JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

IMAGE FORGERY DETECTION AND CLASSIFICATION USING SUPPORT VECTOR MACHINE

Aman, IEC College of Engineering & Technology, Greater Noida, India

Dr. Manoj Kumar Garg ,Electronics & Communication Department, IEC College of Engineering & Technology, Greater Noida, India

Abstract: Nowadays in digital publishing, image forgery is the main issue and the system can be utilized for the purpose of forensic for the image authenticity validation. Image forgery authentication approach is presented in this paper. When any forgery or morphing is applied, homogeneity is lost from the image. In this paper, a proposed technique is presented utilizing the scale-invariant feature transform (SIFT) and support vector machine (SVM). Earlier, SVM failed in many cases for forged picture detection. Single extraction algorithm is not capable. So to overcome the drawbacks, image datasets are first fed to SIFT for feature extraction and the SVM is applied. The accuracy values are obtained by the proposed techniques for different images sets having different number of images. The obtained results by the proposed technique are also compared with the existing techniques. Accuracy obtained by the prosed technique is 91.46%.

Keywords: Image forgery; Scale-invariant Feature Transform; Support Vector Machine; Accuracy

1. Introduction

With the digital image processing platforms availability, it is easy for digital forgeries creation from different images. Due to the image processing software and computer technology development, it is easy to perform digital image forgery [1, 2]. The digital images are reliable and popular information source. In the existing image tampering, digital image manipulations are cutpaste and copy-move forgeries in which image's one or several copied region are pasted on the other part of the same image. During the operation of copy and move, image processing techniques like "rotation, scaling, blurring, compression, and noise addition" are used for forgeries convincing. Because the image parts are copied and moved from the same image, the color and other important properties are compatible with the image [3].

For detection of copy-move forgery, many forging techniques are presented in previous years. There are two main categories of the copy-move forgery detection methods such as block based and feature key point based algorithms [4]. The previous method of block based forgery detection, the input image is divided into overlapping and the image pixel blocks the matching blocks obtains the tampered regions [5, 6]. The image forging technique uses the algorithm for image detection and tracing without any information and security codes. The slicing details forged the images which is called "copymove images". The image copied regions can be post-processed and scaled for the copymove images before pasting to other places for the detail removal. The two images of standard monalisa are presented in Fig 1.

