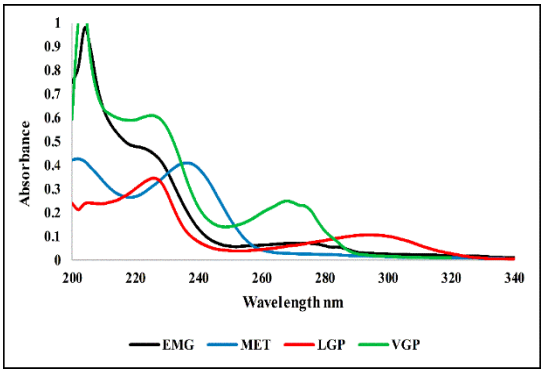
JOURNAL OF ZANKOY SULAIMANI

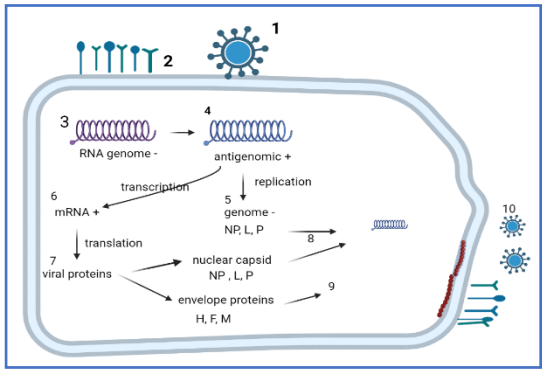
Part -A- (Pure and Applied Sciences)

VOLUME 26 ISSUE 1 June 2024

ISSN: 1812-4100

www.jzs.univsul.edu.iq





Journal homepage www.jzs.univsul.edu.iq
Journal of Zankoy Sulaimani
Part-A- (Pure and Applied Sciences)
ISSN:1812-4100

Secure Evaluation of Image Steganalysis Based on Machine Learning Algorithms

Dlsoz Abdalkarim Rashid[1]*, Marwan B. Mohammed[2], Iqbal A. Baki Mohammed[3], Tara Nawzad Ahmad Al Attar[4]

[1]*Department of Computer Science, College of Science, University of Sulaimani, Sulaimani, Iraq.*
[2]*Department of Computer Science, College of Science, University of Al-Nahrain, Baghdad, Iraq.*
[3]*Department of Computer Technologies Engineering, Al-Turath University College, Baghdad, Iraq.*
[4]*Department of Computer Science, College of Science, University of Sulaimani, Sulaimani, Iraq.*
* Corresponding email: dlsoz.rashid@univsul.edu.iq

Article info

Original: 06/04/2024
Revised: 10/06/2024
Accepted: 10/06/2024
Published online: 20/06/2024

Keywords:
Cover-image, Full Embedded Message and Half Embedded Message, Image Steganalysis, Stego-image, Steganography.

Abstract

The art of discovering concealed messages submerged in digital media using steganography in a secured form is known as steganalysis. Steganography and steganalysis have both gotten a lot of significance from law enforcement agencies and the media. More specifically, universal steganalysis techniques have grown in admiration since they perform regardless of the embedding technique. This paper comparing between three machine learning (ML) algorithms: Support Vector Machine (SVM), Naive Bays (NB), and K-Nearest Neighbor (KNN). These algorithms detect and classify whether images have embedded data within them or not; the images used in the data set have been referred to as “cover images” which means no data is embedded or “stego images” which means data had been submerged. The experiment in this study was run on a genuine dataset of categorized images. Each image in this dataset contains two embedding rates: half embedding (HE) and full embedding (FE). As a result, the comparison of the aforementioned algorithms evaluations showed that SVM is more accurate than NB and KNN algorithms when applied to HE images data, with an accuracy of 0.88 for the 50% test sample and 0.90 for the 30% test sample. When the test sample 50% was 0.82 and the sample 30% was 0.86 the SVM algorithm outperformed also. The development of more accurate and effective techniques using machine learning algorithms with help in the improvement of the security of digital communication which in turn will prevent the unauthorized transfer of sensitive information.

Introduction:

Recently, due to the proliferation of internet-connected devices and reliance on cloud-based services, cyber security threats have become a difficult task around protecting confidentiality over open networks. There is a threat that confidential information can be accessed and used by attackers with malicious internet [1]. As highlighted by Mohammed and Al Attar (2023) Due to the rapid progress of computer networks, plus the fast spread of big data, the importance of cloud computing has risen as well. Cloud computing provides a means to store and process big amounts of data including images [30]. Steganography is considered one of the most promising data security approaches [2], as it provides a way to hide information in plain sight. People were aware of the necessity to conceal information in various ways a long time ago, and steganography is a natural evolution of this idea. In the steganography process, two closely related technologies, fingerprinting and watermarking, were invented which have expanded the scope and applications of steganography. Steganography is a type of information concealment that means covered writing but it has evolved to encompass much more than that. Steganography, in other words, conceals information other than ordinary information, such as image pixels [3, 4], and can be used to embed messages in audio, video, and even text files. Thus, the steganography concept is for the storage of information in a creative way [5]. In general, images are thought to be great bearers of concealed information, and numerous approaches have been developed [6]. Furthermore, the use of steganography enhances security by hiding sensitive data inside digital media, thus preventing unauthorized access and maintaining data integrity [28]. Digital image prevalence on the internet is the most popular can be formulated Steganography process as in the following Equation 1.1 [4]:

Stego Image = Cover Image + Embedded Message (1.1)

