Soft Computing (2023) 27:13877–13888
https://doi.org/10.1007/s00500-023-09042-7

DATA ANALYTICS AND MACHINE LEARNING

Integrating machine learning and features extraction for practical reliable color images steganalysis classification

Ahd Aljarf[1] · Haneen Zamzami[2] · Adnan Gutub[2]

Accepted: 22 July 2023 / Published online: 8 August 2023

Abstract

Steganalysis is a known practice to detect hidden secrecy within covered e-media. Researches claimed obscured detection attainability via features extraction, as for perceiving concealed data within images. This paper verifies practicality of the claim by testing investigation of a steganalysis system that depicts the existence of hidden data focused on statistical features of color images using artificial neural network techniques. The proposed system is built to work for blind image steganalysis representing common security as looked for the most. The work experimentations adopted common steganography techniques to create the stego images for our intended steganalysis challenging practicality evaluation. The study involved machine learning radial basis function and naïve bayes classifiers to sort the remarks improving discovery accuracy. From the investigational results, the proposed system exemplified reliability and enhancements in the recognition rate for most steganographic methods showing attractive annotations. Further, the correlation features displayed increased correctness showing reliable convalescing practicality overcoming many previous steganalysis defects.

Keywords Image steganalysis · Stego image · Hidden data · RBF classifier · Features extraction · GLCM properties

1 Introduction

Steganography, cryptography, and watermarking are three methods that correlate and differ in characteristics. Steganography varies from cryptography as it relies on concealing the presence of a secret in a document, whereas cryptography focuses on scrambling the contents of a secret in a message (Gutub and Almehmadi 2022). Both steganography and cryptography are means of keeping knowledge hidden from prying eyes, but none is impenetrable (Zielińska et al. 2014). In the field of computer security, steganography is known as the science of embedding hidden data in a suitable cover item (Anderson and Petitcolas 1989). Stego is derived from the Greek word stegos which signifies "cover" and grafia represents "writing," making term "covered writing" as used to describe steganography (Duric et al. 2004). Generally, stego file holds hidden information while "clean files" or "carrier files" do not, preserving original e-media (Huayong et al. 2011), trying to avoid and traceability possibility (Singh et al. 2023).

In other words, to avoid eavesdropper suspicion, a steganographic system embeds secret content in unremarkable cover media (Provos et al. 2003). For hiding files in a cover object, researchers have implemented a number of steganography methods and tools (Gutub 2022). Multiple approaches and software support a variety of image formats and integrate hidden files using a variety of stego techniques (Gutub and Al-Qurashi 2020). On the other hand, steganalysis is described as the art of finding secret messages hidden by steganography and focuses on detecting hidden data. Steganalysis is commonly used in computer forensics and electronic security for internet monitoring of illegal activity. Steganalysis also aids in

✉ Adnan Gutub
aagutub@uqu.edu.sa

Ahd Aljarf
amjarf@uqu.edu.sa

Haneen Zamzami
Haneen.Zamzami@gmail.com

[1] Information System Department, Umm Al-Qura University, Mecca, Saudi Arabia

[2] Computer Engineering Department, Umm Al-Qura University, Mecca, Saudi Arabia

improvement of steganographic protection by identifying and remarking weaknesses (Johnson and Jajodia 1998).

For our security reasons, images are generally used as carriers for sensitive data, as their modifications are likely unnoticeable. This research focused on JPEG and BMP color images with various steganographic algorithms correlated to variations of images forms (Morkel et al. 2005). Any computer image file can be built as sequence of dots, known as pixels, arranged in horizontal continuous rows. Each pixel has a distinct hue which is revealed in the image data as red, green, and blue (RGB) in a specific and separate manner. To hide secret data, steganography schemes use variety of algorithms such as blin hide, hide seek, filter first, battle Steg, jsteg, ouguess, F3, F4, and F5, to employ least significant bit LSB steganography and to filter images, as comparatively currently researched differently in Aljarf et al. 2023. Interestingly, jsteg, F3, F4, and F5 algorithms act by embedding hidden data in transform coefficients that satisfy both imperceptibility and robustness requirements (Umamaheswari et al. 2010). However, LSB-based steganography is well-known for concealing huge hidden files in cover images without causing noticeable distortions as allowing high concealing capacity (Thangadurai and Devi 2014). It functions by substituting the hidden data bits for the LSBs of randomly chosen pixels in the cover image. A hidden key, or password, can be used to decide which pixels are selected for this obscurity (Gutub and Al-Roithy 2021).

This paper studies the effectiveness argument of utilizing features extraction for blind color image steganalysis via advancements of machine learning technology benefitting from Sufi et al. 2023. The main idea is to help represent a detection system that can assist our usage of blind steganalysis, i.e., not targeted to specific stego methods or image formats. The suggested approach is based on extracting statistical features integrated with machine learning for proper classification. The image processing and feature extraction were all implemented using MATLAB 2021b and statistically analyzed via SPSS. The work tested the detection system anticipation for its ability to distinguish between many types of stego images created by LSB stego algorithms. The investigation involved radial basis function (RBF) technique and naïve bayes, known as major machine learning (ML) binary classifiers, i.e., showing RBF to display high detection accuracy, as stimulating research contribution.

The paper presentation started by Sect. 2 discussing related work building our study background. Then, Sect. 3 covered the proposed steganalysis system divided into three consecutive stages of preparation (clean and LSB stego) images, extracting the features followed by ML classifiers. Section 4 revealed the different experimentation testing and implementation results followed by Sect. 5 representing all tryouts involving both machine learning classifications of RBF and naïve bayes. Finally, Sect. 6 concludes the research.

2 Related work

In order to study if feature-based classifications and advanced ML can be effective in image steganalysis, several related techniques and algorithms (as relevant image processing) have been reviewed, ensuing stego revision in Thabit et al. 2022. This related work section further provides some discussion of the benefits and drawbacks linked to the previous steganalysis studies. For example, Zhang and Ping (2003) presented techniques that illustrated grayscale images based on the histogram of different images. The substandard association between LSB plane and the remaining bit planes was measured by using the translation coefficient between different pictures histograms. The aforementioned measurement was then utilized to build a classifier that distinguishes stego images from clean images, remarking embedding rates of 10% increments with an average detection rate of 96.3% at the top. The proposed technique performed better than RS analysis in terms of performance and calculation speed for both sequential and random LSB replacements (Zhang and Xijian 2003). Various tests and outcomes were based on the embedding ratio. The new technique illustrated similar results to the RS analysis approach for images recorded in JPEG format, as well as any image of small size, unlike ML analysis work of Roy et al. 2023.

