Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.040512

ARTICLE

Enhanced Steganalysis for Color Images Using Curvelet Features and Support Vector Machine

Arslan Akram[1,2], Imran Khan[1], Javed Rashid[2,3], Mubbashar Saddique[4,*], Muhammad Idrees[4], Yazeed Yasin Ghadi[5] and Abdulmohsen Algarni[6]

[1]Faculty of Computer Science and Information Technology, Department of Computer Science, Superior University, Lahore, 54000, Pakistan

[2]Machine Learning Code (MLC) Lab, Meharban House, House Number 209, Zafar Colony, Okara, 56300, Pakistan

[3]Information Technology Services, University of Okara, Okara, 56310, Pakistan

[4]Department of Computer Science & Engineering, University of Engineering & Technology Lahore, Narowal Campus, Narowal, 51601, Pakistan

[5]Department of Computer Science and Software Engineering, Al Ain University, Al Ain, 11671, Abu Dhabi

[6]Department of Computer Science, King Khalid University, Abha, 61421, Saudi Arabia

*Corresponding Author: Mubbashar Saddique. Email: dr.mubbashar@uet.edu.pk

Received: 21 March 2023 Accepted: 06 December 2023 Published: 30 January 2024

ABSTRACT

Algorithms for steganography are methods of hiding data transfers in media files. Several machine learning architectures have been presented recently to improve stego image identification performance by using spatial information, and these methods have made it feasible to handle a wide range of problems associated with image analysis. Images with little information or low payload are used by information embedding methods, but the goal of all contemporary research is to employ high-payload images for classification. To address the need for both low- and high-payload images, this work provides a machine-learning approach to steganography image classification that uses Curvelet transformation to efficiently extract characteristics from both type of images. Support Vector Machine (SVM), a commonplace classification technique, has been employed to determine whether the image is a stego or cover. The Wavelet Obtained Weights (WOW), Spatial Universal Wavelet Relative Distortion (S-UNIWARD), Highly Undetectable Steganography (HUGO), and Minimizing the Power of Optimal Detector (MiPOD) steganography techniques are used in a variety of experimental scenarios to evaluate the performance of the proposed method. Using WOW at several payloads, the proposed approach proves its classification accuracy of 98.60%. It exhibits its superiority over SOTA methods.

KEYWORDS

Curvelets; fast fourier transformation; support vector machine; high pass filters; steganography

1 Introduction

Steganography algorithms are methods for hiding communications in digital material to be invisible at first glance [1]. The messages are even made to fit the text of the files so that they do not stand out. Image manipulation is the most common type of digital media. It is used for

many things, like sending legal and safe data, illegal or radical reasons, and outbreaks on Instagram and other cloud-based platforms [2]. In light of this, legitimate bodies must be able to determine whether image files have been altered to communicate secret information. Potential benefits of the suggested method for identifying steganography in cloud environments include better data security, cybercrime investigations, digital forensics, and regulatory compliance. This strategy can improve cloud security and prevent sensitive data from being concealed or tampered with. The fundamental goal of Steganalysis is to examine image pixels and matching bit patterns to see if a hidden message exists in a seemingly harmless digital image. Detection of this sort is known as binary analysis, passive analysis, or the more conventional form of Steganalysis. It is the first step in deciphering the hidden message and putting it back together again. There are two distinct types of binary steganography: targeted and universal. According to its name, targeted Steganalysis analyses digital images for anomalies caused by a predetermined steganographic embedding technique [3]. However, this steganalysis technique is limited to a particular steganography archetype and cannot be applied to other algorithms or image formats. The method is practically worthless due to a minor change in the embedding process.

Media such as photographs, audio recordings, and written texts can now be rapidly and easily transmitted via cloud computing thanks to advancements in information transfer technology. Steganalysis, whether universal or blind, is a common recognition technique because it does not require prior knowledge to input [4]. It consists of two phases: first, a picture is modeled using high-dimensional features resistant to being altered, and then, a classifier is trained to distinguish between normal and stego images. Universal Steganalysis, in contrast to Targeted Steganalysis, applies to all steganography techniques and picture formats, albeit at the expense of accuracy. There are three distinct formats used in steganography: a written format employing insert message inscription, an aural format using music or discourse for encryption, and a graphical style using graphic graphics or movies for communications [5]. A message can be concealed in data in any format that allows it to be embedded in a bit stream, be it plain text, coded text, symbol-based text, pictures, or anything else. Making a stego image involves inserting a message into a cover photo. The steps involved in making a stego image can be summarized by referring to the cover image, the added message, and the key. The strength of any given steganography scheme can be gauged by its capacity to remain undetected. These are the most common application areas for image steganography: Examples of cutting-edge methods include S-UNIWARD, HUGO, WOW, and MiPOD [6]. The internet is now an effective medium for speedier information transmission due to the remarkable progression of technological media in the information and communicational area in the past era [7]. Though this technology is respected, on the one hand, it also poses a difficulty in securing personal data and private information without data leaks and resulting abuse. Recent research has found that despite a sizeable embedding payload, state-of-the-art image steganography techniques such as SUNWARD, HUGO, WOW, and others remain undiscovered [8].

Steganalysis is an approach to discovering the items that contain undisclosed messages. Image steganalysis checks if a hidden message is disclosed in an image. Conventional steganalysis methods require procedures to check discriminative statistical structures from photos and classify them [9]. In recent years, private information has been gathered for various reasons, including financial transactions, government I.D.s, military activities, and company licensing and recognition. Because unauthorized use of personal records might result in the loss or contamination of documents, the security of many of those details is critical [10]. Even though numerous solutions are being prepared and implemented, the privacy of realities is in jeopardy. With the development of computer security systems, machine learning (ML) has played a crucial role in resolving practical issues with information

security. Applying ML and deep learning to automate various domains is quite simple. This includes the medical field, agriculture [11], the distribution of adequate water supplies, the recognition of facial expressions [12], smart cities, and the surveillance of urban areas [13,14].

Recently, Shankar et al. [8] utilized a modified version of a standard model for image classification to determine the identities of people depicted in stego and cover images. This category includes methods like F5, LSB Replacement, and Pixel Value Difference (PVD) [11]. Throughout Steganalysis, four unique embedding strategies were utilized. The Support Vector Machine (SVM) and the Support Vector Machine-Particle Swarm Optimization (SVM-PSO) were used for classifications. The best results were obtained using the Dot kernel for both the SVM classifier and the multi-quadratic SVM-PSO. JPEG image evaluation in spatial and Discrete Cosine Transformation (DCT) was introduced and analyzed [3]. The author used a variety of inspection strategies, including straight, rearranged, specified, and automated. First-request highlights, second-request highlights, widened DCT elements, and Markov highlights are the components considered for feature extraction. DCT was used to expand DCT, and Markovian highlights were utilized in element-based steganography. The results of PCA were used to eliminate extraneous characteristics after careful consideration of their influence. SVM and SVM-PSO were used as classifiers to characterize the obtained features.