Steganalysis is a safeguarding and analysis procedure for steganography. Image steganalysis plays an important role in many information protection systems [7, 8]. The goal of steganalysis is to determine whether a given media has embedded data. It has been recommended that subsequent embedding might be used as a tool to increase the accuracy of steganalysis [9]. Blind steganalysis and specific steganalysis are the two types of steganalysis methodologies. Blind steganography, also known as Universal steganalysis, is unrelated to the steganography process. In other words, it detects the presence of concealed messages utilizing various types of steganography algorithms and is capable of detecting them. The goal of Specific steganalysis is to detect specific steganographic media [4, 10, 11]. Specific steganalysis targets known steganography tools [12]. As a result, specific steganalysis is focused on a certain steganography algorithm by studying the embedding process as well as the statistical changes that occur. Steganographic algorithms refer to various techniques that allow concealing messages in open networks to make them imperceptible at sight [13]. Specific steganalysis algorithms can frequently outperform blind steganalysis methods in terms of detection accuracy, as they are tailored to the specific characteristics of the targeted algorithm. However, it is important to note that specific steganalysis is limited in that it cannot identify new or unknown steganography algorithms. Steganography algorithms operating in the spatial domain are typically identified by modifying the pixel value of the cover image directly [14]. As a result, blind steganalysis is gaining popularity because of its capacity to detect any known or unknown steganography algorithm [4, 12]. Steganalysis is of outstanding importance, especially in the field of national security and forensic science. Thus, the discovery of hidden messages may lead to deterrence or protection from any disastrous security incidents [15]. Utilizing one sort of feature to separate the clean and stego images is the major limitation of the steganalysis algorithm. However, combining different features from various domains such as time, frequency, and transform can significantly enhance the discrimination performance of clean and stego images [16].

This work aims to explore two directions in steganalysis to enhance security in digital communication. The first direction involves utilizing Machine Learning (ML) algorithms such as Support Vector Machine (SVM), Naive Bays (NB), and K-Nearest Neighbor (KNN) to detect

whether an image is a cover-image or a stego-image on a Half Embedding (HE) image. the second direction involves repeating the same procedures on a Full Embedding (FE) dataset, which includes a new collection of images obtained by S. M. Hameed and colleagues [15].

Related Works:

This section will present some of the researchers' works within this discipline by stating briefly their published research in steganalysis and steganography in the image.

In 2007 The authors of the paper [17] described a method that detects the Least-Significant Bit (LSB) matching steganography in grayscale photos using a system that is based on feature mining and pattern classification. They used a dynamic evolving neural fuzzy inference system in conjunction with support vector machine recursive feature elimination (SVMRFE). Similarly, in 2013 another study [27] introduced a learning-based steganalysis method that targets LSB steganography. It treats the embedded message as independent noise using a co-occurrence matrix to extract features and employs a support vector machine classifier. This approach has shown high reliability in detecting LSB matching and its improved version.

A blind color image steganalyzer [10] was proposed in 2010. Assess implements the proposed steganalysis approach with payloads ranging from 10% to 25% using well-known steganography algorithms such as Jardine Plastic Hardening-Softening (JPHS), Outguess, Model-based, and Jsteg. They employed the Analysis of Variance (ANOVA) approach to reduce the number of features, and the selected features were given to a nonlinear Support Vector Machine (SVM) for categorization into stego and clean images. The blind steganalysis method exhibited an approximately high accuracy rate for the low embedding rates, and the test results revealed good sensitivity for features of the hidden data. The authors used a fuzzy clustering algorithm for Grayscale Image Steganalysis in 2015 [15], in which the proposed detector is used as a feature set parameter by the fuzzy clustering algorithm to locate the confines of the cover-images and stego-images clusters. In terms of accuracy, detection rate, and false positive ratio, rendering assessments of Fuzzy c-mean FCM with the Highest Common Factor (HCF) are explored and compared with other work based on HCF Centre of Mass (HCF-COM) and calibrated HCF-COM by down sampling.

In 2016, [11] compared different state-of-the-art steganography techniques and varying message embedding rates to the efficiency of Discrete Wavelet Transform (DWT) feature-based steganalysis algorithms. demonstrated the influence of message type, message size, and classification method on the performance of picture steganalysis algorithms, and provided a comparative analysis of existing approaches. When compared to the Bayes, KNN, and SVM classifiers, the findings from the Neural Network classifier were superior.

The authors in 2018 [18] devised an image steganographic methodology that makes use of fuzzy logic edge detection as well as the chaotic method. to conceal a huge volume of data with a high-quality stage image of the human visual system while maintaining communication confidentiality. The results indicated why the stego image had a better high signal-to-noise ratio, image quality index, and payload when compared to other approaches.

In 2018, the authors presented an easier-to-implement [19] technique that relied on an intensity adaptive range table to determine the number of bits for a pixel of the chosen image for encoding secret messages. It also included the random selection of a unique traveling path. The goal of this approach was to minimize some of the disadvantages of the widely used LSB and Pixel Value Differencing Techniques (PVD) approaches. The experimental findings demonstrated that (even in the presence of noise) it was possible to recover a substantial amount of secret messages, proving the efficiency and viability of the proposed procedures.

By building a very big and varied dataset, the authors [20] provided a methodology for revealing inconsistencies in classification-based picture steganalysis in 2019. The method included two

classifiers: one trained using a set comprised of cover and stego images, and the other trained with the set obtained by embedding additional random messages into the original training set. This work has the advantage of being used in batch steganography. Nonetheless, even for a single test image, this method enabled detection. However, if the classification is inconsistent, the classifier should not be utilized to categorize that image.