Similarly, Sun et al. (2008) proposed the co-occurrence matrix-based steganalysis approach to create three-directional differential images for natural images. Authors estimated the forward difference in three directions (horizontal, vertical, and diagonal) toward adjacent pixels to remove redundant data, the differential images are set to threshold with pre-determined beginning. Furthermore, for steganalysis, the co-occurrence matrices of thresholder differential images were employed as features. Different tests were performed depending on the payload (0.1–0.3 bpp) to distinguish between stego and cover images since an SVM with RBF kernel was utilized as a classifier. This approach works well with steganographic schemes in the spatial domain (Sun et al. 2008). Additionally, as the dimension of the suggested method feature vector was fairly large, the BMP format supported by this method, and all images were small in size.

Relatively, Kekre et al. (2011) suggested a steganalysis technique for both grayscale and color images. In the spatial domain, feature vectors obtained from the gray level co-occurrence matrix GLCM, distance measurements, and Euclidean distance, were used for classification. Presented steganalysis method used features extracted from an image's co-occurrence matrix as the results illustrated that Euclidean distance noted high achievability. According to the authors, color image detection accuracy was roughly 18% higher than grayscale image detection accuracy, and low embedding rates are found to be superior (Kekre et al. 2011). It is worth mentioning that only BMP images were supported in this study.

In another research, Verma (2014) utilized multilayer perceptron with backpropagation for image classification. The researcher also used PVDBPA (Pre-processed Vectors Diagonal Back-Propagation Algorithm) to detect the presence of hidden data. Furthermore, BMP steganalysis utilizing gray level co-occurrence matrix was investigated using feature vectors and tested by Euclidean distance measurement (Verma 2014).

In a similar study, Hemalatha et al. (2023) presented how the gray level co-occurrence matrix can be used for 3D seismic data imaging. As for attribute analysis, GLCM demonstrated valuable insight into the subsurface, different than critical deep learning impact analysis (Gutub et al. 2022). Moreover, GLCM has been proven valuable for describing seismic facies by number of authors. GLCM-based qualities were implemented to determine directional differences in seismic data, as it is calculated in multiple directions. This allowed for the distinction of sedimentary facies and fracturing patterns, as well as the delineation of fractured zones strike and dip (Eichkitz et al. 2015).

According to Al-Taie (2017) study, steganalysis model can be expanded via GLCM feature set. The results illustrated that a huge number of grayscale images from public sources were evaluated and included showing discriminant analysis of two-category classifier applicability, though only BMP images were used (Al-Taie 2017). Rasool et al. (2018) adopted statistical textural features based on aspects of grayscale 8-bit pictures. The article runs steganalysis model analysis to identify the existence of hidden data inside uncompressed RGB color photographs, which can be analyzed similar to engineering trust study of Kheshaifaty and Gutub (2021). The selected features were retrieved from clean and stego picture datasets using support vector machine technique to classify them (Rasool et al. 2018).

Lately, Shniperov (2019) developed an artificial immune system for detecting hidden information in JPEG images which detects hidden information with decent image processing time and with adequate precision. The proposed method detected existence of secret information embedded by various common stego tools enjoying sufficient efficiency revealing secrets from JPEG images. However, the work timing consumed master artificial immune system in defecting manner (Shniperov and Prokofieva 2019).

Likewise, Jin et al. (2020) suggested an adaptive scale adjustment-based feature extraction approach for JPEG steganalysis, not like alignment threading technology presented in Abu-Hashem et al. 2022. Jin works that magnitude of feature extraction technique was modified adaptively based on the quality of JPEG images primarily using the Boss Base 1.01 database, which was based on the MD-CFR feature. According to the results, the proposed strategy increased the performance of the steganalysis as reduced the dimensionality of retrieved features, allowing it to be employed in other steganalysis methods based on residual images but can be generalized for all (Jin et al. 2020). Therefore, Shankar (2021) illustrated JPEG format steganalysis on pictures with 10% embedding and tenfold cross-validation. The calibration approach was used to get approximation of cover image matching LSB replacement, pixel value differencing (PVD), and F5 approaches, as different embedding testing strategies (Shankar 2021). In fact, Shankar's research work benefitted from vector machine (SVM) and swarm optimization (SVM-PSO) as smartly used classifiers igniting our work deep understanding and comparison investigations to be in state-of-the-art condition.

3 Proposed system method

The proposed system studied practicality of blind image steganalysis using feature-based classification as clarified in three stages, as shown in Fig. 1, following principle philosophy of Aljarf et al. 2023 in completely different way than all discrepancies of remote techno-tolerance categorizations presented in Abu-Hashem et al. 2023. The work process stage one demonstrates image database which includes clean and stego images created with LSB steganography to train and test the proposed system adopting same standard text stego works in Roslan et al. 2022. Stage two focuses on extracting the features for the purpose of detection. Lastly, stage three classifies results

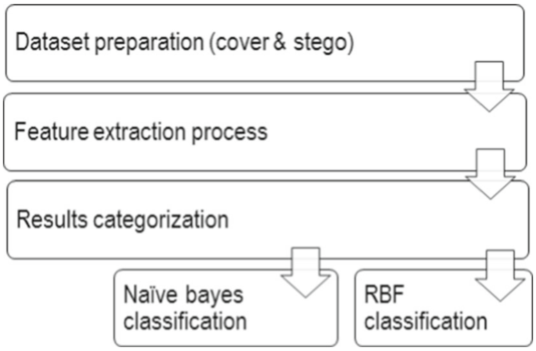

Dataset preparation (cover & stego)
Feature extraction process
Results categorization
Naïve bayes classification
RBF classification

Fig. 1 Process of proposed steganalysis system

using two classification methods: radial basis function classification and naïve bayes classifier for training and testing, as elaborated benefitting from the IoT study of AI-based computing (Singh et al. 2022).

The process testing dataset contains two image databases, as listed in Table 1. First database includes 600 standard test JPEG images with stego versions. Second database also included 600 test images with stego versions but in BMP format. Due to the accessibility of raw photos straight from cameras, this research preferred usage of well-defined images from PhD Thesis (Aljarf 2016) whom authors shared generously for this paper work. Figure 2 shows samples of the dataset material used in this testing steganalysis investigation.