Most research involving artificial intelligence to address security issues related to image steganalysis has also increased. Some things could be improved in recent methods. First, the unavailability of the dataset for Steganalysis created a challenging environment for researchers to develop a dataset according to different schemes. Second, solutions provided in the literature of Steganalysis considered the classification of stego images with information embedded at a high payload and low payload stego image classification still needs to be improved. Third, researchers considered textural and statistical features for classification, which can fetch changes from an image when significant changes occur those are based on high payload embedding. However, it was determined that the images may have low payload data embedded. Stego images can also contain minor artifacts embedded in them. By keeping this in view, it was determined that there were critical areas for improvement in these procedures compared to the standard inspection techniques that utilize image processing.

1. First, there needs to be a standardized, freely available dataset developed with a small amount of payload and a large amount of payload for conducting Steganalysis.
2. Second, modern image classification algorithms with constrained approaches are needed to classify images with high and low payloads. Also, the current methods, which rely heavily on statistical characteristics, generate many feature dimensions from an image. Automating this process with a cheap machine learning-based steganalysis method based on wavelet transformation and support vector machines that any security agency can use to classify images containing embedded information would be a significant step toward solving this problem.

In response to these limitations, this research has some corresponding contributions. Firstly, a new dataset has been developed by applying various steganography methods to various payloads. BossBase and Bag of Visual Words Dataset (BOWS) are two examples of image datasets used in state-of-the-art methods, although they have nothing to do with steganography. It was decided that a shared steganalysis dataset was necessary. The developed dataset includes the original and steganographic versions of 5,000 images using BossBase. Secondly, a robust technique based on a Curvelet transformation to extract wavelet features has been proposed to capture minor and major changes in the image. After that, SVMs will be used to categorize the characteristics. Departments concerned with security and image forensics will find this useful.

The other sections of this article have followed this order: Section 2 describes the related work for steganography and steganalysis techniques. Section 3 describes the stages of the proposed

methodology and provides a short explanation of every step, like preprocessing, then feature extraction, and at last, classification. In this section, databases that are being used for experiments are also described. Section 4 presents an experimental setup and results in discussions for the proposed architecture. It offers tables and figures related to results calculated using the proposed architecture. At last, Section 5 provides conclusions and future directions for this study.

2 Literature Review

Through many insightful developments, scientific Steganalysis hopes to uncover more facts about the hidden message and, in the end, remake the unknown message. While paired Steganalysis can assist in slowing down illegal and undesired interactions, quantitative or measurable Steganalysis seeks to go beyond this I.D. and investigates the substance of such collaborations to decode deeper secrets [9]. Binary Steganalysis mainly focuses on three types of techniques to detect steganography. First is the structural change in images by analyzing an appearance in the spatial domain. Second is the classification method to verify whether an image contains secret information. The third one is to investigate some information from the stego image, like payload, stego key used during the embedding process, and private messages from the stego image [15].

In this article, we have reviewed different approaches related to classifying stego and cover images. State-of-the-art methods show two classification strategies based on the supervised learning approach. Machine learning-based approaches in which an image is first preprocessed to extract relevant information using some preprocessing algorithms. The image then extracts features of interest based on structural changes by analyzing the spatial or frequency domain image. In the classification process bag of features with labels is used to train any classification algorithm like SVM, SVM-PSO [16], and Ensemble. Based on Convolutional Neural Network (CNN), different deep learning and transfer learning approaches have been introduced recently. CNN involves a learning process based on the layered architecture in which several layers are being used for the learning process. Deep learning is based on the fitness of models trained using CNN or other networks. ADAM and ReLU were used as activation functions in almost all CNN-based models.

2.1 Machine Learning Methods for Steganalysis

Ye et al. [7] recently used a traditional machine learning method for stego image classification. Four distinct embedding approaches F5, Least Significant (LSB) Replacement, and PVD were used for Steganalysis. SVM and SVM-PSO were the classifiers employed. Linear, radial, multi-quadratic, ANOVA and polynomial kernels were utilized in classification. The classifier was taught to analyze each coefficient as an independent unit, and the results of this analysis aid in determining the Steganalysis conclusion. PSO classifiers outperformed all other kernels, according to the results. Kang et al. [17] pointed out that shading image steganography weakened the link between the gradient amplitudes of different color channels and presented a color image steganalysis computation based on the channel angle relationship. Each color channel used the gradient amplitude of image channels to obtain gradient amplitude and steganalysis characteristics. It can be observed that the proposed steganalysis method beat existing steganalysis algorithms for both WOW and S-UNIWARD steganography.

The approach made by Chaeikar et al. [16] covered three areas: bunch S.W. steganalysis, outfit S.W. steganalysis, and gathering S.W. steganalysis. In the following section, an SVM classifier ponders the datasets to their associated reference profiles and uses a trapezoidal cushy cooperation ability to choose the degree of enlistment of given pixels. Consequently, six datasets contain all the image pixels' apparent pixel classes and enlistment degrees. The results then diverged from steganalysis systems

with humble examination viewpoints that were comparative. The social event S.W. approach given here achieved 86.771 percent accuracy. This accuracy improved to 99.626 percent, unquestionably the most anytime achieved by any low assessment angle approach. The discoveries of JPEG image appraisal in spatial and DCT changes were introduced [18], and an examination was made. The author utilized straight, rearranged, defined, and computerized inspecting techniques. Four feature extraction elements were considered: request highlights, second request highlights, broadened DCT elements, and Markov highlights. The impact of features has been contemplated, and Principle Component Analysis (PCA) has been used to eliminate unwanted attributes. The acquired attributes were characterized by utilizing two separate classifiers: SVM and SVM-PSO. When utilized in spatial change, the classification portion often gave a high arrangement rate. As we can see, most of the study's authors have used statistical and textural features to get structural changes of an image to classify using SVM or SVM-PSO. Some do not consider evaluating low-payload data, and some who consider this problem have calculated high dimensional features, which will use high computation and storage capacity, which is not accessible to all concerned personnel. Table 1 shows different machine algorithms from recent research on color image steganalysis.

