. | Low generalization ability |

In summary, while significant progress has been made in ICFD techniques and SVM, research on ICFD in the EDF field remains inadequate. Thus, investigating the combination of PSO with ICFD-SVM modeling in EDF is crucial to obtaining favorable outcomes in this area.

# 3 Improved ICFD-SVM model design for PSO optimization for electronic data forensics

In this chapter, ICFD using similarity measure based on GMM and combining SVM with local feature aggregation descriptive coding of GMM for more effective color feature extraction and classification. To raise the model's accuracy and performance, the SVM model's parameters are also tuned via the enhanced PSO algorithm.

## 3.1 ICFD-SVM based on gaussian mixture distribution local feature aggregation description coding

Expectation maximization (EM) is a technique used in clustering that is taught using the Gaussian distribution (GD) as a parametric model [16]. One of the most prevalent distribution types that may be observed in vast quantities in nature is the GD, sometimes known as the normal distribution [17]. In both natural and fake images, each pixel point can be considered as clustered data for GMM. Therefore, training using EM algorithm can effectively deal with the problem of adapting data to GMM in images. By adapting natural and forged images to GMM separately, similarity measurement and detection of image content forgery can be performed. The flow of ICFD algorithm for similarity measurement based on GMM is shown in Figure 1.

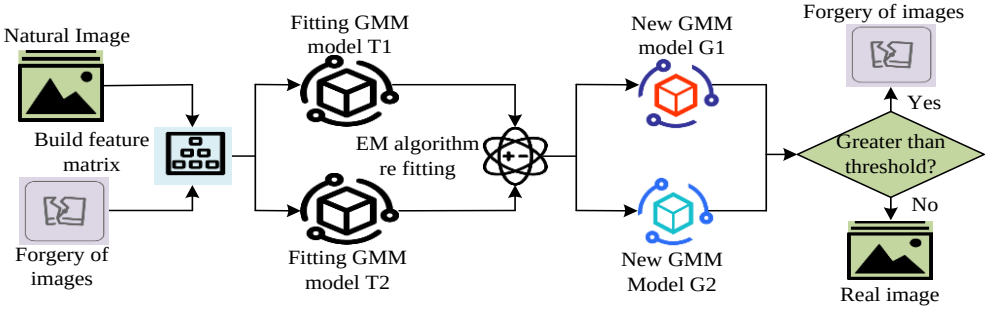


Figure 1: A similarity measurement image forgery detection algorithm based on GMM

In Figure 1, the GMM-based ICFD algorithm for similarity measurement constructs the respective feature matrices by extracting pixel values from natural and fake images, respectively, and uses these feature matrices to fit a GMM model. The GMM model that fits the feature matrix of natural images is set to T1, and the GMM model that fits fake images is set to T2. During the fitting process, the algorithm first processes the parameters a priori to optimize the performance of the model. Next, the algorithm uses the EM algorithm to re-fit each pixel value of the input test image. The parameters obtained from fitting T1 and T2 are processed and refitted to obtain new GMM models, G1 and G2. This stage aims to improve the models' ability to fit the pixel data of both real and fake images, in order to better identify forged and real images. During the refitting process, the algorithm synthesizes new GMM models. Finally, the algorithm takes a computational measure of the similarity between the two new GMM models. The algorithm can identify whether or not the test image is a forged image by evaluating its similarity to either the forged or natural image. The mathematical expression of GMM is shown in equation (1).

$$T(x)=\sum_{k=1}^{k}\pi_k N(x|\mu_k,\sum_k) \tag{1}$$

In equation (1), $T$ denotes GMM, $x$ denotes random pixel, $N(x|\mu_k,\sum_k)$ denotes the $k$ th component in the GMM model, and $\pi_k$ denotes weight. The probability density function expression of GMM is shown in equation (2).

$$P(x|\phi)=\sum_{i}^{k}a_i M_i(x|\phi_i) \tag{2}$$

In equation (2), $P$ denotes the probability density function of the GMM and $\phi$ is the set of parameters of the GMM. $a_i$ is the weight of the $i$ th parameter and $M_i$ is the $i$ th GD of the GMM. $\phi_i$ is the set of parameters of the $i$ th GD. The expression for the set of parameters corresponding to the GD in the image is shown in equation (3).

$$\{(\alpha 1,\beta 1,\delta 1),(\alpha 2,\beta 2,\delta 2),\ldots,(\alpha i,\beta i,\delta i)\} \tag{3}$$

In equation (3), $\beta$ is the covariance matrix of the GD, $\delta$ is the mean of the GD, and $\alpha$ is the weight of the GD. The calculation of the log-likelihood value using the EM algorithm is shown in equation (4).

$$InP(x|\phi)=\sum_{i=1}^{k}In\{\pi_k N(x_i|\delta_i,\beta_i)\} \tag{4}$$

In order to determine the convergence condition, the log-likelihood value is computed using equation (4). This step involves estimating the likelihood that each Gaussian component would provide the digital picture feature data. Equation (5) displays the probability produced by the $k$ th Gaussian component.

$$p(i,k)=\frac{\pi_k N(x_i|\delta_k,\beta_k)}{\sum_{i=1}^{k}\pi_i N(x_i|\delta_i,\beta_i)} \tag{5}$$

In equation (5), $p$ denotes the probability of generating a Gaussian component. The equation for GMM similarity is shown in equation (6).