Steganography research has been traditionally employed by LSB-based data hiding within the spatial domain. This case is assumed because the lowest bit plane of bitmap images is normally used to send/retrieve hidden data. The reason behind all that is its undetectability by naked eye to be noticed, as change is very little in negligible parts of an image (Fridrich et al. 2001). Additionally, the LSB steganography method is basic and well-known approach for hiding bigger amounts of secret information in covers pretending high practicality (Hussain et al. 2018). The aforementioned method operates by substituting secret message bits for the LSBs of randomly chosen or selected pixels in the cover image. A stego key can determine the order of embedding or the selection of pixels. Besides, LSB approach is defined by leaving the fewest number of indicators which is achieved by modifying the plain LSB of a cover image, hiding the major significant bits, and leaving the statistical features of the cover image mainly unaffected. It is to be mentioned that the LSB-based technique is effective when only a few of the cover image's LSB bits are changed, because it is impossible to notice the difference between the cover image and the stego image (Raja et al. 2005).

Replacement and matching are two types of LSB techniques. The classified information in binary form is considered in the LSB replacement. More specifically, this approach replaces the image's LSB bit plane with the message's equivalent bits. This can be applied to all of the pixels in an image or only to a specific area of the image that has been selected randomly. When the rate of embedding is less than unity, and the image's pixel count is more than the concealed message's length, and selective replacement is used. This approach is stated to be asymmetric in nature which can be used in several privacy studies for feature evaluation (Shambour and Gutub 2021). On the other hand, the quantity is lowered by one for odd pixel measurements. This method has been called LSB matching and has been demonstrated to be effective for grayscale images (Shankar 2021). LSB matching can be considered as a modified kind of LSB steganography. The pixel value is maintained fixed if LSB of the cover pixel matches the secret bit; otherwise, it is added or removed by 1 randomly. Each tool has its unique set of capabilities. S-Tool, for instance, decreases the number of colors in an image to 32. Hide and seek, on the other hand, operates by dividing all palette elements by four (Ming and Ru 2006).

Table 1 Steganography methods testing number of images and format

Analysis	Database 1	Database 2
Format of images	JPG	BMP
Number of clean images	300	300
Number of stego images	300	300
Original images size range	201 KB–1244 KB	126 KB–1836 KB
Steganography algorithms	F5	LSB
Size range after embedding	103 KB–1754 KB	442 KB–2563 KB

The process of feature extraction is extremely important due to its diverse features of natural images and steganography approaches. Feature extraction is a method for extracting new features from an original dataset that is highly useful to reduce the number of resources required for processing. Moreover, feature extraction is used to reduce the number of extra characteristics in a study and transforms basic features into more significant features. Additionally, as the high dimensionality of the feature vector is reduced, new features that rely on the original input feature set were constructed. The transformation is carried through using algebraic transformation and optimization criteria. In addition, while dealing with high-dimensional challenges, feature extraction is used to manage critical information by preserving the original relative distance between features and covering the original data potential structure. Dimensionality reduction strategies are utilized to avoid losing considerable amount of information during the feature transformation process (Zebari 2020). Therefore, selected features are extracted from each image of clean and stego images to run our process. The features used are mean, standard deviation, entropy, RMS (root-mean-square), and variance, as formularized next.

Mean computes the average value of matrix elements: Mean $(f_1) = \sum_{i,j=0}^{N-1} i p_{ij}$

Standard deviation $\sigma_i = \sqrt{\sigma_i^2}$, $\sigma_j = \sqrt{\sigma_j^2}$. However, homogeneous scene has high entropy while inhomogeneous scenes have a low first-order entropy. Maximum entropy is reached when all probabilities are equal. Entropy $(f_2) = \sum_i \sum_j p(i,j) \log(p(i,j))$