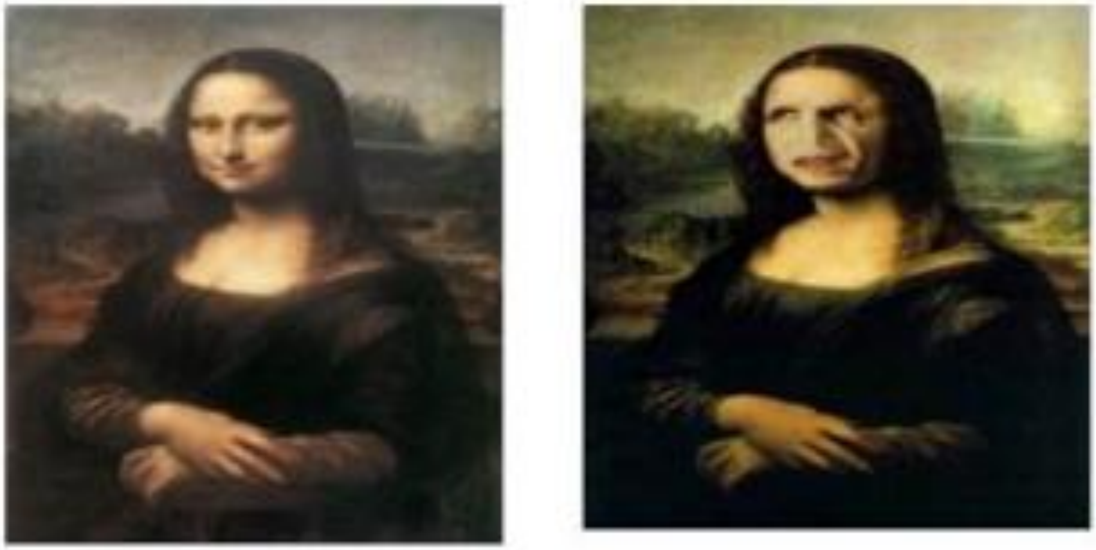


Fig 1: (a) Original Image, (b) Composite Image

The Fig 1 (b) is easily deduced by the one as a fake. With the computer graphics technology advancement, digital image manipulation is easy and impossible for authentic photographic image differentiation. Fig 1 (a) is the original image and the Fig 1(b) is the composite image. Image forgery process is the public perception alteration, modification and the image reproduction. With the advancement in the software's processing of digital images, image manipulation and modifications are easy. Active and passive techniques are the two main categories of the image forgery detection techniques [7]. The image pre-processing is required by the digital image in the active technique. Passive techniques of the image forging are statistical and image content. The basic four types of the image forging are shown in Fig 2.