$$S(T\|G)=\frac{1}{N}\sum_{i=1}^{N}\log\frac{T(x_i)}{G(x_i)} \tag{6}$$

In equation (6), $S$ denotes the similarity of the GMM, and $T$ and $G$ denote the first fitted GMM and the newly fitted GMM, respectively. Direct feature extraction from the dataset may lead to excessive feature dimensionality, which may trigger the problem of dimensionality catastrophe [18]. To solve this problem, feature extraction can be performed using GMM, while feature aggregation can be performed using local feature aggregation descriptive coding. The mathematical expression for local feature aggregation is shown in equation (7).

$$V(x_i)=\arg\min\|x_j-c_j\| \tag{7}$$

In equation (7), $V$ denotes local feature aggregation and $c_j$ denotes the $j$ th center [19]. In local feature aggregation descriptive coding, the local features of each image or video frame are aggregated into a single vector which makes the representation of that frame more concise and efficient [20]. However, when multiple classes of images are mixed together, color features may not be accurately represented, thus affecting the subsequent detection results. To solve this problem, this study innovatively combines SVM into GMM local feature aggregation description coding for color feature extraction and classification. Principal component analysis is a statistical method used for dimensionality reduction in images. Local feature aggregation and description encoding can be used to aggregate the local descriptive features in an image into a separate vector, resulting in efficient and concise image expression. The study employs principal component analysis to perform vector statistics on color features in images. First, K-means clustering is used to learn the codebook that describes the coding, thereby obtaining the color-based local feature aggregation descriptor of the image. Next, each image local descriptor is assigned to the nearest center in the codebook to obtain a quantified index. After assigning descriptors of each image to a center, the vector of the difference between the descriptors and the center can be obtained, and clustering features can be extracted based on the normalized vector. SVM is a supervised learning model that can be used for classification and

regression analysis, and in ICFD, SVM can be used to train classifiers to distinguish real images from fake ones [21]. Figure 2 shows the ICFD-SVM process based on GMM local feature aggregation description coding.

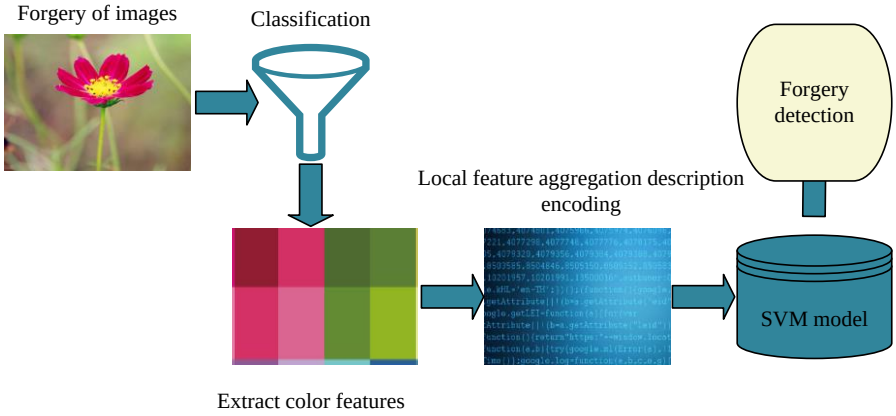



Figure 2: SVM image content forgery detection process based on GMM local feature aggregation description encoding

The two primary steps of the ICFD-SVM method based on GMM local feature aggregate description coding are feature extraction and feature classification (Figure 2). The process begins with identifying the forged image. During this process, the SVM model is trained to recognize the features that distinguish one image from another. Next, the color features are encoded using local feature aggregation description coding. This effectively aggregates the local color features in the image to form a global color description vector. In this way, each image can be represented as a unique color description vector. Finally, these coded features are used as inputs to SVM models for training. These attributes are taught to the SVM model so it can differentiate between authentic and fraudulent photos. By classifying the input features during the training phase, the model progressively gains the ability to differentiate between real and fraudulent images.

## 3.2 ICFD-SVM based on improved PSO optimization

In classification problems, SVMs can be categorized into linearly differentiable SVMs, linearly indivisible SVMs and nonlinear SVMs [22]. Among them, linearly differentiable SVM is the most commonly used type, which correctly separates samples of different classes by finding an optimal hyperplane. This optimal hyperplane is determined by the two samples closest to the separating hyperplane, which form two long bands parallel to the hyperplane. The hyperplane selection process of SVM is shown in Figure 3.

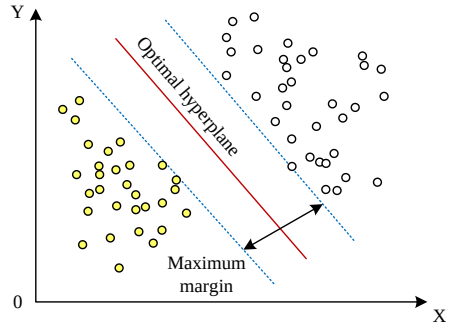



Figure 3: The process of selecting hyperplanes in SVM

In Figure 3, the solid and hollow points represent different two types of samples, the dashed line represents the separation hyperplane, while the solid line represents the two long bands consisting of the two samples closest to the separation hyperplane. In the optimization process of SVM, it is necessary to find a hyperplane that minimizes the classification error of all samples. If there exists a hyperplane that can correctly classify all the samples, the problem is said to be linearly separable; otherwise, the problem is said to be linearly indivisible. The regression function expression for SVM is shown in equation (8).

$$f(x) = \langle \omega \bullet x_i \rangle + \mathrm{b} \tag{8}$$

In equation (8), $\omega$ denotes the weight coefficients and $\mathrm{b}$ is the bias term. The minimum value of the regression function is optimized as shown in equation (9).

$$f_{\min}(x) = \min \frac{1}{2}\omega + \frac{c}{N}\sum_{i=1}^{N} L(y_i, f(x_i)) \quad (9)$$