Table 1: Machine learning approaches for image steganalysis

Ref.	Techniques	Findings	Pros	Cons
[8]	Extended DCT and Markov Features + SVM and SVM-PSO	SVM Dot kernel produces better results than other SVM kernels. PSO classifier has a better outcome.	Both spatial and transform domain steganography images were considered.	Minor Embedding can be detected by using kernels and the sampling method.
[18]	DCT and Markov Features + PCA for removal of unwanted features + SVM and SVM-PSO	SVM with optimization for ANOVA kernel is used to improve results.	The transform domain of image analysis was considered.	Minor Embedding can be detected, and only the transform domain was considered.
[16]	(Pixel color correlation + Color profiles + Edge Pixels) + Modified SVM	The ensemble method for learning was designed and evaluated at different payloads that show the highest sensitivity.	Color correlation for both pixel-wise and channel-wise was calculated.	The payload value was so small as compared to other techniques. Validation measures were not most appropriate as compared to others.
[17]	(Gradient Magnitude + SCRMQ I) + Ensemble Classifier	Image color channel correlation was covered using the channel gradient magnitude of the color channel. The model was tested on different payloads and shows the highest T.P. and F.P. rates.	Color correlation based on the color channel was considered.	The feature dimension was high. One type of stego image was used.

2.2 Deep Learning Methods for Steganalysis

Reinel et al. [19] proposed better architecture than QIAN NET, SR-NET, XU-NET, YE-NET, & ZHU-NET named GBRAS-NET by using spatial details of an image. The accuracy achieved by this architecture with MiPOD, HILL, and HUGO through BOSSbase 1.01 was 68.3, 68.5, and 74.6 for 0.2 bpp. The data augmentation architecture showed the highest accuracy. While BOWS 2 showed the accuracy improvement for WOW and S-UNIWARD-0.7% and 2.2%, respectively. An approach based on Siamese CNN for the Steganalysis of images was proposed by You et al. [20]. Steganographic Noise was extracted from the images' sub-regions of one Siamese network using each subnet. For feature extraction, down sampling was done with a stride value set to 2 on Block B. ROC showed the testing of BOSSbase 1.01 images 256 × 256 with 0.4 bpp. The proposed SiaStegNet was tested on BOSS-256 & BOSS-512. Comparing the proposed with SRNet, the accuracy achieved with S-UNIWARD was 91.89%, with HILL 85.97%. ALASKA#2 dataset was also used to demonstrate the proposed network.

Liu et al. [5] proposed an approach based on CNN techniques having diverse filter modules & squeeze excitation. After each convolution layer, a B.N. layer was added to avoid overfitting and fasten the learning. Using the WOW algorithm & payload of 0.2 & 0.4 bpp, both models were trained. Resized images of BOSSbase 1.01 with the size of 256 × 256 were implanted using 0.1, 0.2, 0.3 & 0.4 bpp on S-UNIWARD & WOW algorithms. The error rate of the proposed method was minimized to 8.5% compared to SRM+EC, and 6.7% error was minimized as compared to Xu Net, 3.9% to Ye Net, and 3% to Yedroudj Net. Singh et al. [21] proposed a solution for Steganalysis by dividing their work into two sections. It was necessary to accurately forecast the cover image from the associated stego image to see accurate noise residual. A denoising learning kernel was applied in this study to obtain a more precise noise. This method created a CNN-based Steganalysis detector, and the noise residual is used to train the detector for more accurate detection. The suggested approach outperforms the other Steganalysis schemes, according to experimental results.

A practical CNN-based Steganalysis approach with a combined domain and nonlinear detection mechanism was introduced by Wang et al. [22]. The nonlinear detection process depended on the spatial rich model to present the maximum and lowest nonlinear residual feature acquisition approach. The author employed high-pass channels for spatial residuals in the joint location framework and used instances from the discrete cosine change remaining (DCTR) for change steganography. The findings also demonstrated that the model's combined WOW and S-UNIWARD identification precision was higher than SRM+EC, Ye-Net, Xu-Net, Yedroudj-Net, and Zhu-Net is roughly 4 to 6 percent higher than the best Zhu-Net. Wu et al. [23] introduced multiple steganography for deliberate image downsampling based on CNN-based Steganalysis. The detection performance can be increased after training with shrunk images. Because the suggested method's preprocessing was so simple, it did not significantly increase CNN training time.

The experiment's findings demonstrated that accuracy is up to 34.8 percent higher than in the traditional approach, especially when the same steganography is integrated. Singh et al. [24] proposed a brilliant Normalization method named Shared Normalization (S.N.). CNN was improved by the expansion of a new convolutional layer named the S.N. layer, bringing about a CNN that was advanced for computerized image steganalysis. Broad investigations were done to show that the proposed S.N. layer and the new CNN model for image steganalysis were compelling. The recommended network was contrasted with the cutting-edge prosperous model procedure and with different as late proposed CNN models. The second approach for Steganalysis is deep learning, as discussed in the introduction section. Table 2 describes some deep learning-based methods to show contributions made in the last few years. The techniques discussed in Most of the research focused on preprocessing images. The

proposed method is inspired by de-noising kernels to get embedded information and classify it using CNN. The proposed method used Curvelet transformation for feature extraction recently published for de-noising any image. So, noise residuals can be fetched through Curvelet features. Table 2 was based on CNN and used different methods and layers to classify stego images.

Table 2: Deep learning approaches for image steganalysis

Ref.	Techniques	Findings	Pros	Cons
[19]	Filter-based noise addition + CNN layers based feature extraction and machine learning	Improved accuracies were achieved on different payloads on two different datasets.	Different adaptive stenographic methods were targeted.	Most work was done in the preprocessing stage.
[21]	Modified CNN layers. ZDNet based on fractal Network	Outperformed against the different state-of-the-art methods.	Spatial, Transform, and adaptive methods of steganography were considered.	Image compression was not considered.
[20]	Siamese, CNN-based architecture with shared parameters	Improved results on multi-sized images from two benchmarked datasets.	Worked on multi-sized images and works well on different types of stego images.	Fixed-sized training parameters were implemented
[5]	(Diverse filters + Squeeze and Excitation) + CNN	CNN outperformed content-adaptive steganographic images with different payloads.	Different techniques like B.N. and TLU were used to enhance the performance of CNN.	Only same-size images were analyzed.
[25]	Denoising kernel to obtain noise residual + CNN	Image denoising was more responsive than fixed high-pass filters.	Different payloads were used to test datasets. Different techniques were tested.	Different neural network-based architectures can be used to obtain Noise.

3 Material and Methods

There are three distinct phases to the procedure at hand. As a first phase, images are selected from BOSSbase 1.01. Selected photos are then subjected to steganographic Noise using S-UNIWARD, WOW, HUGO, and MiPOD with various payloads to generate a dataset. Each stego and cover image produced by the datasets is passed to the block division module to get equal blocks of every passed image, then the feature extraction module, which incorporates the curvelet feature transformation. After extraction of features from images, a support vector machine is used to classify images using the created feature vectors. This all experiment has been carried out using MATLAB R2021a. Fig. 1 depicts the Steganalysis framework for stego image classification.