By using an effective classification algorithm, the authors [21] introduced a new steganalysis strategy with efficient feature selection and optimization strategies to accomplish accurate identification of stego and clean photos in 2019. This work is divided into three stages. In Stage 1, they extracted picture characteristics using a unique coefficient based on the Walsh Hadamard Transform and the Gray Level Co-occurrence Matrix (GLCM). In the second stage, Pine Growth Optimization (PGO), an efficient feature selection technique, is created to choose the ideal features from the retrieved features. The Cross Integrated Machine Learning (CIML) classifier was used in the last stage to classify the stego and clean images. The approach helped to address issues such as poor detection percentage, wasteful results, and increased complexity.

In 2020: The authors provided [22] a multi-scale feature selection approach for steganalysis feature Glomerular filtration rate (GFR). This strategy reduces GFR steganalysis feature dimensionality and execution time and improves stego picture identification accuracy. Three steps summarize this effort. First, they employed SNR (signal-to-noise ratio) to measure each feature component's uselessness and remove unneeded steganalysis feature components. Second, they enhanced the Relief method to ensure the importance of feature components in recognizing stego pictures. Third, they set the threshold for removing superfluous feature components and choose the important ones as the final feature. This method does not depend on the classifier's outcome but instead selects steganalysis features based on their importance.

Because color photos with multiple color channels are commonly utilized, the authors were successful in their attempts to apply the steganalysis methods established for Gray images to the identification of each color channel in 2020 [23].

The reduction in unnecessary features in color image steganalysis features can effectively improve classification accuracy [24]. The detection findings from several color channels were then merged to assess whether or not the color image included hidden messages. Wise Ordering for Writes (WOW) and S-UNIWARD, two common content-adaptive steganography algorithms, were used in this work. The final results for the steganography algorithms WOW and S-UNIWARD have been provided. The proposed maxDSRMQ1 feature has the potential to dramatically reduce detection mistakes, especially when the payload size is tiny.

Another technique is the DeepStegBlock which combines deep learning-enhanced steganography with blockchain technology for secure and imperceptible communication between Internet of Things devices. The framework leverages Convolutional Neural Networks to discreetly send sensitive data by hiding encrypted messages inside multimedia content [29].

Our work is dependent on a dataset constructed as a new dataset by [15]. This dataset just contains the final image cover and stego. In addition, three machine learning methods were used in this study to examine the outcomes of detecting a picture if it is covered or stego and comparing it to the origin classified already present in the dataset. Also, security measures were taken into consideration to protect the dataset from unauthorized access.

The Proposal for image steganalysis

The potential use of steganography for hiding sensitive or confidential information highlights the importance of ensuring that the proposed Machine Learning Image Steganalysis method (ML-IS) is robust against attacks and able to detect hidden messages with a high degree of reliability. Figure 1 depicts the general layout of the proposed Machine Learning Image steganalysis methods (ML-

IS). An important part of ML-IS is the classification process. The main effort in the proposed ML-IS is to represent the image by asset of distinguished feature based on HCF that should be capable enough to reveal the presence or the absence of embedded messages in the image. These features are used to train ML to indemnify the centroid of the cover image and stego-image classes. Afterward, the trained centroids were delivered to the testing part of ML to detect the presence or absence of embedded messages (i.e. to classify tested images into two classes). The following sections present the details of the proposed ML-IS.