In equation (9), $c$ denotes the penalty coefficient and $L$ denotes the insensitive loss function. The mathematical expression of the insensitive loss function is shown in equation (10).

$$L(y, f(x)) = \begin{cases} |y - f(x)|, otherwise \\ 0, |y - f(x)| \le \varepsilon \end{cases} \quad (10)$$

In equation (10), $\varepsilon$ denotes the insensitive error and the insensitive loss function satisfies the obtained constraints as shown in equation (11).

$$\begin{cases} \omega x_i + b - y_i \le \varepsilon + \xi \\ y_i - (\omega x_i + b) \le \varepsilon + \zeta \\ \xi \ge 0, \zeta \ge 0 \end{cases} \quad (11)$$

In equation (11), $\xi$ and $\zeta$ denote the relaxation variable outside the hyperplane and the relaxation variable inside the hyperplane, respectively. The mathematical expression of the linear SVM regression function is shown in equation (12).

$$y = f(x)\sum_{i=1}^{N}(\alpha^* - \alpha)(x_i \bullet x) + b \quad (12)$$

In equation (12), $\alpha, \alpha^*$ denotes the Lagrange multiplier. Nonlinear SVM can be applied to linearly indivisible datasets. Nonlinear SVM maps the data from the original space to a higher dimensional space by using a kernel function, which makes the originally linearly indivisible data linearly differentiable. The choice of kernel function affects the performance of SVM [23]. The study uses Gaussian kernel function for computation as shown in equation (13).

$$K(x_i, x_j) = \exp - \frac{x_i - x_j^{\,2}}{2g^2} \quad (13)$$

In equation (13), $K$ denotes the Gaussian kernel function and $g$ is the kernel function width of the Gaussian kernel function. The parameters selected during SVM model training have a significant effect on the model's accuracy and performance. The revised PSO algorithm can be used to optimize the SVM and determine the ideal set of parameters. The pseudocode for improving the PSO algorithm is shown in Figure 4.

```
procedure PSO
  for each particle i
    Initialize velocity Vi and position Xi
for particle i
     Evaluate particle i and set Pbesti= Xi
   end for
   Gbest=min{Pbesti}
   while not stop
      for i=1toN
         Update the velocity and position
of particle i
           Evaluate particle i
           if fit(Xi)<fit(Pbesti)
                Pbesti=Xi
           if fit(Pbesti)<fit(Gbest)
                Gbest=Pbesti
         end of
      end while
      print Gbest
End procedure
```

Figure 4: Pseudocode for improving PSO algorithm

Figure 4 shows that the improved PSO algorithm incorporates the parameters of each particle into SVM and calculates the fitness of each particle through training and cross-validation. Therefore, when using the improved PSO algorithm to optimize SVM, the penalty parameters in SVM are selected. The improvement of the inertia weights of the PSO algorithm is shown in equation (14).

$$W = W_{\max} - (W_{\max} - W_{\min}) \times \frac{a^z}{a^{z\max}} \quad (14)$$

In equation (14), $W_{\min}$ and $W_{\max}$ denote the minimum inertia weight and maximum inertia weight of the PSO algorithm, $a$ denotes a constant, and $0 < a < 1$, $z$ and $z_{\max}$ denote the current iteration number and maximum iteration number, respectively. The position update improvement of PSO algorithm using random perturbation operator is shown in equation (15).

$$x_{iD}(z+1) = r_3(P_g - h_D(z)) + h_D(z) \quad (15)$$

In equation (15), $r_3$ denotes the random number, and $h_D(z)$ denotes the position where the worst adapted particle is located at the $z$ th iteration. The enhanced PSO algorithm overcomes the limitations of the traditional PSO algorithm, which tends to be premature and prone to local optima. It offers the benefits of a simple structure, easy implementation, and fast convergence speed. Figure 5 displays the ICFD-SVM flow optimized using the enhanced PSO technique.

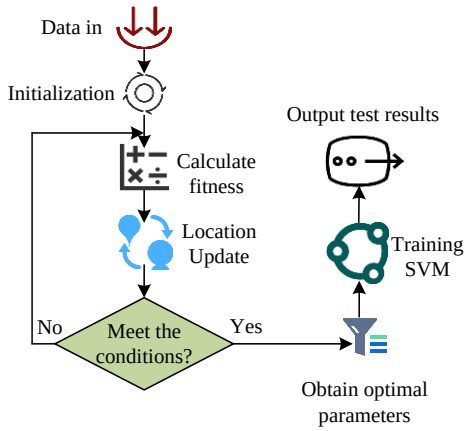



Figure 5: Optimization of SVM image content forgery detection process based on improved PSO algorithm