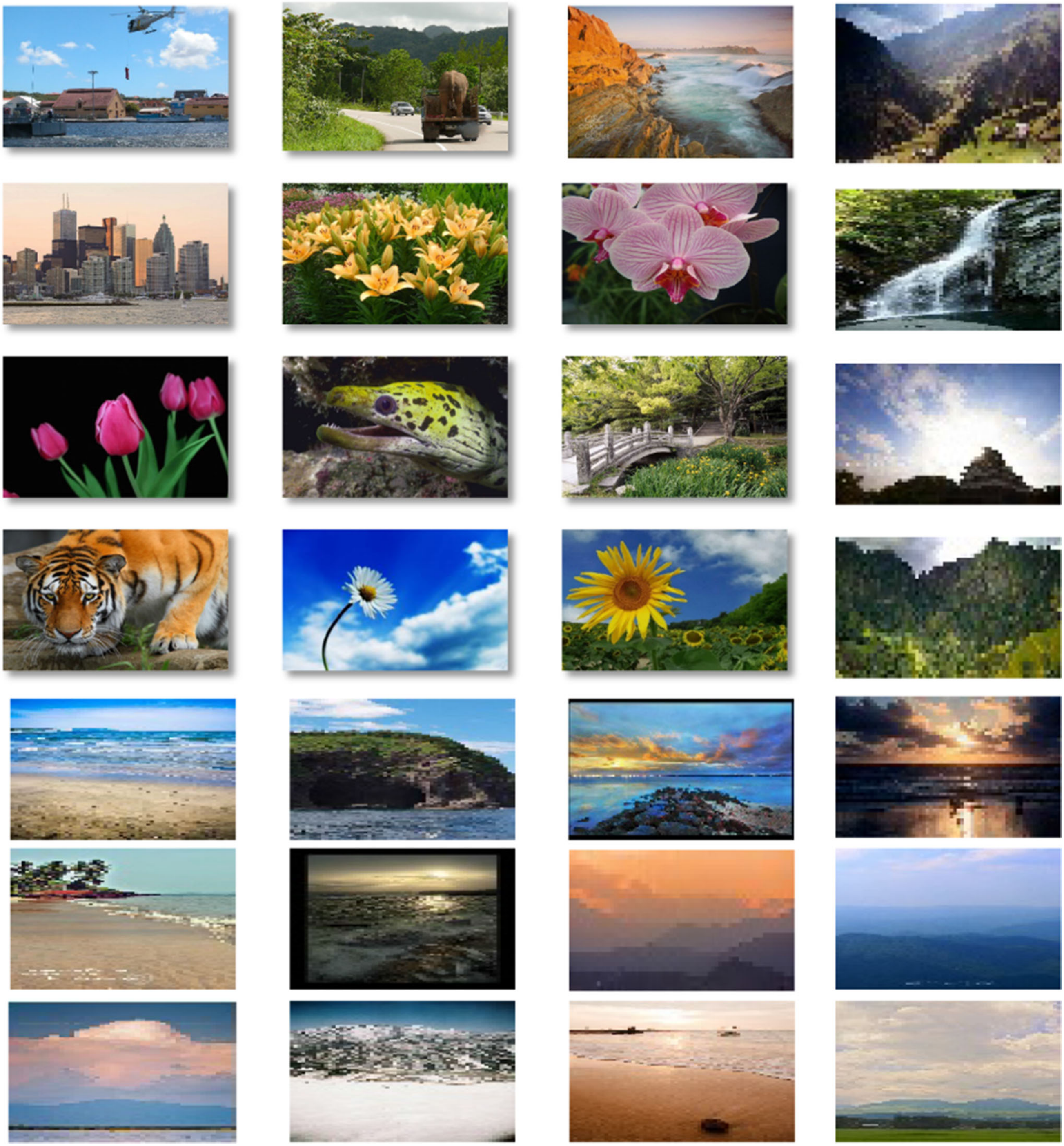


Fig. 2 Sample of database set images

RMS (root-mean-square) = $\sqrt{\frac{1}{N}\sum_{n=1}^{N}|x_n|^2}$. Variance is measure of how far a set of numbers is spread out. It is one of several descriptors of probability distribution, describing how far the numbers lie from the mean. Variance (f_3) = $\sum_i \sum_j (i-\mu)^2$ p (i,j)

The following pseudo-code shows the proposed steganalysis procedure flow main idea:

```
1. Load images from source file
2. Read image
3. Select specific color channel (red or blue or green)
4. Extract mean features
5. Extract standard deviation features
6. Extract entropy features
7. Extract RMS features
8. Extract variance features
```

9. Save the result in Excel sheet
10. End

The proposed organization used two different classification methods to test, train, and validate the system. The sample MATLAB code tuned to extract GLCM features is represented as below:

```
scrFile=dir('C:\Users\s4320\OneDrive\grayImages\jpg\stego1\*.jpg');
for i=1:length(scrFile)
                x=(scrFile(i).name);
      filename=strcat('C:\Users\s4320\OneDrive\grayImages\jpg\stego1',x);
      I=imread(x)
      file=convertCharsToStrings(x);
   gray=rgb2gray(I);
glcm=graycomatrix(gray);
F=graycoprops(glcm,{'Energy', 'Contrast', 'Homogeneity', 'Correlation',});
contrast=F.Contrast;
homogeneity=F.Homogeneity;
correlation=F. Correlation;
energy=F.energy;
data=[file,energy,contrast,homogeneity,correlation];
disp(data);
writematrix(data, 'new-jpg.xlsx','WriteMode','append')
end
```

This sample MATLAB routine extracts GLCM features: energy, contrast, homogeneity, and correlation, as were used in this experiment. The RBF binary classifier was used in the classification process. A comparison was made by using the naïve bayes classifier, which is also used in steganalysis experimental work. Implementation of the proposed model used the RBF, and naïve bayes classifiers are utilized from available SPSS libraries, as interfaces shown in Figs. 3 and 4, respectively.

Note that RBF is a mathematical concept that describes both strong points of neural networks marking pattern categorization and function fitting. Furthermore, three-layer forward network and input layer with the same number of nodes as the input dimension were used. The concealed layer has the exact equivalent quantity of nodes as the input dimension; and the transmission layer has the identical number of nodes as the input dimension. The dimension of output data is equal to the number of nodes in the layer, as the roles of the various levels of the RBF neural network were varied, and nonlinearity was in the hidden layer. The RBF function was utilized as the basis function to translate the input vector space into the hidden layer space, resulting in a linear inseparable problem and a linear output layer (Sun et al. 2019).

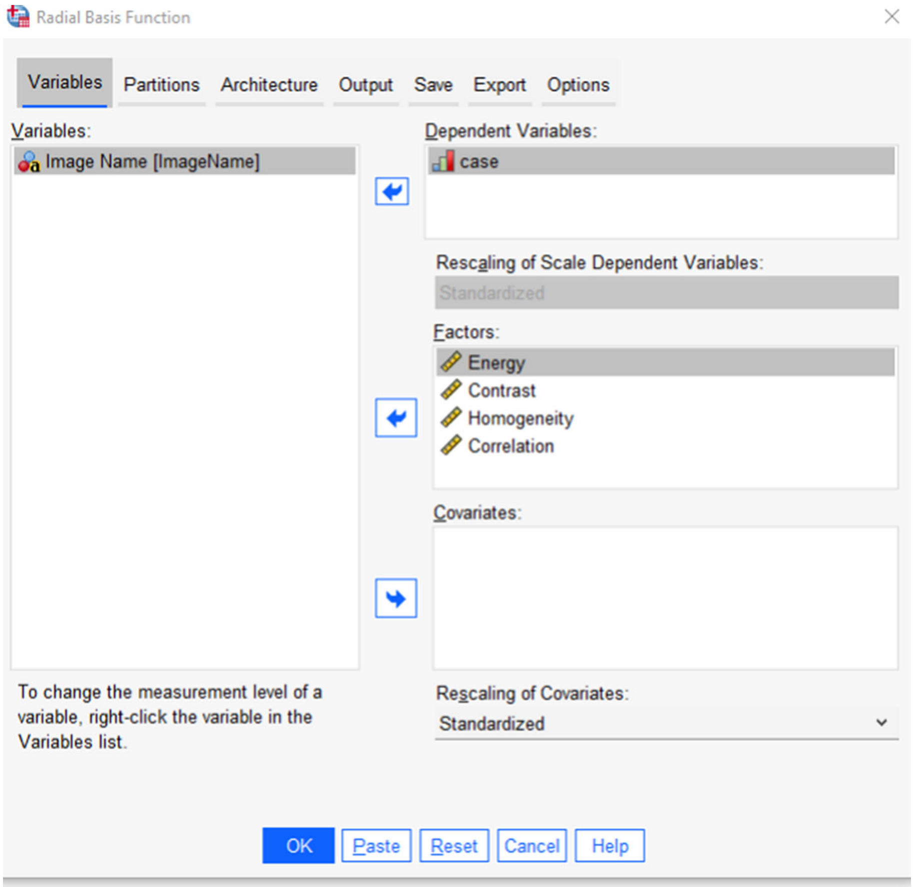
This classification strategy is based on bayes theorem and the assumption of predictor independence. In simple terms, a naïve bayes classifier assumes that the existence of one feature in a class has no bearing on the presence of subsequent features. The naïve bayes model is simple to construct, particularly useful for huge datasets, and renowned to outperform even the most advanced classification systems. The naïve bayes algorithm is a simple probability classifier which determines a set of probabilities by counting the frequency and combinations of values in a dataset. When assessing the value of the class variable, the algorithm employs bayes theorem and assumes that all variables are independent. Although this conditional independence assumption is rarely valid in practical applications, the algorithm learns swiftly in a variety of controlled classification situations (Saritas and Yasar 2019).