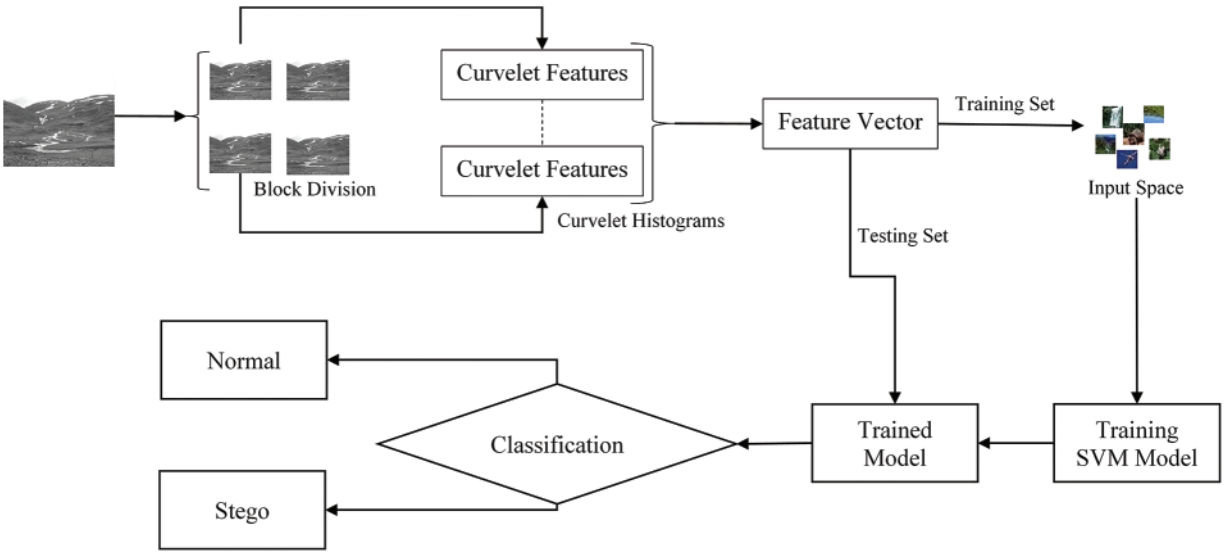

Figure 1: Proposed steganalysis framework for stego image classification

3.1 Dataset

An image with steganographic content has a type of distortion in that image. So, modules like S-UNIWARD, WOW, HUGO, and MiPOD [19] are used to embed this distortion using spatial details of the image used in this experiment. Researchers in Steganalysis rely heavily on the massive and varied BOSSBase 1.01 dataset. Each of the 10,000 color images in BOSSBase 1.01 has a resolution of 256 pixels on the longest side and 256 pixels on the shortest side. The dataset was designed as a standard against which steganographic and Steganalysis methods might be measured. It features a variety of visual elements, such as landscapes, textures, and graphics, to depict various situations in the actual world. This dataset can be used to train and evaluate steganalysis machine learning methods. The dataset contains photos modified using several steganographic algorithms, making it a valuable tool for researching and developing new steganalysis methods. The database discussed is mined for the original images. For experiments, we made use of a variety of steganographic techniques to create stego images. Normal images were taken from a public database and created stego images using the steganography algorithms previously discussed. In subsequent experiments, a steganalysis framework has been used. The dataset has been separated so that each group of stego photos is coupled with a normal image.

Each dataset developed is further divided into two sets of training and testing datasets to do some experimentations using the proposed steganalysis framework. This table shows the total number of normal, payload, and stego images in various steganographic datasets. S-UNIWARD is the initial dataset; it consists of a thousand normal images with payloads of 0.1, 0.2, 0.3, and 0.4. There are 4,000 steganographic images in this data set. The WOW dataset has 1,000 normal and 4,000 stego images, but the payload values are unknown. HUGO, the third dataset, similarly has 1,000 normal images and 4,000 stego images, but again, details need to be given concerning the payload. The final dataset, MiPOD, consists of 1,000 normal and 4,000 stego images, although the payload values utilized still need to be discovered. The four datasets contain 4,000 reference images and 16,000 stego images, making them excellent tools for steganography study. These datasets help create and evaluate steganalysis algorithms, which can uncover secret content in digital photographs. Following

the creation of steganographic images, we have split the dataset into subsets for practical purposes shown in Table 3.

Table 3: Division of datasets for experimentation

Sr.	Dataset	Normal images	Payload	Stego images
1	S-UNIWARD	1,000	0.1, 0.2, 0.3, 0.4	4,000
2	WOW	1,000		4,000
3	HUGO	1,000		4,000
4	MiPOD	1,000		4,000
Total		**4000**		**16000**

3.2 Preprocessing

Information embedded into images can reside in any part of the image, so images are read from the directory then block division is implemented using non-overlapping block division by using a script written in MATLAB R2021a to reduce error in getting interested features in the feature extraction process. The script gets an image of any size and augments it into equal blocks of 256 × 256. Each image is adjusted to size with respect to multiples of 8 through padding so it can be divided into blocks of size 256 × 256. After this process, an image is converted into blocks of 256 × 256 as shown in Fig. 2.

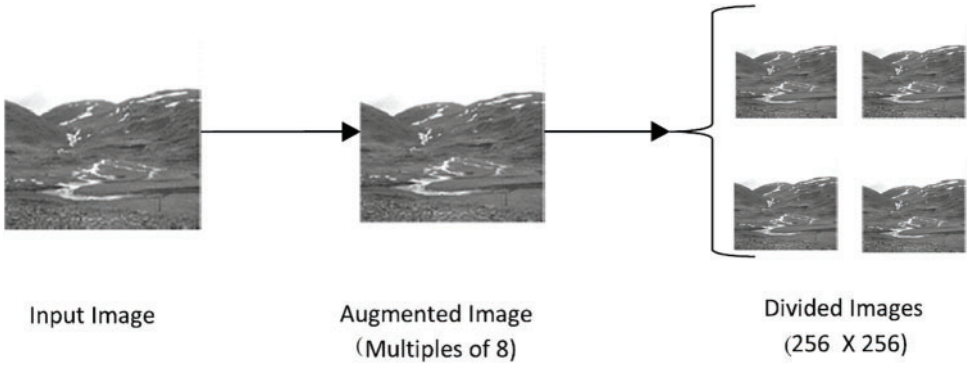

Figure 2: Workflow of the preprocessing stage

3.3 Feature Extraction

Curvelet is a multiscale geometric analysis tool that efficiently takes image curve singularities. Each image block is passed to curvelet transform to get texture features of an image that will be used for differentiation and learning for normal, Stego, and Cover images. Unlike methods like Wavelet transformation, curvelet transformation can be used on images in numerous dimensions and scales. Compared to Wavelet transformation, Curvelet transformation is more advantageous because of its sparse representation of local features, edges, and textures and its ability to capture curved edges and finer details in an image. Images are described in a curvelet domain, where the basic functions can be orientated in many ways. Curvelet transformation may have been chosen for feature extraction in a specific study because of its improved ability to capture and express highly curved qualities

like contours and textures. Since it faithfully encodes curved and anisotropic features, the Curvelet transform is a viable option for image analysis, object recognition, and denoising.