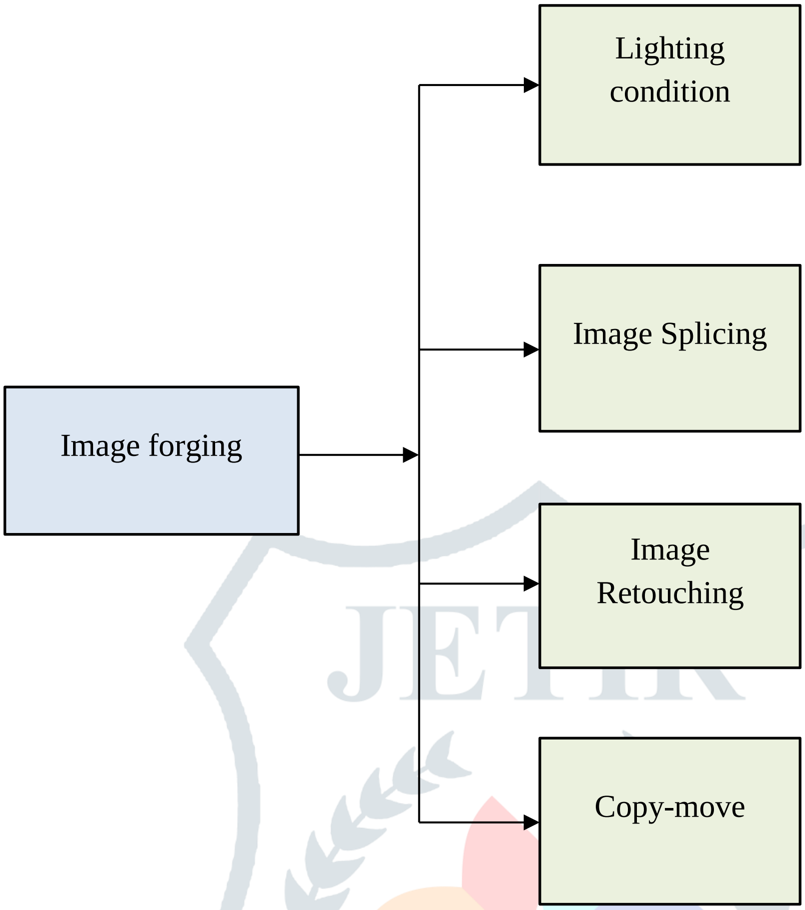


Fig 2: Types of Image Forgery

2. Literature Review

Author developed a method for image forgery detection including object removal, and replacement. SVM classifier is utilized having similar functional form to NN [8]. Features of image are extracted and analyzed and calculated the hash values. Two phases that are training and testing phases are consisted in the process. Large dataset of images is used for training of SVM classifier. Image classification is done by SVM classifiers as genuine or forged. Nowadays, image forgery is a main issue in digital publishing. System can be used for forensic purpose for the image authenticity purpose. "Image forgery authentication" is presented by the author in this paper [9]. In non-spectral domain, homogeneity is shown by the non-morphed and non-forged image. The DCT statistics and LBP features are combined with "curve-let statistics and Gabor transform" for image representation in transform domain. Hidden Markov model is trained by the transformed images and probabilistic state information is extracted from statistical model. The system accuracy is shown by the results is around 89% for the test instances. The face recognition and parameters effecting structure and shape information is detailed in this paper [10]. In pattern recognition, the face recognition is the difficult field however constancy with new difficulties is attained in this field. Age and the real image feature vectors are generating by the user for synthesized feature vectors creation. The facial image is shown by the texture vector and structure. The HOG meta-fusion technique and Sasi elements classifier is used for the imaging forgery detection. In this paper, photographic manipulation image composition or splicing is analyzed [11]. The subtle inconsistencies are exploited by utilizing the forgery detection. Machine Learning technique is utilized for two or more people images. The input of extracted texture, skin pigmentation- and edge-based features are provided for ML technique for decision making. The SVM meta-fusion classifier achieves the classification performance. Author presented Splicing and Copy-move forgery detection approach in this paper. The forgery detection techniques Copy-move and Splicing are utilizing in this paper [12]. The image is fed to the copy-move and splicing forgery. The pre-processing and the threshold methods are utilized for splicing and copy move and extracted image features. The SVM is utilized after feature extraction by using RBF. When the forged id identified by the SVM then PCA algorithm is utilizing, the authentic region is removed. Author details that the digital images are the information sources under pandemic situation that can be visualized in social media [13]. Nowadays, image forging utilizing the image editing software and image forgery detection is essential. Author in this paper presented the "Discrete-Time Cosine Wavelet and Spatial (DTCWS) Markov feature-based algorithm" for forgery detection. The Markov features in DTCWS domain extracted the Markov features and reduce the Markov features dimensionality with "Principal Component Analysis". An optimized ensemble classifier is utilized for the classification and then evaluates the results. The 99.9% accuracy is achieved by the presented technique and also consumed less time.

3. Proposed Methodology

The proposed technique utilizing different techniques for forgery image detection is presented. Dataset utilized for the evaluation of proposed technique is also detailed in this section. First of all, preprocessing of the technique is done to remove the noise from the image and to improve the image quality for enhancing the image features for the post processing. After that the SIFT based feature extraction technique is employed in the presented technique. The SVM classifier is then utilized for the forgery image detection and classification. The proposed technique flowchart is presented in Fig 3.