4 Experimental results

The effectiveness of the suggested strategy and its outcomes have been investigated via five experimentations strategies shown in Fig. 5.

The effect of images format BMP/JPG was tested. The consequence of features extraction has been confirmed extensively, the merging of features also has been considered, the outcome of the color channel (red, green, and blue), and adding new features to enhance our system accuracy, all have been remarking the implementation results contribution.

Note that the RGB channels turn the eight features into 24 predictors, as involved within the process graphically shown in Fig. 6. The red, green, and blue channels are used to separate the results. Furthermore, each of them is



Variables:
Image Name [ImageName]

Dependent Variables:
case

Rescaling of Scale Dependent Variables:
Standardized

Factors:
Energy
Contrast
Homogeneity
Correlation

Covariates:

To change the measurement level of a variable, right-click the variable in the Variables list.

Rescaling of Covariates:
Standardized

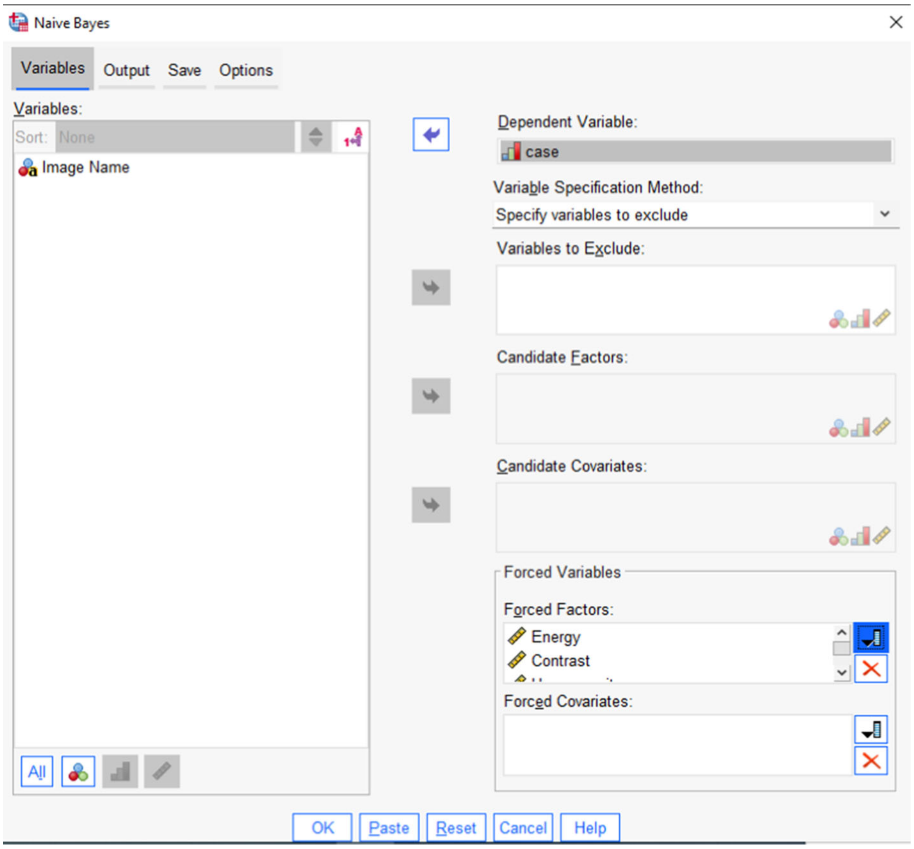
Fig. 3 User interface of the RBF in SPSS

regarded as a separate predictor. The findings are then collected and sorted into various Excel sheets. These sheets are categorized based on the color channel, image type, and whether they are clean or stego. The RBF and NB classes are then implemented in IBM SPSS statistics version 28.0 to train and test the system. All Excel sheets are then imported. Following the implementation of the two classifiers, the expected system's accuracy is discovered.

To analyze the practicality philosophy of adopting feature-based classification for our blind image steganalysis, this experiment tested 600 clean images with 600 stego images (1200 in total) running different BMP/JPG format considerations. The work analysis involved 15 features (Variance_Blue, Variance_Green, Variance_Red, RMS_Blue, RMS_Green, RMS_Red, Entropy_Blue, Entropy_Green, Entropy_Red, Standard_Deviation_Blue, Standard_Deviation_Green, Standard_Deviation_Red, Mean_Blue, Mean_Green, and Mean_Red) to gain fair investigation. The effect of features extraction has been confirmed extensively, as the merging of features also has been considered via adding new features, i.e., to enhance our system accuracy.

To be specific, Table 2 lists the different testing effects of images format BMP and JPG individually in all experimentations. For example, experiment 1(a) BMP format showed the overall percentage of testing as 91.7% sets for RBF, which was greater than that of naive bayes classifier representing 86.5% sets. Differently, experiment 1(b) JPG format gave RBF and naïve bayes classifiers performance relatively equally predicted as an overall accuracy rate of 85.7% and 84.2%, respectively.

On the other hand, experiment 2 tests the effect of features extraction individually, as experiment 2(a) remarks mean for all images with overall accuracy percentage of RBF classifier reached 100% while naïve bayes classifier reached an overall prediction rate of 88.9%. Relatively, experiment 2(b) Standard_Deviation notation for all images in the testing set gave the RBF classifier an overall accuracy percentage approaching 100% while naïve bayes classifier reached 91.7% overall prediction rate. Likewise, experiment 2(c) of entropy testing samples the RBF classifier displaying an overall accuracy of 100% while naïve bayes classifier reached only 78.1%. In a different way, experiment 2(d) RMS estimation of running the testing set indicates that the RBF classifier displayed a poor



Variables:
Sort: None
Image Name

Dependent Variable: case

Variable Specification Method: Specify variables to exclude

Variables to Exclude:

Candidate Factors:

Candidate Covariates:

Forced Variables

Forced Factors:
Energy
Contrast

Forced Covariates:

Fig. 4 User interface of the naïve bayes in SPSS

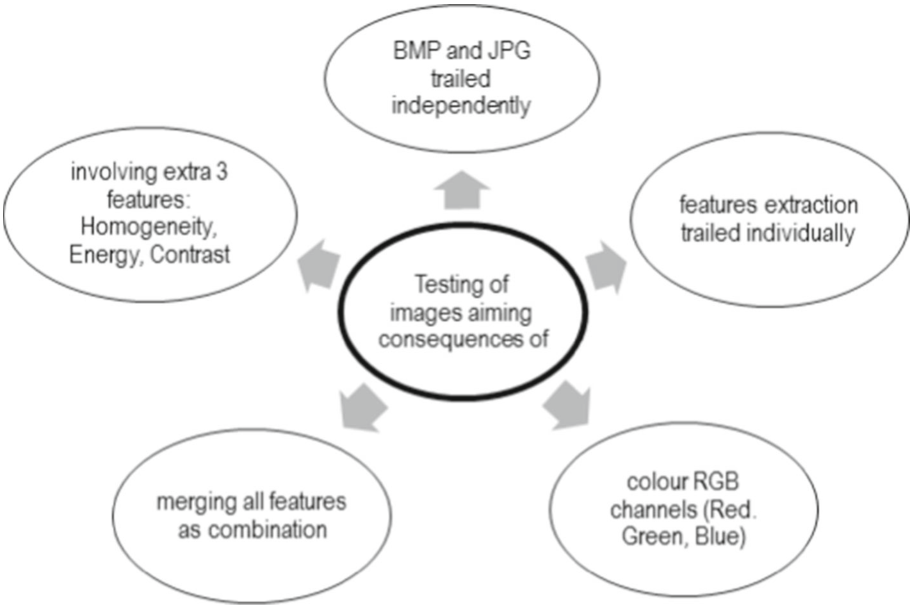

BMP and JPG trailed independently
features extraction trailed individually
colour RGB channels (Red. Green, Blue)
merging all features as combination
involving extra 3 features: Homogeneity, Energy, Contrast
Testing of images aiming consequences of

Fig. 5 Research color images different experimentations

overall performance of 62.1% while naïve bayes classifier displayed an enhanced overall rate of 80.5%. However, experiment 2(e) variance measured the RBF classifier displaying an overall accuracy of 100% while naïve bayes classifier reached 85.9%, as matching feature to most other testing representations.

Similarly, experiment 3 is testing the effect of color channels of images (red, blue, and green) providing interesting remarks. For example, experiment 3(a) tests the effect of merging the red channel for all features showing the overall accuracy percentage of RBF classifier around 100% while naïve bayes classifier almost 82.2%.

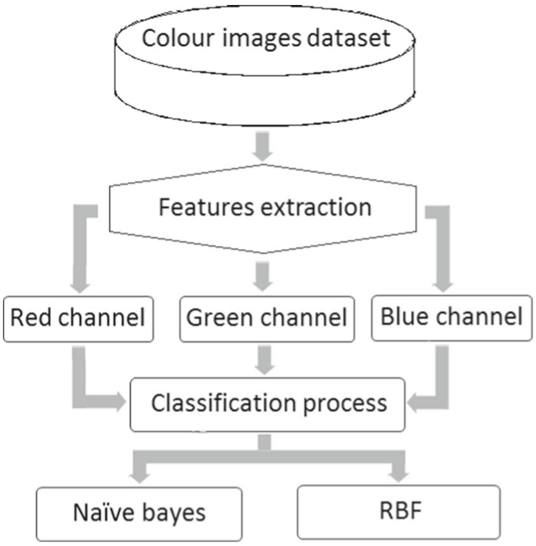


Fig. 6 The RGB channels predictors classification process

Experiment 3(b) tests the effect of merging the green channel for all features exposing accuracy percentage of RBF classifier reached 100% while naïve bayes classifier touched 81.6%. Experiment 3(c) tests the effect of merging the blue channel for all features providing analogous RBF classifier reaching 100% while naïve bayes classifier rating 83.7%.

Differently, experiment 4 presents merging all features of BMP/JPG format with RBG colors channels. Experiment 4(a) merges entropy, standard deviation, mean, and variance, representing the overall accuracy percentage of RBF classifier as 93.3% while naïve bayes classifier as 71.2%. Experiment 4(b) combines slightly different features of mean, standard deviation, entropy, RMS, and variance, presenting unlike overall accuracy percentage of RBF classifier as 83.3% while naïve bayes classifier rating 81.3%.

The work involved integrating new features: homogeneity, energy, and contrast, presented as experiment 5. This experiment 5 noted the overall accuracy percentage of RBF classifier almost 100% while naïve bayes classifier approaching 97.3%. To be focused in our observation, i.e., correlating the naive bayes classifier with the prediction percentage of the RBF classifier, the RBF remarks were noticeably showing the mostly higher performance.

5 Analysis and comparisons

As indicated before, Table 2 overall results of percentages achieved by the RBF is commenting to be higher than naive bayes classification methods for almost all experimentations, i.e., during the training and testing phases. The general results also showed that the BMP images format performed frequently better than the JPG images format, as for both classifications. In terms of features, the RMS feature was found to achieve the lowest accuracy with the RBF classifier, while entropy feature achieved the lowest accuracy with the naive bayes classifier. Furthermore, the study demonstrated that merging single color channel of features does not influence any of the results for both

Table 2 Experimentations results

Experiment	Radial basis function	Naive bayes		
	Training (%)	Testing (%)	Training (%)	Testing (%)
Experiment 1(a): BMP format only	87.3	91.7	100	86.5
Experiment 1(b): JPG format only	85.7	85.7	100	84.2
Experiment 2(a): Mean—all images	100	100	100	88.9
Experiment 2(b): Standard_Deviation—all images	100	100	100	91.7
Experiment 2(c): Entropy—all images	100	100	100	78.1
Experiment 2(d): RMS—all images	58.7	62.1	97.9	80.5
Experiment 2(e): Variance—all images	100	100	100	85.9
Experiment 3(a): Test effect of merging red channel for all features	100.0	100.0	100	82.2
Experiment 3(b): Test effect of merging green channel for all features	100.0	100.0	100	81.6
Experiment 3(c): Test effect of merging blue channel for all features	100.0	100.0	100	83.7
Experiment 4(a): Merging (entropy, Standard_Deviation, mean, and variance)	100	93.3	100	71.2
Experiment 4(b): Merging all features (mean, standard deviation, entropy, RMS, and variance)	84.2	83.3	100	81.3
Experiment 5: Adding new features (homogeneity, energy, and contrast)	81.5	100	100	97.3

Table 3 Comparison with the previous works

	Accuracy	Dataset	Texture features	Classifier
Kunal (2010)	91%	105 images downloaded from various websites	GLCM	Not reported
Qin (2014)	83%	public dataset of grayscale images	GLCM	Ensemble classifiers
Kumar (2016)	–	publicly available MRI images in grayscale	GLCM and shape features	Not reported
Lin (2016)	94%	public dataset of grayscale images	LBP	Ensemble classifiers
Jyothy (2019)	93%	not reported	GLCM, DWT, and CT	Ada-boost
Hammad (2022)	90%	Public dataset of color images	SFTA	GDA
Our proposal	97%	BMP and JPEG images format used for color images	GLCM and RMS	RBF with naïve bayes

Table 4 Area under the curve performance classification evaluation

	Image type	Number of features	Area under the curve
Lin (2016)	Color	48	0.8022
Dong (2008)	Gray	36	0.618
Aljarf (2016)	Gray	70	0.916
Our proposal	Color	24	0.961

classifications. The results were all better accumulating GLCM features of homogeneity, contrast, and energy, rather preferred among merging the other features of mean, standard deviation, entropy, RMS, and variance.