Scale- and orientation-invariant picture characteristics are particularly well captured by curvelet transformation. This opens the door to discovering hidden information by revealing hidden patterns and textures. The key to their interpretability is an insight into the correspondence between these multi-scale traits and certain steganographic methods or artifacts. Subtle alterations to an image's texture are common in steganography. Using Curvelet features can bring out these subtle alterations in texture, revealing previously unseen details. The presence and type of steganographic content can be deduced by analyzing the unique texture patterns retrieved via Curvelet transformation.

Furthermore, its parabolic scaling capabilities provide nearly optimal sparse symbols of objects with C.S. ("curve singularities"). On the other hand, the curve singularities can be achieved by dividing the image into sub-images and then applying the R.T. ("ridgelet transform") to all the sub-images obtained. C.T. (Curvelet transform) was the name for this block-based transform. However, the ridgelet's imprecise geometry has hampered the first-generation curvelets' use in various applications. Then, a second-generation curvelet transform was offered to solve the difficulties with first-generation curvelets. We employ quick DCT ("discrete curvelet transform") instead of wavelets and their derivatives to capture more directional data because the texture information of an image includes a mess of curves and lines. The following are the basic mathematical initiations of the CCT ("continuous curvelet transformation") and DCT ("Discrete curvelet transforms"). The CV ("Curvelet transform") can be defined as an inner product for a given signal f as

$$C(j,l,k) = \langle f, \varphi_{j,l,k} \rangle \tag{1}$$

We can express the inner product as an integral over the frequency plane by expressing it as an integral over the frequency plane. Where the curvelet bases function is $\varphi_{j,l,k}$ And parameters are j, l, and k, which are scale, direction, and position are j, l, and k, respectively. The continuous curvelet transform is implemented in 2D, i.e., (R2) and can be displayed in the frequency domain using x as the spatial and frequency domain variables. In the frequency domain, r and are the polar coordinates. Given a pair of smooth, non-negative, real-valued windows W(r) and V(t), referred to as radial and angular windows, respectively, with r ($\frac{1}{2}$, 2) and t [1,1]. W and V will always meet the following requirements:

$$\sum_{j=-\infty}^{\infty} W^2\left(2^j r\right) = 1, \quad r \in \left(\frac{3}{4}, \frac{3}{2}\right) \tag{2}$$

$$\sum_{l=-\infty}^{\infty} V^2(t-1) = 1, \quad t \in \left(\frac{-1}{2}, \frac{1}{2}\right) \tag{3}$$

The frequency window Uj in the Fourier domain is then given for each j ≥ j0.

$$cU_j(r,\theta) = 2^{\frac{-3j}{4}} W\left(2^{-j} r\right) V\left(\frac{2^{\left\lfloor \frac{j}{2} \right\rfloor}\theta}{2\pi}\right) \tag{4}$$

where $\left\lfloor \frac{j}{2} \right\rfloor$ represents the integer portion of $\frac{j}{2}$. As a result, the support of U_j is a polar wedge that is interpreted by the support of W and V, which are applied in each direction with scale-dependent window widths. To generate real-valued curvelets, consider the symmetric variant of U_j, i.e., $U_j(r+\theta) + U_j(r, \theta+\pi)$. Let us describe the waveform $\varphi_j(x)$ using its Fourier transform $\varphi_j(\omega) = U_j(\omega)$, where $U_j(\omega_1, \omega_2)$ is the polar coordinate system window. In the sense that all curvelets at size 2^{-j} are formed by

rotations and translations of φ_j. It can be considered the mother curvelet. Curvelets can be generated at scale 2^{-j}, orientation. θ_l, and position $x_k^{j,l}$ using the function x = (x1, x2) by

$$c\varphi_{j,l,k}(x) = \varphi_j\left(R_{\theta_l}\left(x - x_k^{(j,l)}\right)\right) \tag{5}$$

where $k = (k_1, k_2) \epsilon Z^2$ specifies the order in which the translation parameters are applied, $\theta_l = 2\pi.2^{-\left\lfloor \frac{j}{2} \right\rfloor}.l, l = 0, 1, \ldots$ such that $0 \leq \theta_l < 2\pi$, and $x_k^{(j,l)} = R_{\theta_l}^{-1}\left(k_1.2^{-j}, k_2.2^{\frac{-j}{2}}\right)$. R_θ and R_θ^{-1} denote the rotation by θ radians and its inverse, respectively, and are defined as

$$cR_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}, R_\theta^{-1} = R_\theta^T = R_{-\theta} \tag{6}$$

The inner product of an element f and a curvelet is the curvelet coefficient. $\varphi_{j,l,k}$, i.e.,

$$cC(j,l,k) = \left\langle f, \varphi_{j,l,k} \right\rangle = \int_{R^2} f(x)\,\overline{\varphi_{j,l,k}} dx \tag{7}$$

$$cC_{j,l,k} = \frac{1}{(2\pi)^2}\int \hat{f}(\omega)\,\overline{\hat{\varphi}_{j,l,k}(\omega)}\,d\omega = \frac{1}{(2\pi)^2}\int \hat{f}(\omega)\,U_j\left(R_{\theta_l}\omega\right) e^{i\left\langle x_k^{(j,l)}, \omega \right\rangle} d\omega \tag{8}$$

The integral function combines the Fourier transform of the input image with the curvelet transform's directional filters and scale functions to compute the coefficient value C(j,l,k) at the specified scale, angle, and position. This coefficient represents a localized feature or pattern in the image, capturing its multi-scale and multi-directional information. The linear-digital curvelet transform of a Cartesian input array $f(t_1, t_2); 0 \leq t_1, t_2 < n$ is defined by a set of coefficients as

$$C^D(j,l,k) = \sum_{0 \leq t_1, t_2 < n} f[t_1, t_2]\,\overline{\varphi_{j,l,k}^D[t_1, t_2]} \tag{9}$$

3.4 Classification

Instead of focusing on creating the best possible classifier, we have chosen to improve feature extraction and use previously obtained findings to determine which classification algorithm to use. We rely on the Support Vector Machine, a machine learning algorithm with superior feature representation ability to power our classification system. Because of its robustness and classification accuracy, the SVM has shown to be an effective machine learning and data mining tool. The primary objective in detecting stego instances is high sensitivity and high throughput. The labels were then classified as either Stego cases or others. Different SVMs have been trained on various kernels, and the one with the greatest classification performance has been selected for this study. We have created 72 features for training data from all steganographic produced photos. For educational reasons, cross-validation is a popular technique. We have utilized a cross-validation scheme with 10 samples and 5 results. Seventy percent of the data was used for instructional purposes, while the remaining thirty percent was used for assessment purposes. The SVM model performs admirably on high payload data, such as that seen in photos.