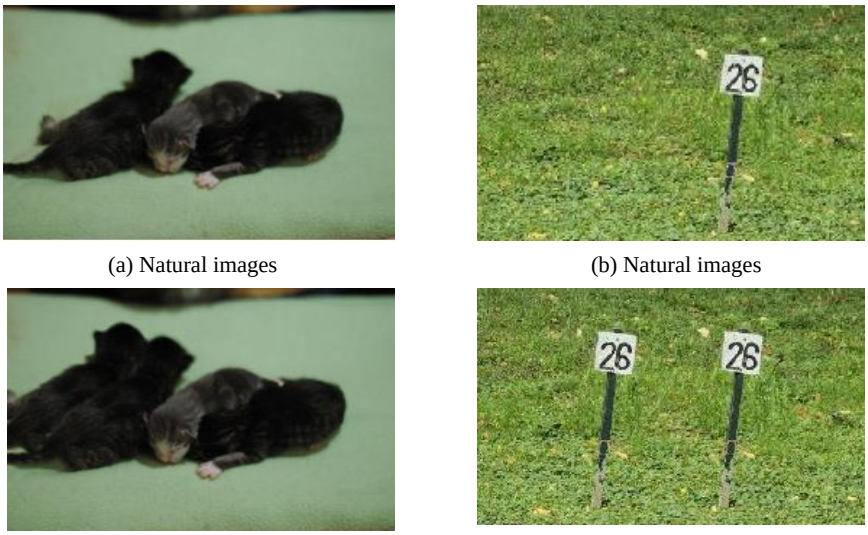
Initializing the particle swarm, including its quantity, locations, and velocities, is the first step in the ICFD-SVM process optimized using the enhanced PSO method in Figure 5. The particles' initial values can be set based on the problem domain knowledge or randomly generated. The fitness function of each particle is determined by calculating the classification accuracy of its corresponding SVM model. The velocity and position of each particle are then adjusted based on its fitness function value and the historical best position of the population. The global best position is updated for each particle whose fitness function value exceeds the current global best fitness function value. The algorithm terminates when a predetermined number of iterations or an error threshold are achieved.

# 4 ICFD-SVM model validation for improved PSO optimization for electronic data forensics

In this chapter, the specific environment of the experiment is configured, and then the various performances of the branch ICFD-SVM model optimized by the improved PSO algorithm are experimentally verified.

## 4.1 Experimental environment configuration

The datasets used for the experiments are obtained from ImageNet and COCO datasets, and the images are processed with region-copying forgeries and the processed dataset is divided into experimental training set and experimental testing set [24]. The dataset contains a total of 1400 sample images, with resolutions ranging from 320 x 240 to 800 x 600, with an average resolution of 384 x 256. The ImageNet and COCO datasets are both sourced from publicly available datasets. The ImageNet dataset is characterized by its large scale, rich diversity, and high-quality annotated images. Experiments using this dataset can verify the generalization ability of the model due to its diverse image content. The COCO dataset, on the other hand, features images with rich object detection, segmentation, and subtitle annotation. The COCO dataset's rich annotation information makes it valuable for tasks like image recognition and segmentation. Using this dataset for experiments can help verify the model's universality. The types of image forgery in the dataset include homologous stitching and heterologous stitching forgery operations. To increase the difficulty of detecting forged images and the diversity of the dataset, the study performed forgery operations such as multi-region tampering and geometric transformations on some of the images. The forged parts and contents of these images were randomly generated. To more precisely assess the model's performance, the 1400 samples in the gathered and processed dataset are split into training and test sets at a ratio of 6:4. additionally, the study assembled 500 samples from the images that are manipulated geometrically and by multi-region tampering into a validation set. The example images of the data used in the test and training sets in the experiment are shown in Figure 6.



(a) Natural images (b) Natural images

(c) Regional replication forgery of images (d) Copying and moving forged images

Figure 6: Example images of data used in the test and training sets in the experiment

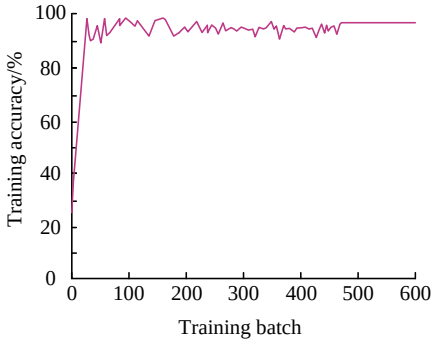
The Python 3.7 programming language is used to conduct the trials, which are carried out on the Windows 10 operating system. The study utilizes the Pytorch framework to build an experimental environment, and uses a high-performance NVIDIA TITAN BLACK GPU as the cloud host for model training. The CUDA framework is also used to perform efficient graphic calculations. At the same time, the experiment configures 64GB of memory core and 6GB of graphic memory for Windows 10 system to support large-scale data processing. The experimental environment's precise configuration is displayed below:

Table 2: Specific experimental environment configuration

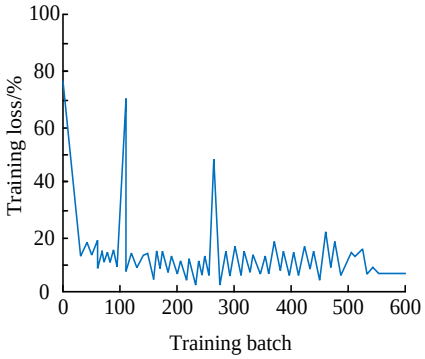
| Experimental environment | Configuration |
|---|---|
| Operating system | Windows10 |
| Memory | 64GB |
| GPU | NVIDIA TITAN BLACK GPU |
| Graphics memory | 6G |
| PyTorch framework | PyTorch 1.8.1 |
| CUDA framework | CUDA11.1 |
| Programming Language | Python 3.7 |

## 4.2 Improved PSO Optimized ICFD-SVM Model Performance Validation

The SVM model is initially trained in order to verify the performance of the enhanced PSO optimized ICFD-SVM model. The model's bach_size value is set to 32, and the initial learning rate is set to 0.001. The training accuracy and training loss of the SVM model are shown in Figure 7. In Figure 7(a), the training accuracy shows a steady increase. After 20 training batches, the training accuracy maintains a small oscillation in the range of 95% to 100%. In Figure 7(b), the training loss of the model, although it oscillates substantially in the initial phase of training, gradually stabilizes as the training progresses as the model approaches 600 batches. Thereafter, the training loss value of the model stabilized within the range of 10% without further large fluctuations. Comprehensively, it can be seen that the model has effectiveness and is suitable for ICFD. Meanwhile, the parameter values of learning rate and other parameters set in the experiment are reasonable and can be verified in subsequent experiments.