The proposed method is further compared to others in order to assess its performance practicality. All other works focused on one type of images to detect stego secrecy while we run on multi-types of images. The extraction of texture features is the main element of these image steganalysis classification algorithms to be considered. Several works did not report the classifiers adopted, such as Kunal (2010) and Kumar (2016), but others mentioned some info though not being very useful as ensemble classifiers (Kumar and Vs 2016). The proposed approach is further compared with existing methods relying on feature-based steganalysis as presented in Table 3. The comparison shows that the proposed method outperforms current state-of-the-art methods in terms of classification rates.

Furthermore, our work classifier is evaluated via area under the curve (AUC) performance approximation, as listed in Table 4. The AUC is often used to quantify categorizers' functions in binary classification. According to Fawcett (2004), the AUC is calculated to quantify the function of the network and classifies the operation optimization to indicate the chance that an unsystematically chosen advantageous event is assigned a higher value than an unsystematically chosen unfavorable event. This strategy has been shown to be very helpful for evaluating categorizers, especially when allocated categories are overly unequal. In fact, as mentioned earlier, AUC is useful for gaining access to categorizers' functionality, and the AUC is also resistant to category dispersion as our work is showing interesting results worth remarking as promising steganalysis approach.

6 Conclusions

This paper evaluated the steganalysis system based on gray level co-occurrence matrix features extraction to verify its practicality for blind image steganalysis. The research runs four experiments conducted to test the effectiveness of different stego images. During the examination, some experiments showed that all features demonstrated sophisticated performance using RBF classifier, except RMS compared to the other classifier. Interestingly, standard deviation feature achieved higher results using naive bayes classifier but still have not been highest significant. However, after adding new features together with common ones, the remarks analysis further experimentations revealed dramatical increase in the accuracies of the proposed steganalysis system making the work opening new research path directions. Accordingly, the tryouts proved that the extracted features were very sufficient in order to distinguish between clean and stego images. It demonstrated that the features extraction process is still one of the appropriate effective methods for blind secrecy detection within images.

Although the discussed results of the proposed method displayed an improvement in the detection rate for some steganographic methods, it is recommended for future research to examine more stego images aiming to reveal other features and to seek extra in depth steganalysis estimations. In addition, testing other types of color images with different classifiers may be usefully conducted to show practical reliability and further advance stego secrecy works. This current approach assessments are hard to compare with others because of the used specialized images dataset. Upcoming stirred practice can use public datasets to help other scientists reproduce the research and propose further improvement strategies. Also, the upcoming analysis can be planned to incorporate different stego methods besides the dissimilar image formats aiming to seek its steganalysis validity against sophisticated hiding methods. Lastly, the work can be further developed involving the steganalysis timing and process delay especially as advanced image processing techniques are getting more and more tangled to human lives.

Acknowledgements The authors would like to express their gratitude toward Umm Al-Qura University (UQU), Saudi Arabia, for the support of this study. The authors declare that this work is original and is not considered to be published in any other publication media.

Funding Authors herby that this work received no external funding.

Data availability Data sharing not applicable—no new data generated.

Declarations

Conflict of interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Ethical approval The authors declare that the article does not contain any studies involve human participants or/and animals.

Informed consent Authors herby that informed consent was obtained from all individual participants involved in the study.

References

Abu-Hashem M et al (2022) Efficient computation of Hash Hirschberg protein alignment utilizing hyper threading multicore sharing technology. CAAI Transact Intell Technol 7(2):278–291

Abu-Hashem M et al. (2023) Discrepancies of remote technotolerance due to COVID-19 pandemic within Arab middle-east countries. J Umm Al-Qura Univ Eng Archit. Springer. in press. https://doi.org/10.1007/s43995-023-00026-0

Aljarf A (2016) Development of a detection system for colour steganographic images based on extraction of colour gradient co-occurrence matrix features and histogram of difference image, PhD Thesis from Computer Sciences at Coventry University, UK.

Aljarf A et al. (2023). Is blind image steganalysis practical using feature-based classification?. Multimedia tools and applications (MTAP), in press. https://doi.org/10.1007/s11042-023-15682-6

Al-Taie Z (2017) Statistical steganalysis detector model for 8-bit depth images. Unpublished master thesis, Middle East University, Amman, Jordan.

Anderson R, Petitcolas F (1989) On the limits of steganography. IEEE J Sel Areas Commun 16(4):474–481

Dong J, and Tan T 2008 Blind image steganalysis based on run-length histogram analysis. IEEE International conference on image processing, pp. 2064–2067, San Diego, CA, USA. https://doi.org/10.1109/ICIP.2008.4712192

Duric Z, Jacobs M and Jajodia S (2004). Information hiding: steganography and steganalysis. Preprint Submitted to Elsevier Science.

Eichkitz C et al. (2015). Grey level co-occurrence matrix and its application to seismic data. First break. 33(3).

Fawcett T (2004) ROC graphs: notes and practical considerations for researchers. Mach Learn 31(1):1–38

Fridrich J, Goljan M and Du R (2001). Reliable detection of LSB steganography in grayscale and color images. Proceeding of ACM, special session on multimedia security and watermarking, Ottawa, Canada, pp. 27–30.