3.5 Evaluation of Steganographic Techniques

Making a difference between cover and stego image is quite a difficult task for a human, so statistical tools like Peak Signal Noise Ratio (PSNR) and Structured Similarity are being used to check the difference between cover and generated stego image.

$$PSNR = 10.log_{10}\left(\frac{MAX_{IM}^2}{MSE}\right) \tag{10}$$

Peak Signal-to-Noise Ratio (PSNR) is a metric used to evaluate the quality of a reconstructed or compressed image, and the accompanying equation represents its calculation. The ratio between the original signal's maximum power and the strength of any noise or distortion introduced during reconstruction or compression is known as the Signal-to-Noise Ratio (SNR). The maximum squared pixel value (MAX_IM2) is divided by the Mean Squared Error (MSE) to get PSNR for the reconstructed/compressed image. After that, a logarithmic scale with a base of 10 is applied to the final output. A higher PSNR number suggests a higher quality image since it indicates less distortion or noise in the reconstructed image. PSNR is commonly given in decibels (dB).

3.6 Evaluation of Steganalyzer

When considering steganalyzer, detection loss is the assessment parameter utilized most of the time. Many distinct measures, such as training accuracy, TPR, FNR, and AUC may be used to evaluate an SVM-based classification process. So, in this study, we will evaluate the proposed approach, which may be found below, using three different parameters.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{11}$$

where *Accuracy* is the total number of correct guesses divided by the total number of correct forecasts, then multiplied by 100 to get a percentage, the percentage of correctly identified samples in the true positive rate is determined using.

$$\mathrm{TPR} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \tag{12}$$

The percentage of samples that are wrongly identified constitutes the false positive rate, which is computed using:

$$FNR = \frac{FP}{FP + TN} \tag{13}$$

Here, the terms "T.P.," "T.N.," "F.P.," and "F.N." refer to the quantities of true positives, true negatives, false positives, and false negatives, respectively, as defined in the previous section. The area under the curve (AUC) is a robust metric for gauging a classifier's efficacy in a two-class classification task. It is a crucial aspect of ROC analysis, which compares the true positive rate (TPR) against the false positive rate (FPR) at various cutoffs for making a correct classification. The area under the curve (AUC) can be viewed as a metric of the feature space's capacity to distinguish between the two classes. If the AUC is greater, the classifier did a better job distinguishing between the two groups. It's also a measure of the classifier's ability to rank instances based on their likelihood of being in the right class.

4 Results and Analysis

The recommended model was developed with the help of MATLAB R2021a and its Curvelab package so that it could be evaluated. The performance of the recommended scheme was subjected to a complete set of tests to evaluate its steganalysis capabilities; the results of those tests are presented in this section. A variety of methods were applied to achieve the results of the performance evaluation. A script written in MATLAB was used to embed steganographic data. Additionally, MATLAB was

used to implement feature extraction and classification learning, which was utilized for classification using SVM. A non-overlapping block division is used as the first phase in our process as a preliminary step. When it came time to train and assess SVM models, we relied on the evaluation method described in Section 3.6.

These areas were the focus of the experiments:

1. Evaluation of embedding techniques used to develop stego images at different payloads.
2. Performance evaluation of proposed steganalysis framework among different steganography methods.
3. Comparative analysis of proposed method with state-of-the-art methods.

4.1 Evaluation of Embedding Distortion in Images

Different steganographic techniques were used to embed extra data in images so images could be classified accurately. Four types of steganographic methods named S-UNIWARD, WOW, HUGO, and MiPOD are used to embed Noise as information at the payload of 0.1, 0.2, 0.3, and 0.4. The Noise was added at different payloads using MATLAB R2021a, and PSNR was calculated for each image with a distorted image to evaluate each image after making it a stego image. In this case, Noise is considered as data embedded in an image as any changes occur, while steganography changes the structure of any image. So, Noise is also data added to standard images to change their structure to get structural changes from an image to classify any stego image. After adding Noise, some or much of the data of the image is changed. To check how many changes are made using a specific method PSNR is calculated between the cover and stego image. The peak signal-to-noise ratio between two images, measured in decibels, is computed by the PSNR block. This proportion is used to compare the original and distorted images' quality. The quality of rebuilt image improves with increasing PSNR. Payload is the most critical measure to consider while embedding data in images. It can be observed through the table that as the payload increases from 0.1 to 0.4 for each steganographic method, PSNR also increases. This means that as data grows in images, PSNR shows that generated image signals have high-payload data. Table 4 shows the average PSNR between images.

Table 4: Data embedding results on different steganography methods

Steganographic method	Payload (bpp)	PSNR
S-UNIWARD	0.1	55.04
	0.2	58.10
	0.3	62.30
	0.4	67.11
WOW	0.1	52.10
	0.2	58.35
	0.3	63.13
	0.4	69.27
HUGO	0.1	51.10
	0.2	55.03
	0.3	60.20
	0.4	65.31

(Continued)

Table 4 (continued)

Steganographic method	Payload (bpp)	PSNR
MiPOD	0.1	49.20
	0.2	53.15
	0.3	59.43
	0.4	64.26

4.2 Performance Evaluation of Proposed Steganalysis Framework

The experiment used support vector machines with 10-fold cross-validation using MATLAB R2021a. Four steganographic methods were used to develop the steganalysis dataset. After steganography, we have five datasets, as described in Section 3.1. Features set of each dataset created using S-UNIWARD, WOW, HUGO, and MiPOD contains 1,000 samples for normal and 4,000 samples for stego. Each feature is divided into two sets of training and testing after splitting it into two parts by a ratio of 70:30, respectively. The model was trained with the SVM training parameters provided in Section 3.5, and it was exported using the SVM kernel with the most outstanding performance. After the training model test dataset was imported, the model was tested.