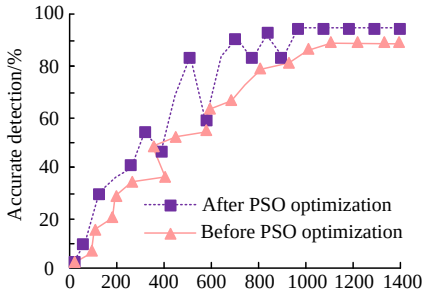



(a) The Training Accuracy of SVM Models

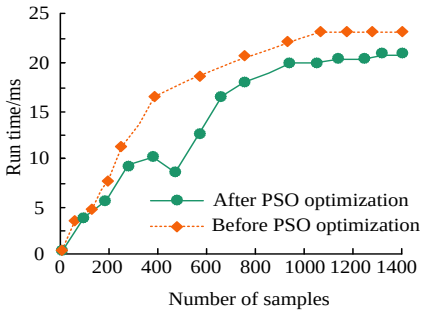



(b) Training loss of SVM model

Figure 7: The training accuracy and training loss of SVM models during the training process




(a) Comparison of detection accuracy of models before and after PSO optimization

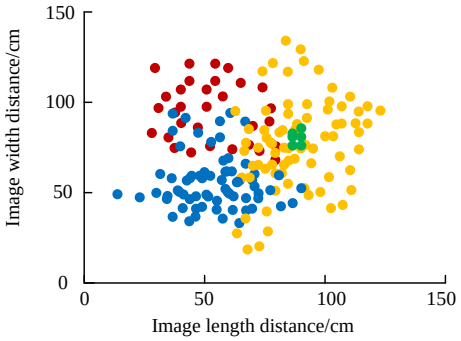



(b) Comparison of efficiency between models before and after PSO optimization

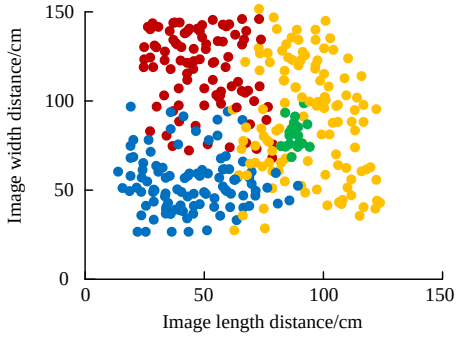
Figure 8: Comparison of detection accuracy and efficiency of models before and after PSO optimization

In Figure 8, the improved PSO-optimized ICFD-SVM model is compared with the unimproved PSO-optimized model on the dataset in terms of detection efficiency and accuracy to confirm its benefits in terms of detection performance. In Figure 8(a), when the samples is 1400, the detection accuracies of the improved PSO optimized pre- and post-optimized models at this time are 89.36% and 94.89%, respectively. The detection accuracy of the model after improved PSO optimization is improved by 5.53% compared to the pre-optimization. In Figure 8(b), when the number of samples is 1400, the detection runtime of the improved PSO pre-optimization and post-optimization models are 22.64 ms and 22.06 ms, respectively. the runtime of the improved PSO-optimized model has been reduced by 2.56% compared with the pre-optimization. Comprehensively, the ICFD-SVM model after improved PSO optimization has effectively improved the detection accuracy as well as the detection efficiency.

To verify the application of local feature aggregation description coding in the model, the ICFD-SVM model based on the local feature aggregation description coding of GMM is compared with the clustering of the ICFD-SVM model that did not use local feature aggregation description coding, as shown in Figure 9. The GMM with local feature aggregation description coding has a clearly higher number of clusters than the GMM without it. This suggests that local feature aggregation description coding effectively improves the model's ability to extract features, which in turn improves the model's performance in terms of detection.

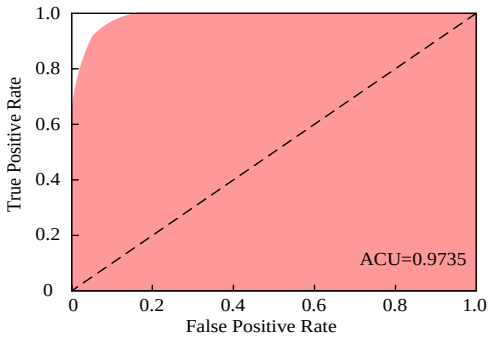



(a) Image feature clustering map based on GMM

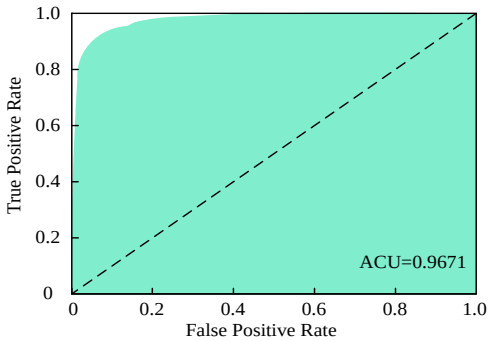



(b) Image Feature Clustering Map Based on GMM Local Feature Aggregation Description Encoding

Figure 9: Gaussian image clustering comparison chart




(a) ROC curve of image detection model on training set




(b) ROC curve of image detection model on the test set

Figure 10: ROC curve of image content forgery detection model optimized by PSO and SVM

The study compared the detection accuracy on the training and test sets, respectively, to confirm the improved PSO-optimized ICFD-SVM model's performance in terms of detection accuracy. The ROC plot of the improved PSO-optimized ICFD-SVM model is displayed in Figure 10. In Figure 10(a), the improved PSO-optimized SVM model exhibits a detection accuracy of up to 97.35% on the training set. This figure indicates that the model has excellent learning and generalization capabilities on the training dataset, and is able to accurately identify and classify both forged and real images. In Figure 10(b), the model achieved a detection accuracy of 96.71% in the test set. Taken together, the improved PSO-optimized ICFD-SVM model exhibits high detection accuracy.