Gutub A, Al-Qurashi A (2020) Secure shares generation via M-blocks partitioning for counting-based secret sharing. J Eng Res (JER) 8(3):91–117

Gutub A, Al-Roithy B (2021) Varying PRNG to improve image cryptography implementation. J Eng Res 9(3A):153–183

Gutub A, Almehmadi E (2022) Arabic text watermarking tuned for medical e-record semi-authentication. J Eng Res. https://doi.org/10.36909/jer.18943

Gutub A, Shambour M, Abu-Hashem M (2022) Coronavirus impact on human feelings during 2021 hajj season via deep learning critical twitter analysis. J Eng Res (JER). https://doi.org/10.3690/jer.19493

Gutub A (2022) Dynamic smart random preference for higher medical image confidentiality. J Eng Res. https://doi.org/10.3690/jer.17853

Hammad B, Ahmed I, Jamil N (2022) A steganalysis classification algorithm based on distinctive texture features. Symmetry 14(2):236. https://doi.org/10.3390/sym14020236

Hemalatha J et al (2023) Towards improving the performance of blind image steganalyzer using third-order SPAM features and ensemble classifier. J Inf Secur Appl 76:103541. https://doi.org/10.1016/j.jisa.2023.103541

Hossain K and Parekh R (2010) Extending GLCM to include color information for texture recognition. Am Inst Phys (AIP) Conf Proc. 1298(1).

Huayong G, Mingshenge H and Qiana W (2011) Steganography and steganalysis based on digital image. International congress on image and signal processing, Shanghai, China.

Hussain M, Abdul-Wahab A, Idris Y, Ho A, Ki-Hyun J (2018) Image steganography in spatial domain: a survey. Signal Process Image Commun 65:46–66

Jin Z, Feng G, Ren Y, Zhang X (2020) Feature extraction optimization of JPEG steganalysis based on residual images. Signal Process 170:107455

Johnson N, Jajodia S (1998) Exploring steganography: seeing the unseen. Computer 31(2):26–34

Jyothy T, Sreelatha G, Pradeep R and Sajith V (2019). Texture-based multiresolution steganalytic features for spatial image steganography. International conference on smart systems and inventive technology (ICSSIT), Tirunelveli, India, pp. 966–971.

Kekre H, Athawale A, Patki S (2011) Steganalysis of LSB embedded images using gray level co-occurrence matrix. Int J Image Process (IJIP) 5(1):36

Kheshaifaty N, Gutub A (2021) Engineering graphical captcha and AES crypto hash functions for secure online authentication. J Eng Res. https://doi.org/10.36909/jer.13761

Kumar P, Vs D (2016) Extraction of texture features using GLCM and shape features using connected regions. Int J Eng Technol 8(6):2926–2930

Kunal H, Parekh R (2010) Extending GLCM to include color information for texture recognition. AIP Conf Proc 1298:583. https://doi.org/10.1063/1.3516370

Lin Q, Liu J and Guo Z (2016). Local ternary pattern based on path integral for steganalysis. IEEE international conference on image processing (ICIP), Phoenix, AZ, USA, pp. 2737–2741.

Ming C and Ru Z (2006). Analysis of current steganography tools: Classifications and features. Int Conf Intell Inform Hiding Multimed Signal Process.

Morkel T, Eloff J and Olivier M (2005). An overview of image steganography. ISSA. 1(2).

Provos N, Honeyman P (2003) Hide and seek: an introduction to steganography. IEEE Secur Priv 1(3):32–44

Qin J, Xiang X, Deng Y, Li Y, Pan L (2014) Steganalysis of highly undetectable steganography using convolution filtering. Inf Technol J 13:2588

Raja K, Chowdary C, Venugopal K and Patnaik L (2005). A secure image steganography using LSB, DCT and compression techniques on raw images. IEEE Int Conf Intell Sens Inform Process, pp. 170–176.

Rasool Z, Al-Jarrah M, Amin S (2018) Steganalysis of RGB images using merged statistical features of color channels. Int Conf Dev eSyst Eng (DeSE). https://doi.org/10.1109/DeSE.2018.00048

Roslan NA et al (2022) Systematic literature review and analysis for Arabic text steganography method practically. Egypt Inform J 23(4):177–191

Roy PK et al (2023) Analysis of community question-answering issues via machine learning and deep learning: state-of-the-art review. CAAI Transact Intell Technol 8(1):95–117

Saritas M, Yasar A (2019) Performance analysis of ANN and Naive Bayes classification algorithm for data classification. Int J Intell Syst Appl Eng 7(2):88–91

Shambour MK, Gutub A (2021) Personal privacy evaluation of smart devices applications serving Hajj and Umrah rituals. J Eng Res. https://doi.org/10.36909/jer.13199

Shankar D, Azhakath A (2021) Minor blind feature based Steganalysis for calibrated JPEG images with cross validation and classification using SVM and SVM-PSO. Multimed Tools Appl 80(3):4073–4092

Shniperov A and Prokofieva A (2019) Steganalysis method of static JPEG images based on artificial immune system. Int Conf Secur Inform Netw. pp. 1–7.

Singh A et al (2022) AI-based mobile edge computing for IoT: applications, challenges, and future scope. Arab J Sci Eng (AJSE) 47(8):9801–9831

Singh A et al. (2023) Redefining food safety traceability system through blockchain: findings, challenges and open issues. Multimedia Tools Appl (MTAP), in press. https://doi.org/10.1007/s11042-022-14006-4

Sufi F et al (2023) Automating global threat-maps generation via advancements of news sensors and AI. Arab J Sci Eng (AJSE) 48(2):2455–2472

Sun Z, Hui M and Guan C (2008) Steganalysis based on co-occurrence matrix of differential image. IEEE Int Conf Intell Inform Hiding Multimed Signal Process.

Sun Z, Kai L and Zhongyi L (2019) Prediction of concrete compressive strength based on principal component analysis and radial basis function neural network. IOP Conf Series Mater Sci Eng. 677 (2).

Thabit R et al (2022) CSNTSteg: color spacing normalization text steganography model to improve capacity and invisibility of hidden data. IEEE Access 10:65439–65458

Thangadurai K and Devi G (2014) An analysis of LSB based image steganography techniques. IEEE Int Conf Comput Commun Inform.

Umamaheswari M, Sivasubramanian S, Pandiarajan S (2010) Analysis of different steganographic algorithms for secured data hiding. Int J Comput Sci Netw Secur 10(8):154–160

Verma A (2014) A non-blind steganalysis through neural network approach. Int J Multidiscip Consort 1(1):1–13

Zebari R (2020) A comprehensive review of dimensionality reduction techniques for feature selection and feature extraction. J Appl Sci Technol Trends 1(2):56–70

Zhang T and Xijian P (2003) Reliable detection of LSB steganography based on the difference image histogram. IEEE Int Conf Acoust, Speech, Signal Process. 3.

Zielińska E, Mazurczyk W, Szczypiorski K (2014) Trends in steganography. Commun ACM 57(3):86–95

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.