Classification results of the proposed method on different steganographic methods are shown in Table 5. It illustrates three performance measures Accuracy, TPR, FNR, and AUC. Accuracy indicates to what extent the SVM model accurately classifies normal and stego images. TPR is the proportion of accurate forecasts in predictions of the positive class. FNR is the proportion of positive data cases mistakenly labeled as negatives to all positive instances in the data. The likelihood that a random positive (green) example will be placed in front of an unexpected negative (red) example is represented by AUC. AUC has a value between 0 and 1. A model with 100% incorrect predictions has an AUC of 0.0, whereas a model with 100% correct predictions has an AUC of 1.0. Performance metrics show the highest performance on two steganography methods, S-UNIWARD and HUGO, 97.2% and 98.6%, respectively. On the other hand, we have evaluated the proposed method on the combined dataset by combining all the features. SVM shows the accuracy of 95.9%, as shown in Table 5.

Table 5: Classification results of proposed steganalysis framework using BOSSBASE 1.0 using different steganography methods

Steganography method	Accuracy	TPR	FNR	AUC
S-UNIWARD	97.2	95	5	0.96
WOW	95.4	96	4	0.98
HUGO	98.6	99	2	0.98
MiPOD	92.4	96	5	0.98
Combined	95.9	98	3	0.98

Classifiers better identify positive and negative data when their AUC values are closer to 1. The AUC measures how likely the classifier will assign a higher score to a randomly selected positive example than a randomly selected negative one. The AUC for a perfect classifier is 1, while the AUC for a random classifier is 0.5. The suggested method achieved much better binary classification results

than any other available datasets. The area under the curve (AUC) must first be calculated to evaluate the proposed model properly. Fig. 3 presents the receiver operating graph, which allows for visualizing the area under the curve. On the left graph, the area under the curve (AUC) for the normal class is 0.97, and the area under the curve for the stego class is presented on the right graph. Both of these values are relatively near to 1, which indicates that this model produced the best results when applied to the classification process.

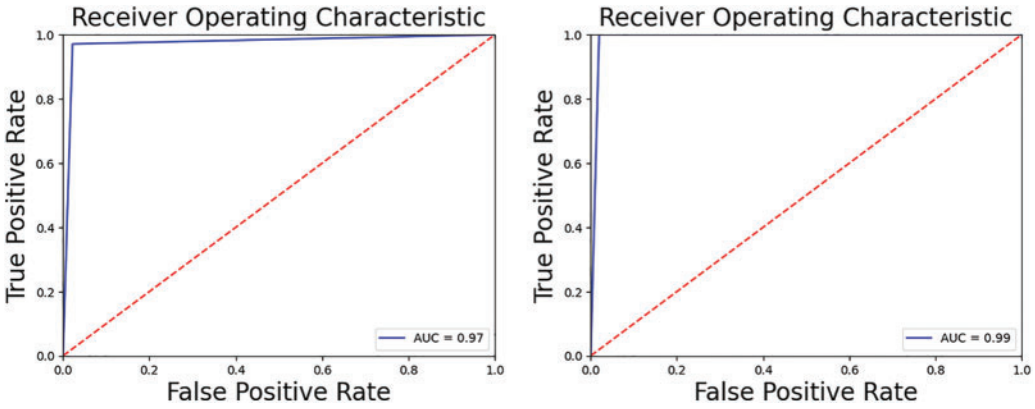

Figure 3: The receiver operating curve for both classes (left) normal class (right) stego class

4.3 Comparative Analysis with State-of-Art Methods

Different techniques for steganalyzer were described in Section 2. Some are machine learning-based, and others are based on deep learning. To evaluate the efficacy of a new model, it is useful to compare it to others that have been tried and tested using the same data. As part of this research project, we compared our approach to similar current approaches. SRNET [25], GBRAS-Net [19], and LSCA-YeNet [26] were the methodologies examined and compared. SRNET [26] showed 89.18% accuracy at the payload of 0.4 using S-UNIWARD, GBRAS-Net showed 89.8% accuracy at 0.4 payloads using WOW, and LSCA-YeNet showed 84.44% of accuracy at 0.4 payloads using WOW as we know that payload is directly proportional to detection rate. As a result, our system outperforms other approaches in the comparison study while using a minimal set of characteristics. As a rule, more features are seen to be better. Yet, when sophisticated calculations are unavailable, the time required to complete a particular task rises because of the large number of characteristics. It is already a challenge in model training to accomplish classification jobs that a high feature count might increase classification time with massive datasets. Table 6 shows the proposed efficiency and accuracy among them.

Table 6: Comparative analysis with state-of-the-art methods

Citation, year	Method	Steganography algorithms	Accuracy
[25], 2022	SRNET	S-UNIWARD WOW	89.08 89.18

(Continued)

Table 6 (continued)

Citation, year	Method	Steganography algorithms	Accuracy
[19], 2021	GBRAS-Net	S-UNIWARD	87.1
		WOW	89.8
		HUGO	84.5
		MiPOD	81.4
[26], 2020	LSCA-YeNet	S-UNIWARD	82.57
		WOW	84.44
Proposed	**Curvelet transformation and SVM**	**S-UNIWARD**	**97.20**
		WOW	**95.40**
		HUGO	**98.60**
		MiPOD	**92.40**

5 Conclusion

This article's proposed framework mainly focuses on preprocessing and feature extraction stages and outperforms different steganalysis frameworks. It uses a novel image feature extraction method to get optimal features of an image and trains an SVM to classify stego images. Accuracy, TPR, and FNR are used to compute the performance of the SVM model. The proposed architecture classifies images with the best accuracy on two steganography methods, S-UNIWARD and HUGO, 97.2% and 98.6%, respectively. On the other hand, the proposed method evaluated the combined dataset by combining all the features and showed an accuracy of 95.9%. Additionally, experiments were conducted to show how SVM performed against different steganographic datasets at different payloads, and the proposed method showed the best performance among other state-of-the-art methods. There are constraints to think about, even though the suggested approach shows promising results and outperforms existing state-of-the-art methods in steganalysis. A future CNN-based model will hopefully overcome these obstacles, as will the current emphasis on certain steganography techniques. The framework's credibility, generalizability, and potential impact in the fight against the unlawful transmission of steganographic content will all be boosted by fixing these issues. In future work, we will study ALASKA 2 and LARGE-SCALE IMAGES databases for further investigation. Moreover, we will work on the development of a novel model based on CNN and will introduce an efficiently trained model to classify stego images. So, the dispensation of illegal transmission can be prohibited.

Acknowledgement: The authors would like to thank Deanship of Scientific Research at King Khalid University, Department of Computer Science, Superior University, Lahore, Pakistan, and Department of Computer Science & Engineering, University of Engineering & Technology Lahore, Narowal Campus, Narowal, Pakistan and University of Okara for providing us wonderful technical support in the research. The authors acknowledge the MLC Research Lab, Okara for their important and fruitful comments to enhance the quality of the current article.

Funding Statement: This research was financially supported by the Deanship of Scientific Research at King Khalid University under Research Grant Number (R.G.P.2/549/44).