To further validate the effectiveness of improving the performance of the PSO-optimized ICFD-SVM model, the study compares and validates it with the commonly used image detection models such as learning to weight (LTW) based on weighted learning, adaptive manipulation traces extraction network (AMTEN) based on adaptive operation trace extraction network, forensic transfer network (FTNet) based on forensic transfer network, and Leveraging frequency analysis (LFA) based deep pseudo image recognition detection The study compared and validated commonly used image detection models.

The terms specificity and sensitivity mathematically describe the accuracy of a test in reporting the presence or absence of conditions, where those that meet the conditions are considered "positive" and those that do not meet the conditions are considered "negative". Sensitivity, also known as true positive rate, refers to the condition under which the detection result is "positive", while specificity, also known as true negative rate, refers to the condition under which the detection result is "negative". Therefore, using specificity and sensitivity, the performance of algorithms to determine whether an image has undergone regional replication and forgery can be evaluated. Domain wide face forgery detection based on weighted learning. The specificity and sensitivity comparison results of different ICFD models are shown in Table 3. In the training set, the model achieved a maximum value of 96.54% for specificity, which is an improvement of 15.9%, 16.90%, 23.38%, and 23.90% compared to the LTW, AMTEN, FTNet, and LFA models, respectively. And in the test set, the sensitivity of the model achieved a maximum value of 95.14%, which is improved by 3.10%, 5.53%, 4.46% and 3.45% compared with the LTW, AMTEN, FTNet and LFA models, respectively. Taken together, the improved PSO-optimized ICFD-SVM model shows a superior performance when comparing with other detection models.

Table 3: Comparison of specificity and sensitivity of different image content forgery detection models

| Model | Training set | | Test set | |
|---|---|---|---|---|
| | Specificity/% | Sensitiveness/% | Specificity/% | Sensitiveness/% |
| LTW | 80.64 | 91.54 | 79.16 | 92.04 |
| AMTEN | 79.64 | 88.98 | 78.15 | 89.61 |
| FTNet | 73.16 | 91.51 | 73.57 | 90.68 |
| LFA | 72.64 | 81.14 | 70.61 | 91.69 |
| PSO-SVM | 96.54 | 95.10 | 96.08 | 95.14 |

To conduct a more comprehensive study of the model, a benchmark test analysis of existing models will be conducted. This model will be compared and analyzed with other advanced modeling methods such as LTW, AMTEN, FTNet, and LFA on public datasets. As illustrated in Figure 11, the detection accuracy of the improved PSO-optimized ICFD-SVM model is compared with that of the LTW, AMTEN, FTNet, and LFA models in the validation set in order to more intuitively evaluate the detection performance of this model. From Figure 11, the dots represent outliers and the crosses represent the mean. The confidence interval of the improved PSO-SVM model is (96.12 $\pm$ 2.13), while the confidence intervals of LTW, AMTEN, FTNet, and LFA models are (78.10 $\pm$ 2.59), (77.83 $\pm$ 1.36), (71.51 $\pm$ 0.98), and (76.07 $\pm$ 11.09), respectively. It can be seen that the improved PSO-SVM model has the highest detection accuracy of 98.15%. In comparison, LTW, AMTEN The highest detection accuracy values of FTNet and LFA models are 80.69%, 79.19%, 72.49%, and 87.16%, respectively. Therefore, the improved PSO-SVM model has improved detection accuracy by 17.46%, 18.96%, 25.66%, and 10.99%, respectively. These data clearly demonstrate the superiority of the improved PSO-SVM model, further confirming its excellent performance in ICFD tasks. In summary, the PSO-SVM model addresses the limitations of traditional models that are prone to premature convergence and falling into local extremes. This demonstrates the potential of the PSO-SVM model in detecting image content forgery.

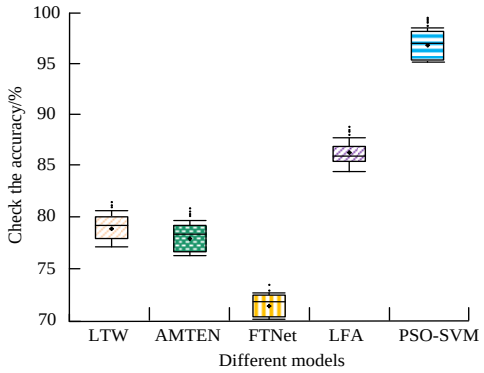



Figure 11: Comparison of detection accuracy of different model

Experiments are carried out on the validation set to identify the localization of the model with various forgery techniques in order to validate the performance of the enhanced PSO-optimized ICFD-SVM model in practical applications. The results of image forgery region localization detection are shown in Table 4. The model's localization accuracy exceeds 92% on different forgery methods. On the image scale transformation forgery content, the model's detection and localization precision achieves the highest value of 94.06%, on the image splicing forgery method, the model's recall achieves the highest value of 92.68%, and on the forgery method of adding noise interference, the model's F1 value achieves the highest value of 96.34%. Comprehensively, in practical validation, the model has high localization performance for images forged by different forgery methods.