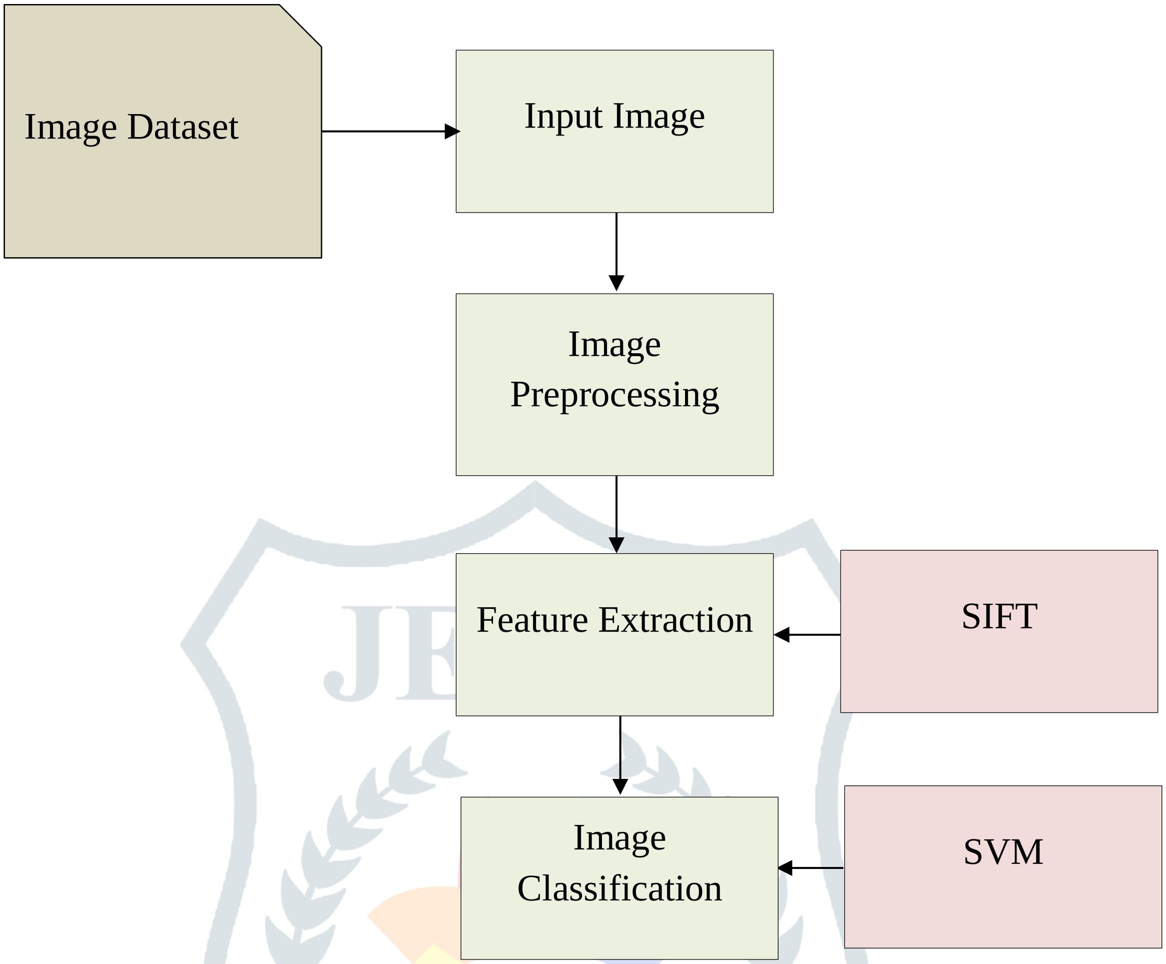


Fig 3: Flowchart of the proposed image forgery technique

A. Database

A database is generated and trained with a number of images in the training phase. The images of extension jpg and jpeg can be either downloaded from the Internet or captured utilizing digital cameras having different image sizes, resolutions and bit depths. MICC F-220 is also utilized in this work.

B. Pre-processing

First of all the input images are converted into grayscale from the RGB scale. Image noises present in the images are removed by utilizing the filter. After filtering, image enhancement techniques are then applied. Preprocessing includes the contrast manipulation, edge crispening, sharpening, magnification, colouring and so on. Overall the preprocessing is done improve the quality of image processing.

C. Feature extraction

The features are extracted from the images. Basic block diagram of feature extraction is shown in Fig 4.

1) Image analysis: In the image analysis, MATLAB operator is utilized for the image edges analysis.

2) Analysis of pixel values: The image mean and standard deviation are calculated.

Mean gray value is the average gray value within the selection and the sum of the gray values of all the pixels divided by the pixels numbers. Gray value standard deviation is utilized for mean gray value generation.

3) Texture analysis

The texture boundaries can be finding by utilizing the texture analysis. The regions characterization is referred by the texture analysis by the content of texture. An image texture is characterized by the GLCM functions by calculating the pixel pairs with values and the image spatial characteristics.