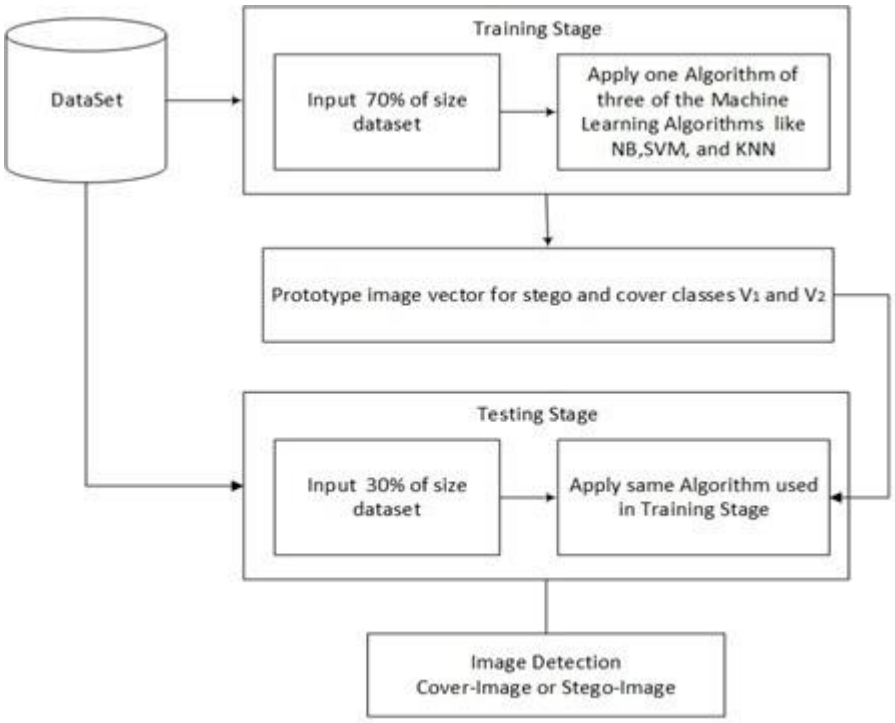


Figure 1: Diagram of the proposed steganalysis system

Image Dataset

The image dataset produced by [15] has been used as an input $S = s_1, s_2, \ldots, s_n$ of images. This image dataset was created in August 2015, by researchers S. M. Hameed and colleagues. This dataset is a collection of different Joint Photographic Experts Group (JPEG) images that have been selected randomly from different internet websites to create a dataset containing a set of cover images and stego-images. Each image is resized to 256 256 pixels and converted to grayscales (8bpp). Then, two different types of stego-images are created from the cover grayscale image using two steganography methods: LSB replacement and LSB matching. The embedded message in all the created stego-images is fixed in content and length and is embedded with three embedding rates (100%, 50%, and 25%) of the total size of the cover image. In this work, the embedding rate taken is (100% and 50%) only for evaluation. Each rate consists of 200 rows (or records), each of three columns when the Embedding rate is 100% which represents a Full Embedded (FE) message in the image, and the Embedding rate is 50% which represents Half embedded (HE) message in the image. Thus, the total number is 400 rows (or records), each for the three columns. Each row corresponds to one random image. While each column represents one attribute or feature characterizing the image at the

corresponding row. The first three features are variables and the last one indicates if it is a cover-image (0) or stego-image (1). The total number of stego n_s in the dataset is fifty from the total number of cover-image n_c.

Training Module

The construction of two vectors, referred to as the cover-images vector and the stego-images vector, is supposed to be the end result of the training step. The construction of these two vectors is something that may be accomplished by specifying the prototype value (also known as the centroid) of each individual vector.

Methods for Finding Cover Image

This paper will use three machine learning (ML) algorithms, SVM, NB, and KNN, on a dataset gathered by the authors S. M. Hameed and colleagues in [15]. By searching the Internet for past studies, it was discovered that this dataset was not submitted to any other machine learning algorithms other than those used by the researchers above. The goal of applying these techniques, which were mentioned above as pure and unaltered, is to determine their ability to detect stego-image or cover-image with the presence or absence of secret messages in grayscale images in two stages: training and testing. The training step is started by randomly selecting two vectors (v_1, v_2) that represent the beginning centers of the training image dataset.

Testing stage

Two vectors as two centroids who have been fully trained will be examining the rest of the dataset of grayscale image steganalysis, which comprises 30% that was not entered in the training phase. The purpose of using these centroids is to know how they can distinguish between cover-images, which do not contain secure messages, and stego-images, which do contain secure messages. In this paper, a binary classifier is defined with respect to a set of parameters, as in Equation 3.1:

$$F(m,\theta) = \begin{cases} C_{stego} & if\ m\ is\ image \\ C_{cover} & if\ m\ is\ image \end{cases} \quad (3.1)$$

Where (m) is a grayscale image to be classified as either stego or cover (clean). θ is a vector (target) of parameters that characterizes the grayscale image steganalysis function F, and have a great influence on the final classification accuracy. C_{stego} and C_{cover} are output labels to be assigned to the Grayscale image.

Results and Discussion

The experiments will be carried out using the stego-analysis image-based dataset, which was explained in greater detail in section 3.1. It is broken down into two stages, which are the training datasets and the testing datasets. In the first one, the dataset was divided into two equal parts, 50% represents the training sample and 50% represents the test sample randomly selected. In the second one, the dataset was divided into two different parts, which is 70% representing the training sample and 30% representing the test sample also randomly selected. The goal of using these two ways is to compare the results and achieve the highest performance accuracy through the algorithms used in this work. Note, this system worked on windows 10, CPU cori5, and RAM 8GB.

The training dataset is devoted to the purpose of adjusting the classification prototype. Furthermore, the training dataset has two types. First one FE message in the image and the other HE message in the image such that each type should contain 200 samples. The size samples taken for training samples from each type are separated randomly is 100 samples, when the

dataset is divided into 50% to represent training and 50% to represent testing, as Table 1 explains, the number of samples in the training dataset in full and half embedding. When dividing the dataset into 70% to represent training and 30% to represent testing, the size samples taken in order of training samples from each type separated randomly is 140 samples for the training.

Table 1: Number of Samples in Full and Half Embedding dataset in the Training stage

Ratio	Type Embedding in Image	Number of Samples	Cover Samples	Stego Samples
50%	Full Embedding Message	100	50	50
	Half Embedding Message	100	50	50
70%	Full Embedding Message	140	70	70
	Half Embedding Message	140	70	70

The test dataset is dedicated to evaluating the methods of Naive Bays, SVM, and KNN. The testing dataset is divided into two types the FE message in the image and the HE message in the image. Each type contains several samples, which are 100 samples from each type selected randomly from the image dataset when dividing the dataset into a 50% ratio for testing and 60 samples from each type randomly when specifying a 30% ratio of dataset size for testing. Table 2 explains the number of samples in a testing dataset in full and half embedding.

Table 2: Number of samples in a full and half embedding dataset in the training stage

Ratio	Type Embedding in Image	Number of Samples	Cover Samples	Stego Samples
50%	Full Embedding Message	100	50	50
	Half Embedding Message	100	50	50
30%	Full Embedding Message	60	30	30
	Half Embedding Message	60	30	30

The performance of steganalysis detection can be measured using a confusion matrix. A confusion matrix is a type of matrix that has two rows and two columns. Each matrix input is assigned one of four possible values: True Negative (TN), True Positive (TP), False Positive (FP), and False Negative (FN). TP is applied to correctly classified stego- images, whereas FP occurs when cover-images are incorrectly classified as spam. TN considers correctly classified cover-images, whereas FN occurs when the stego-images action is misclassified as cover-images. The confusion matrix work is shown in Table 3.