Table 4: Image forgery area localization detection results

| Forgery methods | Precision/% | Recall% | F1 value% |
|---|---|---|---|
| Multi region tampering | 93.16 | 90.36 | 95.61 |
| Transform | 92.15 | 91.64 | 96.18 |
| Mosaics | 92.94 | 92.68 | 95.91 |
| Image scale transformation | 94.06 | 90.67 | 96.15 |
| Add noise interference | 93.39 | 89.19 | 96.34 |
| Sharpening | 92.06 | 90.91 | 95.09 |

# 5 Discussion

The development of information technology has made image data a crucial tool for information dissemination. However, the rise of artificial intelligence technology has also led to an increase in image forgery, which has had a significant impact. To accurately identify forged images, PSO-SVM was proposed for image forgery recognition. The results indicated that the optimized model achieves a detection accuracy of 94.89% when the sample size reaches 1400, which is 5.53% higher than the pre-optimized model. This improvement was significant compared to similar models in other literature. For instance, Arunkumar P M's research team's fuzzy Fisher face model detection method achieved an accuracy of 89.32% in the dataset [12]. Styawati S's research team achieved the highest accuracy of 89% in sentiment classification using an SVM-based model [13]. The model in this study is more accurate than the above methods. Additionally, the research successfully reduced the computational complexity of the model and improved detection speed by optimizing the algorithm and model structure. For a sample size of 1400, the post-optimized model's detection running time decreased by 2.56% compared to the pre-optimized model. The method's improvement enhances the model's ability to meet real-time and efficiency requirements in practical applications. Additionally, the study successfully optimized the parameters of the SVM model by improving the PSO algorithm, resulting in improved detection accuracy. The study aimed to verify the model's generalization ability and universality by conducting research on different datasets. To ensure stability and reliability, representative public datasets were selected and sufficient preprocessing and feature extraction work was conducted. This allowed the model to better learn the inherent patterns and features of the data, resulting in improved detection performance. In summary, the study proposes the PSO-SVM model, which has not only achieved significant improvement in detection accuracy after optimizing the PSO algorithm but also demonstrated unique advantages in methods, dataset usage, and computational efficiency. These advantages make the model a valuable contribution to related fields with broad application prospects.

# 6 Conclusion

ICFD plays a critical role in the EDF industry. To enhance its accuracy, this study incorporates SVM with GMM local feature aggregation description coding based on the GMM model and optimizes the parameters of the SVM model using the improved PSO algorithm. When the number of samples reached 1400, the model optimized by the improved PSO was found to improve detection accuracy by 5.53% compared to the pre-optimized version, with a resultant detection accuracy of 94.89%. Additionally, the running time was observed to decrease slightly by 2.56% post-optimization. In the training set and test set, the model demonstrated detection accuracy of 97.35% and 96.71%, respectively. Moreover, the model attained a maximum specificity of 96.54% in the training set, surpassing the specificity of the LTW, AMTEN, FTNet, and LFA models by 15.9%, 16.90%, 23.38%, and 23.90%, respectively. In the test set, this model achieved a maximum sensitivity value of 95.14%. This was higher by 3.10%, 5.53%, 4.46%, and 3.45% compared to the LTW, AMTEN, FTNet, and LFA models, correspondingly. In addition, the model achieved the highest precision for detection and localization of 94.06% for image scale transformation forgery, the highest recall value of 92.68% for image splicing forgery, and the highest F1 value of 96.34% for the forgery method with added noise interference. In summary, the results suggest that the combination of PSO with the ICFD-SVM model in EDF enhances the detection accuracy of forged images. However, the study was solely validated experimentally against six image forgery methods, and further improvements regarding comprehensive experimental results are necessary.

# Acknowledgements

The research is supported by 2020 Education Research Project of Young and middle-aged Teachers of Fujian Provincial Department of Education "Research on Public Security Intelligence Analysis Technology Based on Data Mining" (JAT200384).

# References


[1] S. Walia, and K. Kumar, "Digital image forgery detection: a systematic scrutiny," Australian Journal of Forensic Sciences, vol. 51, no. 5, pp. 488-526, 2019. https://doi.org/10.1080/00450618.2018.1424241

[2] D. C. Toledo-Pérez, J. Rodríguez-Reséndiz, R. A. Gómez-Loenzo, and J. C. Jauregui-Correa, "Support vector machine-based EMG signal classification techniques: A review," Applied Sciences, vol. 9, no. 20, pp. 4402-4405, 2019. https://doi.org/10.3390/app9204402

[3] L. Liao, Y. Lei, and C. Xu, "Research on the legal effect of electronic evidence under the background of digital intelligence empowerment," Journal of Heilongjiang University of Technology (Comprehensive Edition), vol. 23, no. 09, pp. 59-63, 2023. https://doi.org/10.16792/j.cnki.1672-6758.2023.09.005

[4] D. J. S. Raj, and J. V. Ananthi, "Recurrent neural networks and nonlinear prediction in support vector machines," Journal of Soft Computing Paradigm, vol. 1, no. 1, pp. 33-40, 2019. https://doi.org/10.36548/jscp.2019.1.004

[5] V. Singh, R. C. Poonia, S. Kumar, P. Dass, P. Agarwal, V. Bhatnagar, and L. Raja, "Prediction of COVID-19 corona virus pandemic based on time series data using support vector machine," Journal of Discrete Mathematical Sciences and Cryptography, vol. 23, no. 8, pp. 1583-1597, 2020. https://doi.org/10.1080/09720529.2020.1784535

[6] A. Altan, and S. Karasu, "The effect of kernel values in support vector machine to forecasting performance of financial time series," The Journal of Cognitive Systems, vol. 4, no. 1, pp. 17-21, 2019.