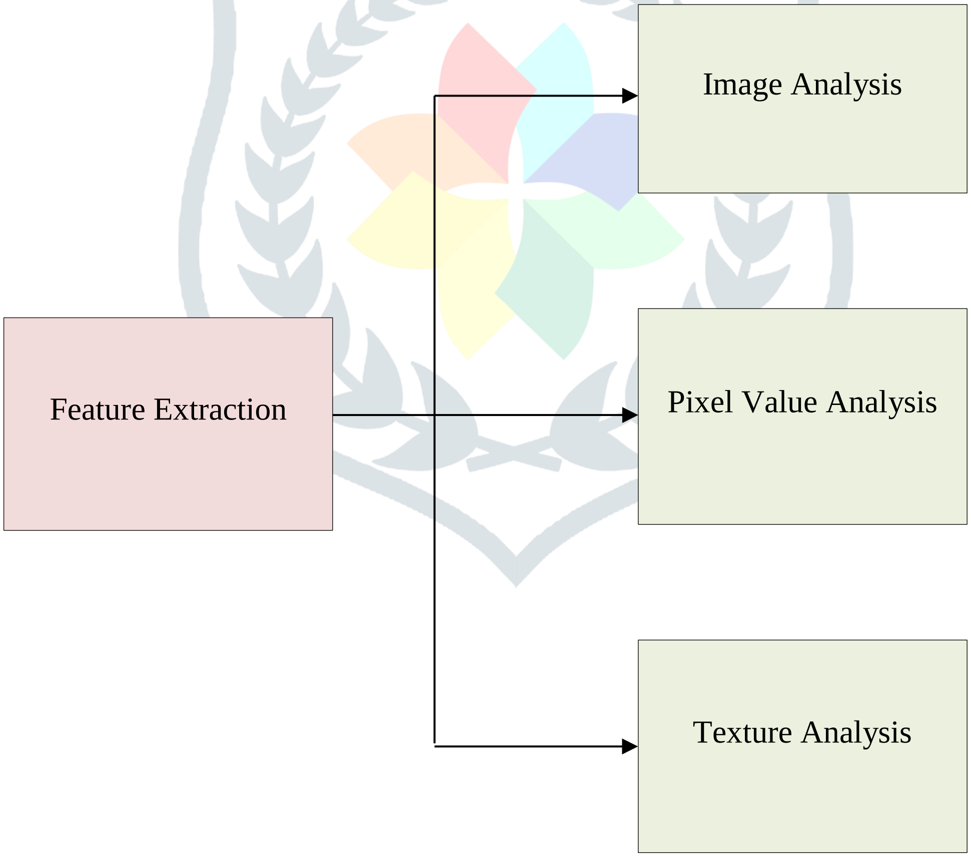


Fig 4: Image feature extraction basic block diagram

D. SIFT Based Feature extraction

The SIFT is invariant for image scaling and rotation. In SIFT, features are local and robust for cluttering. It is distinctiveness as the individual features can be matched to the object database. It is very efficient and very effective for real time performance. It can be extended to various types of features with robustness.

E. Support Vector Machine (SVM) Classifier

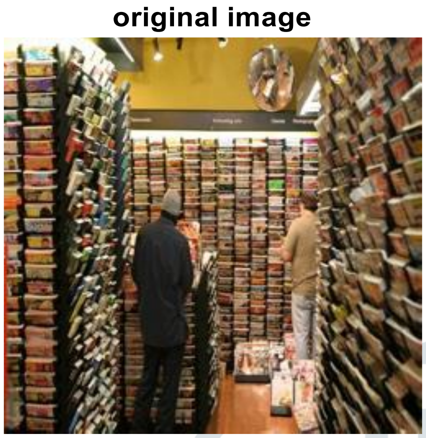
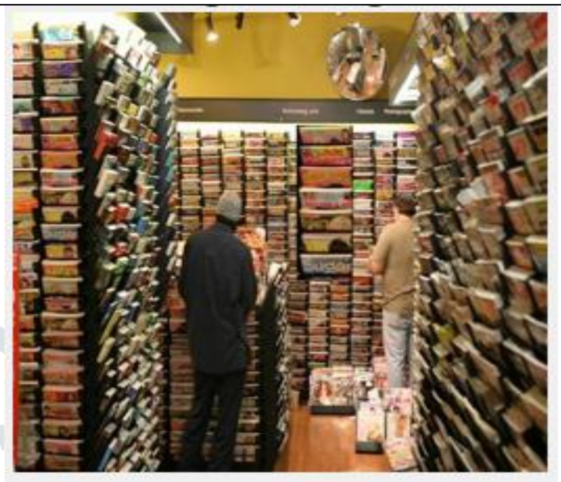
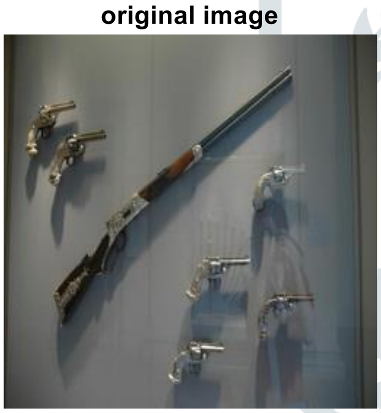
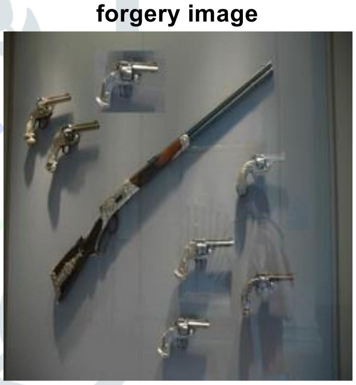
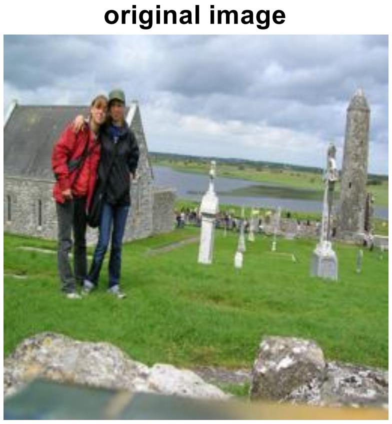
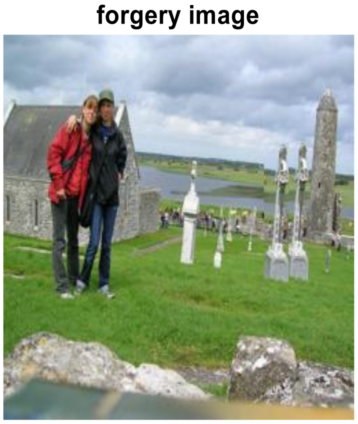
The image is splitted by SVM into two classes and a hyper-plane is getting which is the best classifier. The unsupervised method doesn't required training data for pixel grouping with homogeneous attributes. By utilizing the intensity, texture image based features, the algorithm automatically decides the number of classes. Clustering, hybrid techniques are included in the unsupervised methods. Some techniques are combined together to provide the detection results.