Table3: Confusion Matrix

	Predicted Cluster	
	Negative class (Cover-image)	Positive class (Stego-image)
Actual Cluster	Cover-image TN	FP
	Stego-image FN	TP

Accuracy (ACC): This measure gives the correct percentage predicates [25, 26]. It can be calculated in equation 4.1:

$$ACC = \frac{TP + TN}{TP+FP+FN+TN} \quad (4.1)$$

Stego Recall (SR): is defined as the ratio of the number of correctly detected stego-images. It can be calculated in equation 4.2[25, 26]:

$$SR = \frac{TP}{TP+F} \quad (4.2)$$

Stego Precision (SP): is the ratio of the predicted positive cases that are correct and which are actually positive. It canbe calculated in equation4.3 [25, 26]:

False Positive Rate (FPR): represents the number of cover-images flagged as stego-image divided by the total cover- images. This number measures the amount of cover-images flagged as stego-image as in equation 4.4 [25].

$$FPR = \frac{TP}{TN + FP} \quad (4.4)$$

Full embedding (FE) message in the image

In the FE message in the image, Table 4 presents the accuracy, Stego Precision (SP), Stego Recall (SR), and False PositiveRate (FPR) results of the three methods as shown below.

Table 4: Accuracy, Stego Precision, Stego Recall, and False Positive Rate results of three methods in FE

Methods	Ratio	TP	FP	FN	TN	ACC	SP	SR	FPR
Naive Bays	50%	38	12	6	44	0.82	0.76	0.863	o.214
	30%	22	8	7	23	0.75	0.733	0.758	0.258
SVM	50%	46	4	14	36	0.82	0.92	0.766	0.1
	30%	27	3	5	25	0.866	0.9	0.843	0.107
KNN	50%	39	11	10	40	0.79	0.78	0.795	0.215
	30%	25	5	8	22	0.783	0.833	0.757	0.185

SVM results presented in Table 4 clarifies generally whether the test sample 50% or 30% best accuracy is achieved in full embedding (FE) in the image. Figure 2 depicts ACC, SP, SR, and FPR.

In the testing sample 50%, the Metrics of the SVM algorithm are compared with NB and KNN algorithms where the accuracy of the SVM algorithm is (0.82), NB is (0.82) which is equaling the SVM algorithm's result, and KNN: is 0.79% which is less than SVM and NB algorithms. In the testing sample 30%, metrics of the SVM algorithm are compared with two algorithms, these are NB and KNN, where the accuracy of the SVM algorithm is (0.86667 0.87), NB is (0.75) which is less than the SVM algorithm, and KNN is (0.783 0.78) which is less than SVM and larger than NB algorithms. Although accuracy results are similar to NB and SVM accuracy achieved 0.82%

in the testing sample 50%. But in other metrics like SR which reflect the ratio of the number of correctly detected stego-images, the NB algorithm presents the best performance in recognizing and detecting stego-images where the SR in NB is (0.86), KNN is (0.79592 0.80), and SVM is (0.76) which is less than NB and KNN algorithms. This indicates that the NB algorithm is very good in the detection stego-images when using a testing sample of 50%.

While the SVM algorithm presents the best performance in recognizing and detecting stego-images, the SR in SVM is (0.84375 0.84), NB is (0.75862 0.76), and KNN is (0.757 0.76). This indicates that the SVM algorithm overcomes the two algorithms NB and KNN for detecting stego-images when using a testing sample of 30%. This means that NB is very good at correctly detecting when a training sample and the test sample are equal.

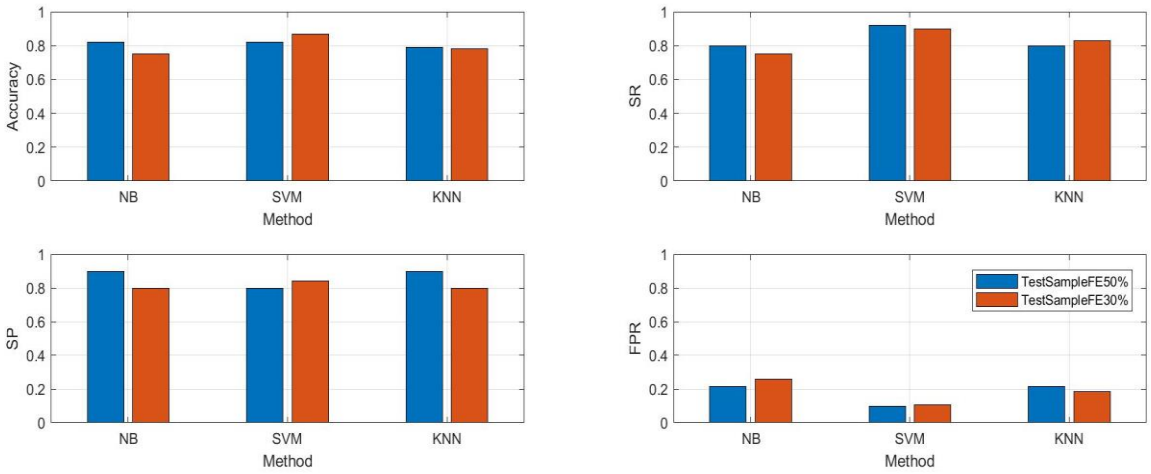


Figure 2: Accuracy, Stego-Presision (SP), Stego-Recall (SR), and False Positive Rate (FPR) in Full-embedding in Image.