Author Contributions: The authors confirm contribution to the paper as follows: conceptualization, methodology, programming, research draft, dataset creation: Arslan Akram; programming, dataset creation, supervision: Imran Khan; technical framework, proof reading, supervision: Javed Rashid; revision, theoretical framework, resources: Mubbashar Saddique; revision, programming, proof reading: Muhammad Idrees; revision, methodology: Yazeed Yasin Ghadi; proof reading, resources, funding: Abdulmohsen Algarni. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Conflicts of Interest: The authors declare they have no conflicts of interest to report regarding the present study.

References

[1] R. T. Bindu and T. Kavitha, "A survey on various crypto-steganography techniques for real-time images," in *Proc. of Intelligent Cyber Physical Systems and Internet of Things: ICoICI 2022*, Coimbatore, Tamilnadu, India, pp. 365–373, 2023.

[2] J. Kim, H. Park and J. I. Park, "CNN-based image steganalysis using additional data embedding," *Multimedia Tools and Applications*, vol. 79, no. 1, pp. 1355–1372, 2020.

[3] D. Hu, S. Zhou, Q. Shen, S. Zheng and Z. Zhao, "Digital image steganalysis based on visual attention and deep reinforcement learning," *IEEE Access*, vol. 7, pp. 25924–25935, 2019.

[4] L. Demidova, I. Klyueva, Y. Sokolova, N. Stepanov and N. Tyart, "Intellectual approaches to improvement of the classification decisions quality on the base of the SVM classifier," *Procedia Computer Science*, vol. 103, pp. 222–230, 2017.

[5] F. Liu, X. Zhou, X. Yan, Y. Lu and S. Wang, "Image steganalysis via diverse filters and squeeze-and-excitation convolutional neural network," *Mathematics*, vol. 9, no. 2, pp. 189, 2021.

[6] M. Dalal and M. Juneja, "Steganography and steganalysis (in digital forensics): A cybersecurity guide," *Multimedia Tools and Applications*, vol. 80, no. 4, pp. 5723–5771, 2021.

[7] J. Ye, J. Ni and Y. Yi, "Deep learning hierarchical representations for image steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2545–2557, 2017.

[8] D. D. Shankar and A. S. Azhakath, "Minor blind feature based Steganalysis for calibrated JPEG images with cross validation and classification using SVM and SVM-PSO," *Multimedia Tools and Applications*, vol. 80, no. 3, pp. 4073–4092, 2021.

[9] M. Cococcioni, F. Rossi, E. Ruffaldi and S. Saponara, "Fast approximations of activation functions in deep neural networks when using posit arithmetic," *Sensors*, vol. 20, no. 5, pp. 1515, 2020.

[10] S. Chutani and A. Goyal, "A review of forensic approaches to digital image steganalysis," *Multimedia Tools and Applications*, vol. 78, no. 13, pp. 18169–18204, 2019.

[11] J. Rashid, I. Khan, G. Ali, S. H. Almotiri, M. A. AlGhamdi *et al.,* "Multi-level deep learning model for potato leaf disease recognition," *Electronics*, vol. 10, no. 17, pp. 2064, 2021.

[12] A. Akram, J. Rashid, F. Hajjej, S. Yaqoob, M. Hamid *et al.,* "Recognizing breast cancer using edge-weighted texture features of histopathology images," *Computers, Materials & Continua*, vol. 77, no. 1, pp. 1081–1101, 2023. https://doi.org/10.32604/cmc.2023.041558

[13] H. Chu, M. R. Saeed, J. Rashid, M. T. Mehmood and I. Ahmad, "Deep learning method to detect the road cracks and potholes for smart cities," *Computers, Materials & Continua*, vol. 75, no. 1, pp. 1863–1881, 2023.

[14] A. Akram, J. Rashid, M. A. Jaffar, M. Faheem and R. Ul Amin, "Segmentation and classification of skin lesions using hybrid deep learning method in the Internet of Medical Things," *Skin Research and Technology*, vol. 29, no. 11, pp. e13524, 2023. https://doi.org/10.1111/srt.13524

[15] Y. Yousfi, J. Butora, E. Khvedchenya and J. Fridrich, "ImageNet pre-trained CNNs for JPEG steganalysis," in *Proc. of IEEE Int. Workshop on Information Forensics and Security (WIFS)*, New York, NY, USA, pp. 1–6, 2020.
[16] S. S. Chaeikar and A. Ahmadi, "Ensemble SW image steganalysis: A low dimension method for LSBR detection," *Signal Processing: Image Communication*, vol. 70, pp. 233–245, 2019.
[17] Y. Kang, F. Liu, C. Yang, L. Xiang, X. Luo *et al.,* "Color image steganalysis based on channel gradient correlation," *International Journal of Distributed Sensor Networks*, vol. 15, no. 5, pp. 1550147719852031, 2019.
[18] M. G. Gireeshan, D. D. Shankar and A. S. Azhakath, "Feature reduced blind steganalysis using DCT and spatial transform on JPEG images with and without cross validation using ensemble classifiers," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 5, pp. 5235–5244, 2021.
[19] T. S. Reinel, A. H. Brayan, B. O. Alejandro, M. R. Alejandro and A. G. Daniel, "GBRAS-Net: A convolutional neural network architecture for spatial image steganalysis," *IEEE Access*, vol. 9, no. 2, pp. 14340–14350, 2021.
[20] W. You, H. Zhang and X. Zhao, "A Siamese CNN for image steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 291–306, 2020.
[21] B. Singh, M. Chhajed, A. Sur and P. Mitra, "Steganalysis using learned denoising kernels," *Multimedia Tools and Applications*, vol. 80, no. 4, pp. 4903–4917, 2021.
[22] Z. Wang, M. Chen, Y. Yang, M. Lei and Z. Dong, "Joint multi-domain feature learning for image steganalysis based on CNN," *EURASIP Journal on Image and Video Processing*, vol. 2020, no. 1, pp. 1–12, 2020.
[23] S. Wu, S. Zhong and Y. Liu, "A novel convolutional neural network for image steganalysis with shared normalization," *IEEE Transactions on Multimedia*, vol. 22, no. 1, pp. 256–270, 2019.
[24] B. Singh, A. Sur and P. Mitra, "Steganalysis of digital images using deep fractal network," *IEEE Transactions on Computational Social Systems*, vol. 8, no. 3, pp. 599–606, 2021.
[25] G. Xie, "Adaptive spatial image steganography and steganalysis using perceptual modelling and machine learning," Ph.D. thesis, University of Strathclyde, UK, 2022.
[26] W. Ren, L. Zhai, J. Jia, L. Wang and L. Zhang, "Learning selection channels for image steganalysis in the spatial domain," *Neurocomputing*, vol. 401, pp. 78–90, 2020.