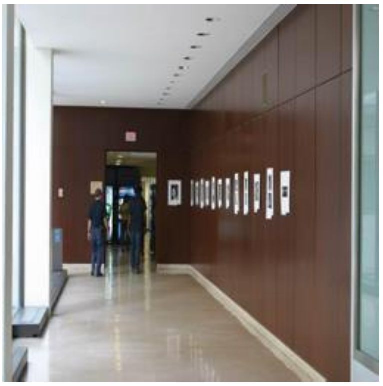
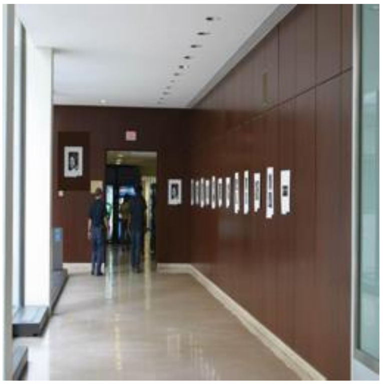
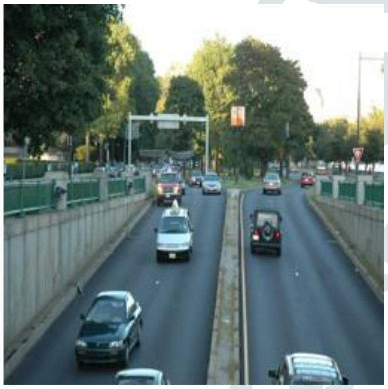
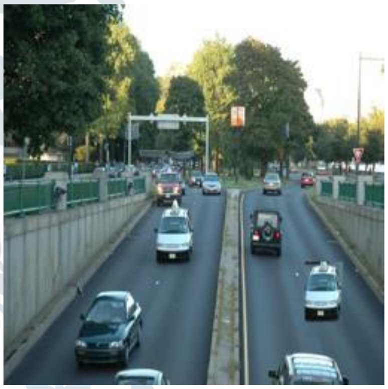
4. Results and Discussion

4.1 Presented technique analysis

In this section, results obtained by the proposed technique are detailed and discussed. Table 1 represents the original and the obtained forgery images by the proposed technique. The quality of the obtained forgery images is high and they are visually same as that of original images for all the image dataset.