Half embedding (HE) message in the image

In the HE message in the image, the results of three methods shown in Table 5 present the accuracy, Precision, TruePositive rate, and True Negative rate.

Table 5: Accuracy, Precision, Recall, and False Positive Rate rate in HE

Methods	Ratio	TP	FP	FN	TN	ACC	SP	SR	FPR
Naive Bays	50%	41	9	5	45	0.86	0.82	0.891	166
	30%	25	5	5	25	0.833	0.833	0.833	0.166
SVM	50%	48	2	10	40	0.88	0.96	0.827	0.047
	30%	29	1	5	25	0.90	0.966	0.852	0.036
KNN	50%	41	9	10	40	0.81	0.82	0.803	0.183
	30%	27	3	6	24	0.85	0.90	0.818	0.111

SVM results presented in Table 5 clarifies generally whether the test sample is 50% or 30% the best accuracy is achieved in Half embedding in the image. Figure 3 depicts to Accuracy, Stego-Presision, Stego-Recall, and False Positive Rate. In the testing sample 50%, metrics of the SVM algorithm are compared with NB and KNN algorithms where the accuracy of the SVM algorithm is (0.88), NB is (0.86), and KNN is (0.81) which is less than SVM and NB algorithms. While, in the testing sample 30%, the metrics of the SVM algorithm are compared with two algorithms these are NB and KNN, where the accuracy of the SVM algorithm is (0.90), NB is (0.83) which is less than the SVM algorithm, and KNN is (0.85) which is less than SVM and larger than NB algorithms. The KNN algorithm gives an indicator of very good performance when a training sample and large, and the test sample is small this with what has appeared in the results in bothtest samples. While the NB algorithm shows that it is active and able to get the best result, the training samples (50%) should be equal to the test samples (50%). However, the SVM algorithm proved that it has perfect performance whether the test sample large or small compared with NB and KNN algorithms.

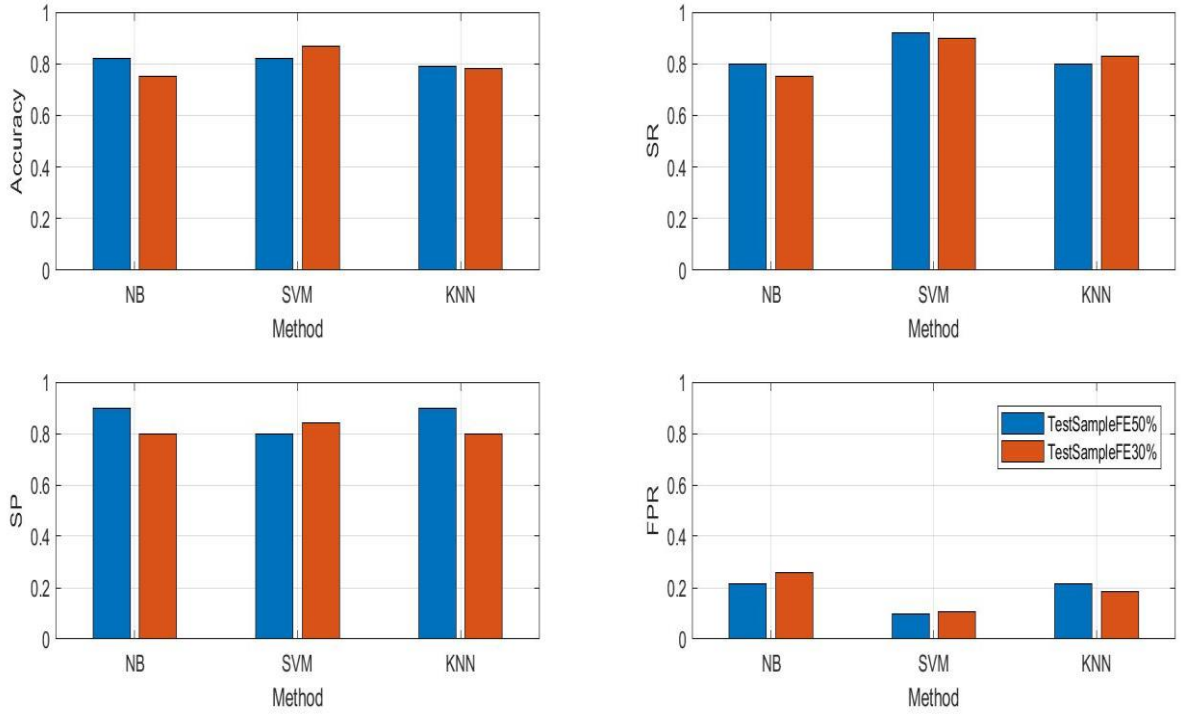


Figure 3: Accuracy, StegoPresision, StegoRecall, and False Positive Rate in Half-Embedding in Image

The metric Setgo-Recall explains by results that NB algorithm presents the best performance in recognizing and detecting stego-images where the SR in NB is (0.89), SVM is (0.83), and KNN is (0.80) which is less than NB and SVM algorithms. This indicates that the NB algorithm is very good at detecting stego-images when using a testing sample of 50%. The SVM algorithm presents the best performance in recognizing and detecting stego-images where the SR in SVM is (0.85), NB is (0.83), and KNN is (0.82). This indicates that the SVM algorithm overcomes two algorithms NB and KNN to the detection of stego-images when using a testing sample of 30%. This means that NB is very good at correctly detecting when a training sample and the test sample are equal. On the other hand, the metric of FPR explains through results that the SVM algorithm achieved less ratio in FPR than NB and

KNN algorithm in both testing samples 50% and 30%. This means that the SVM algorithm proved that it can recognize cover images also.