[7] X. Ding, J. Liu, F. Yang, and J. Cao, "Random radial basis function kernel-based support vector machine," Journal of the Franklin Institute, vol. 358, no. 18, pp. 10121-10140, 2021. https://doi.org/10.1016/j.jfranklin.2021.10.005

[8] Z. Li, D. Zhang, J. Liu, J. Zhang, L. Shao, X. Wang, and W. Zhu, "Polarization-assisted visual secret sharing encryption in metasurface hologram," Advanced Laser Photonics Research, vol. 2, no. 11, pp. 2100175, 2021. https://doi.org/10.1002/adpr.202100175

[9] Z. Li, X. Kong, J. Zhang, L. Shao, D. Zhang, J. Liu, and C. W. Qiu," Cryptography metasurface for one-time-pad encryption and massive data storage," Laser Photonics Research, vol. 16, no. 8, pp. 2200113, 2022. https://doi.org/10.1002/lpor.202200113

[10] S. Chen, T. Yao, Y. Chen, S. Ding, J. Li, and R. Ji, "Local relation learning for face forgery detection," Proceedings of the AAAI Conference on Artificial Intelligence, vol. 35, no. 2, pp. 1081-1088, 2021. https://doi.org/10.1609/aaai.v35i2.16193

[11] M. Baskar, R. Renuka Devi, J. Ramkumar, P. Kalyanasundaram, M. Suchithra, and B. Amutha, "Region centric minutiae propagation measure orient forgery detection with finger print analysis in health care systems," Neural Processing Letters, vol. 55, no. 1, pp. 19-31, 2023. https://doi.org/10.1007/s11063-022-10888-5

[12] P. M. Arunkumar, Y. Sangeetha, P. V. Raja, and S. N. Sangeetha, "Deep learning for forgery face detection using fuzzy fisher capsule dual graph," Information Technology and Control, vol. 51, no. 3, pp. 563-574, 2022. https://doi.org/10.5755/j01.itc.51.3.31510

[13] S. Styawati, and K. Mustofa, "A support vector machine-firefly algorithm for movie opinion data classification," IJCCS (Indonesian Journal of Computing and Cybernetics Systems), vol. 13, no. 3, pp. 219-230, 2019. https://doi.org/10.22146/ijccs.41302

[14] S. Muthukrishnan, H. Krishnaswamy, S. Thanikodi, D. Sundaresan, and V. Venkatraman, "Support vector machine for modelling and simulation of heat exchangers," Thermal Science, vol. 24, no. 1, pp. 499-503, 2020. https://doi.org/10.2298/TSCI190419398M

[15] A. A. Aldino, A. Saputra, A. Nurkholis, and S. Setiawansyah, "Application of support vector machine (SVM) algorithm in classification of low-cape communities in lampung timur," Building of Informatics, Technology and Science, vol. 3, no. 3, pp. 325-330, 2021. https://doi.org/10.47065/bits.v3i3.1041

[16] A. H. Saber, M. A. Khan, and B. G. Mejbel, "A survey on image forgery detection using different forensic approaches," Advances in Science, Technology and Engineering Systems Journal, vol. 5, no. 3, pp. 361-370, 2020. https://doi.org/10.25046/aj050347

[17] S. alZahir, and R. Hammad, "Image forgery detection using image similarity," Multimedia Tools and Applications, vol. 79, no. 39-40, pp. 28643-28659, 2020. https://doi.org/10.1007/s11042-020-09502-4

[18] C. Deep Kaur, and N. Kanwal, "An analysis of image forgery detection techniques," Statistics, Optimization & Information Computing, vol. 7, no. 2, pp. 486-500, 2019. https://doi.org/10.19139/soic.v7i2.542

[19] S. S. Ali, I. I. Ganapathi, N. S. Vu, S. D. Ali, N. Saxena, and N. Werghi, "Image forgery detection using deep learning by recompressing images," Electronics, vol. 11, no.3, pp. 403-408, 2022. https://doi.org/10.3390/electronics11030403

[20] E. U. H. Qazi, T. Zia, and A. Almorjan, "Deep learning-based digital image forgery detection system," Applied Sciences, vol. 12, no. 6, pp.

2851-2857, 2022. https://doi.org/10.3390/app12062851

[21] V. Singh, R. C. Poonia, S. Kumar, P. Dass, P. Agarwal, V. Bhatnagar, and L. Raja, "Prediction of COVID-19 corona virus pandemic based on time series data using support vector machine," Journal of Discrete Mathematical Sciences and Cryptography, vol. 23, no. 8, pp. 1583-1597, 2020. https://doi.org/10.1080/09720529.2020.1784535

[22] Q. Guo, Z. Wang, "A Deep Reinforcement Learning Model-based Optimization Method for Graphic Design," Informatica, vol. 48, no. 5, pp. 1343-1366, 2024. https://doi.org/10.31449/inf.v48i5.5295

[23] M. Cui, Y. Wang, X. Lin, and M. Zhong, "Fault diagnosis of rolling bearings based on an improved stack autoencoder and support vector machine," IEEE Sensors Journal, vol. 21, no. 4, pp. 4927-4937, 2020. https://doi.org/10.1109/JSEN.2020.3030910

[24] F. Kromp, E. Bozsaky, F. Rifatbegovic, L. Fischer, M. Ambros, M. Berneder, and S. Taschner-Mandl, "An annotated fluorescence image dataset for training nuclear segmentation methods," Scientific Data, vol. 7, no. 1, pp. 262, 2020. https://doi.org/10.1038/s41597-020-00608-w