Table 1: Represents the original and the obtained forgery images

Original images	**Forgery images**
	
	
	

original image 	forgery image 
original image 	forgery image 

4.2 Performance parameters Evaluation

Accuracy of the proposed technique is obtained for the large dataset of images and compared with the existing techniques. The obtained value and the comparative analysis are shown in Table 2. Comparative analysis is done with the DWT+SOM, DWT+SVM with linear kernel and DWT+PCA+KSVM (LIN). Highest accuracy value is obtained by the presented technique that is 91.46%. Accuracy values obtained by the DWT+SOM, DWT+SVM with linear kernel and DWT+PCA+KSVM (LIN) are 60%, 87% and 89% respectively.

Table 2: Comparative analysis of the classification accuracy

Approach from literatures	Passive systems
DWT+SOM	60%
DWT+SVM with linear kernel	87%
DWT+PCA+KSVM (LIN)	89%
Proposed Method	**91.46%**

Accuracy value is depending upon the number of image datasets. Accuracy values obtained by the proposed technique are also calculated for different sets of images. The accuracy values for different image datasets are tabulated in Table 3.

Table 3: Classification of accuracy on number of images

Number of images	Passive systems
500	92%
450	91.4%
400	90.5%
350	90%

Higher the number of images, higher will be the accuracy. The accuracy value of the image datasets having 500 images, 450 images, 400 images and 350 images are 92%, 91.4%, 90.5% and 90% respectively.

5. Conclusion

An effective image forgery detection technique is presented in this paper utilizing SIFT and SVM methods. Features are extracted from the image by using SIFT after performing the image preprocessing. After preprocessing and feature extraction, SVM classifier is used for the forgery image classification. The performance of the proposed technique is evaluated and accuracy value is obtained. The resulted accuracy of the proposed technique is also compared with the other techniques. After comparative analysis, it is obtained that the proposed technique gives higher accuracy as compared to other existing technique.

References

[1] Mehta, R., Aggarwal, K., Koundal, D., Alhudhaif, A., & Polat, K. (2021). Markov features based DTCWS algorithm for online image forgery detection using ensemble classifier in the pandemic. *Expert Systems with Applications*, *185*, 115630.

[2] Soni, R., & Amhia, H. (2021). A Review Article Enhancement of Image Forgery and Improvement of Image Parameters Using DWT Algorithm.

[3] Jaramillo, R. (2018). *A multi-agent control approach for optimization of central cooling plants* (Doctoral dissertation, Purdue University).

[4] Su, Q., & Chen, B. (2018). Robust color image watermarking technique in the spatial domain. *Soft Computing*, *22*(1), 91-106.

[5] Lee, J. C., Chang, C. P., & Chen, W. K. (2015). Detection of copy–move image forgery using histogram of orientated gradients. *Information Sciences*, *321*, 250-262.

[6] Yao, H., Wang, S., Zhao, Y., & Zhang, X. (2011). Detecting image forgery using perspective constraints. *IEEE Signal Processing Letters*, *19*(3), 123-126.

[7] Ooi, S. Y., Teoh, A. B. J., Pang, Y. H., & Hiew, B. Y. (2016). Image-based handwritten signature verification using hybrid methods of discrete radon transform, principal component analysis and probabilistic neural network. *Applied Soft Computing*, *40*, 274-282.

[8] Reshma, P. D., & Arunvinodh, C. (2015, March). Image forgery detection using SVM classifier. In *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)* (pp. 1-5). IEEE.

[9] Jain, N. K., Rathore, N. K., & Mishra, A. (2018). An efficient image forgery detection using biorthogonal wavelet transform and improved relevance vector machine. *Wireless Personal Communications*, *101*(4), 1983-2008.

[10] Bansal, D., & Kaushal, S. A novel Analysis of Image Forgery Detection Using SVM. *International Journal of Engineering and Applied Sciences*, *3*(12), 257542.

[11] Jothilakshmi, S. L., & Ranjith, V. G. (2017). Automatic Machine Learning Forgery Detection Based On SVM Classifier. *International Journal of Computer Science and Information Technologies*, 3384-3388.

[12] Farquad, M. A. H., & Bose, I. (2012). Preprocessing unbalanced data using support vector machine. *Decision Support Systems*, *53*(1), 226-233.

[13] Mehta, R., Aggarwal, K., Koundal, D., Alhudhaif, A., & Polat, K. (2021). Markov features based DTCWS algorithm for online image forgery detection using ensemble classifier in the pandemic. *Expert Systems with Applications*, *185*, 115630.