Finally, the SVM algorithm presents the best performance in most measures used in this work compared with NB and KNN algorithms whether in test samples (especially with HE) or with FE in images as Figure 4 shows the overall results briefly.

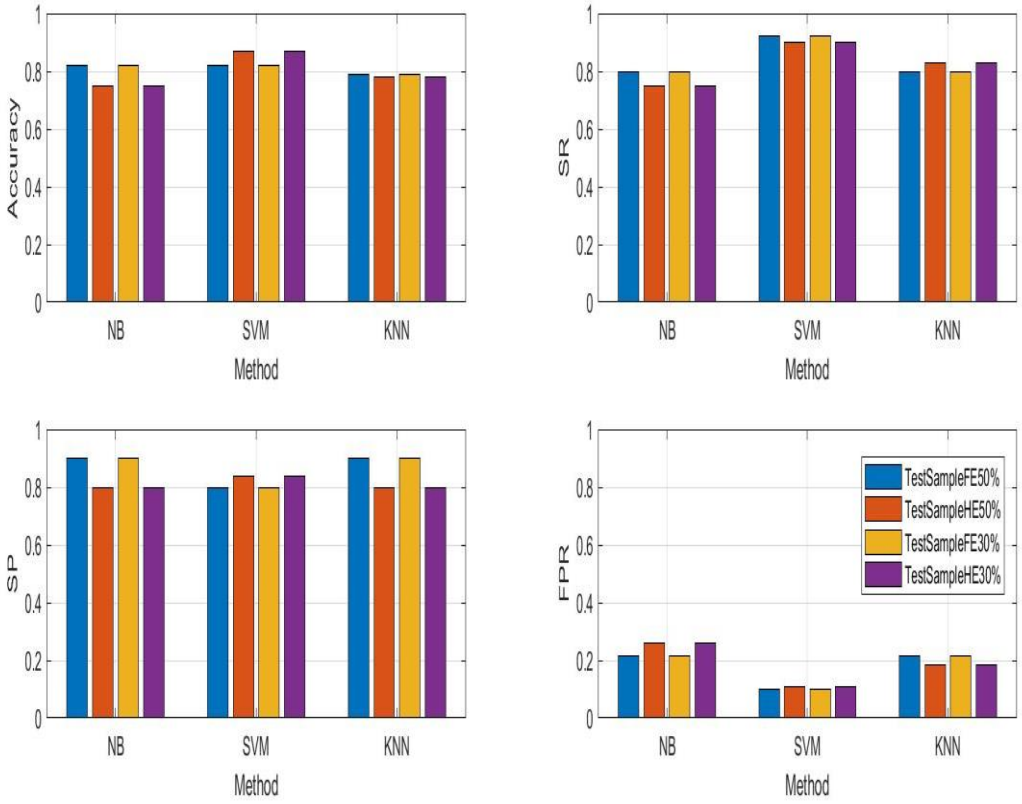


Figure 4: Accuracy, StegoPresision, StegoRecall, and False Positive Rate between FE and HE in Image to each sample ratio

Conclusions and Future Work

It is important to notice that steganalysis plays a crucial role in detecting hidden information within a given medium, particularly as the use of steganography continues to evolve and become more sophisticated. Consequently, steganalysis algorithms will need to be continuously updated and refined to maintain their ability to detect hidden data with a high degree of accuracy. The following algorithms were shown: NB, SVM, and KNN, which were used to recognize and detect stego-image: The performance of the NB algorithm depends on the size of the training sample and test sample if they are equal, the NB algorithm becomes able to increase the accuracy and StegoRecall. while it has been deduced that the results of SVM algorithm performance achieved the best in accuracy and StegoRecall in half embedding in images, whether the test sample is 50% or 30%. The reason may be that the information embedded in the images is smaller. Also, SVM performance overcame the rest of the algorithms, so that achieved the best results in Full Embedding in the image when the test sample was 30%. This means that SVM algorithm accuracy increases when the size of the training sample is large. Finally, the metrics of the SVM algorithm overall achieved the best results in full embedding and half embedding in the image compared with the NB and KNN algorithms. In future work, other machine learning algorithms can be used to compare the results with them. Also, the results of this work can be improved by developing algorithms that improve the ability of steganalysis to detect data securely in digital media. Can use artificial intelligence techniques to evaluate and verify to be written by humans as future work.

Conflict of Interest

The authors declare no conflicts of interest regarding this manuscript's publication and/or funding.

References

[1] I. Hussain, J. Zeng, X. Qin, and S. Tan, A survey on deep convolutional neural networks for image steganography and steganalysis, KSII Transactions on Internet and Information Systems (TIIS) (2020). Vol 14, no. 3, Pages1228-1248.

[2] S. Marwan, A. Shawish, and K. Nagaty, Utilizing DNA Strands for Secured Data-Hiding with High Capacity, International Journal of Interactive Mobile Technologies (2017). Vol 11, no. 2.

[3] M. B. Dastgheib, M. F. Jahromi, and J. T. Nejad, A Low Cost Image Steganalysis by Using Domain Adaptation, International Journal of Information Science and Management (IJISM) (2018). Vol 16, no. 1

[4] A. M. Rabee, M. H. Mohamed, and Y. B. Mahdy, Blind JPEG steganalysis based on DCT coefficients differences, Multimedia Tools and Applications (2018). Vol 77, no. 6, Pages 7763-7777.

[5] H. T. S. ALRikabi and H. T. Hazim, Enhanced data security of communication system using combined encryptionand steganography, IJIM (2021). Vol 15, no. 16, Page 145.

[6] A. Nissar and A. H. Mir, Classification of steganalysis techniques: A study, Digital Signal Processing (2010). Vol 20, no. 6, Pages 1758-1770.

[7] J. Zhang, K. Chen, C. Qin, W. Zhang, and N.-H. Yu, Distribution-preserving-based

automatic data augmentation for deep image steganalysis, IEEE Transactions on Multimedia (2021).
[8] H. Martyniuk, V. Kozlovskiy, T. Meleshko, and A. Sorokun, Method of Finding Cover Signal for Audio Steganalysis Calibrated Methods, in 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, (IDAACS) (2021). Volume 2: IEEE, Pages 1095-1100.
[9] D. Megias and D.Lerch-Hostalot, Subsequent embedding in targeted image steganalysis: Theoretical framework and practical applications, IEEE Transactions, on Dependable and Secure Computing (2022).
[10] M. Sheikhan, M. S. Moin, and M. Pezhmanpour, Blind image steganalysis via joint co-occurrence matrix and statistical moments of contourlet transform, in 2010 10th International Conference on Intelligent Systems Design and Applications, IEEE, (2010). Pages (368-372).
[11] M. B. Desai and S. Patel, Performance analysis of image steganalysis against message size, message type, and classification methods, in 2016 IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT): IEEE (2016), Pages 295-302.
[12] R. R. Chhikara, P. Sharma, and L. Singh, An improved dynamic discrete firefly algorithm for blind image steganalysis, International Journal of Machine Learning and Cybernetics (2018), Vol 9, no 5 Pages 821-835.
[13] T.-S. Reinel et al., GBRAS-Net: a convolutional neural network architecture for spatial image steganalysis, IEEE Access (2021), Vol 9, Pages 14340-14350.
[14] 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 (2020), Vol 2020, no 1, Pages. 1-12.
[15] S. M. Hameed, R. A. Mohammed, and A. Baraa'A, Fuzzy Based Clustering for Grayscale Image Steganalysis, Iraqi Journal of Science (2015), Vol 56, no 2A, Pages. 1161-1175.
[16] A. Dehdar, A. Keshavarz, and N. Parhizgar, Image steganalysis using modified graph clustering based ant colony optimization and Random Forest, Multimedia Tools and Applications, (2022), Pages 1-18.
[17] Q. Liu, A. H. Sung, Z. Chen, and J. Xu, Feature mining and pattern classification for steganalysis of LSB matching steganography in grayscale images, Pattern Recognition (2008), Vol 41, no 1, Pages 56-66.
[18] C. Vanmathi and S. Prabu, Image steganography using fuzzy logic and chaotic for large payload and high imperceptibility, International Journal of Fuzzy Systems (2018), Vol 20, no 2, Pages 460-473.
[19] S. Kaur, S. Bansal, and R. Bansal, Estimating the Effect of Noises over an Efficient Image Steganography Algorithm Based on Intensity and Path Adaptation, (2018).
[20] D. Lerch-Hostalot and D. Meg´ıas, Detection of classifier inconsistencies in image steganalysis, in Proceedings of the ACM Workshop on Information Hiding and Multimedia Security (2019), Pages 222-229.
[21] J. B. Guttikonda,A new steganalysis approach with an efficient feature selection and classification algorithms for identifying the stego images, Multimedia Tools and Applications (2019), Vol 78, no 15, Pages 21113-21131.
[22] X. Yu, Y. Ma, R. Jin, L. Xu, and X. Duan, A multi-scale feature selection method for steganalytic feature GFR, IEEE Access (2020), Vol 78, no 8, Pages 55063-55075.

[23] C. Yang, Y. Kang, F. Liu, X. Song, J. Wang, and X. Luo, Color image steganalysis based on embedding change probabilities in differential channels, International Journal of Distributed Sensor Networks (2020), Vol 16, no 5, Page 1550147720917826

[24] J. Xu, J. Yang, Y. Ma, K. Qu, and Y. Kang, Feature selection method for color image steganalysis based on fuzzy neighborhood conditional entropy, Applied Intelligence, (2022), Pages 1-18.

[25] S. M. Hameed, M. B. Mohammed, and B. A. Attea, Fuzzy based spam filtering, Iraqi Journal of Science (2015), Vol 56, no 1B, Pages 506-519.

[26] A. Odeh, I. Keshta, and E. Abdelfattah, Efficient detection of phishing websites using multilayer perceptron, IJIM (2020), Vol 14, no 11, Pages 22-31.

[27] Z. Xia, X. Wang, X. Sun and B. Wang, Steganalysis of least significant bit matching using multi-order differences. Security and Communication Networks (2014), Vol 7, no 8. pages 1283-1291.

[28] S. Pramanik and R.P. Singh, Role of Steganography in Security Issues. International Conference on Advanced Studies in Engineering and Science. (2017).

[29] V. Raja and K.S. Suresh, Deep Steg Block: Deep Learning-Enhanced Steganography for Secure Communication in IoT Devices Using Blockchain. Education Administration: Theory and Practice (2024). Vol 30, no 4. pages 2958-2972.

[30] M. Mohammed and T. Al Attar, Fully Homomorphic Encryption Scheme for Securing Cloud Data. UHD Journal of Science and Technology (2023). Vol 7, no 2 2023. pages 40-49.