Journal of Population Therapeutics & Clinical Pharmacology

RESEARCH ARTICLE
DOI: 10.53555/3r2rnm36

SECURED IMAGE: A PRACTICAL SYSTEM FOR DETECTING MALICIOUS PAYLOADS HIDDEN IN IMAGES

Aklovya Kumar Yadav,[1] Himanshu Verma,[2] Bhupal Arya,*[3] Dr. Tanveer Hassan[4]

[1]Computer Science Engineering Galgotias University, Greater Noida, India
yadavaklovya@gmail.com
[2]Computer Science Engineering Galgotias University, Greater Noida, India
*[3]Assistant Professor Galgotias University Greater Noida , India bhupalarya@gmail.com
[4]Assistant Professor School of Computer Science & Engineering
Galgotias University, Greater Noida India Tanveer.hassan@galgotiasuniversity.edu.in

***Corresponding Author:** Bhupal Arya
Assistant Professor Galgotias University Greater Noida , India
*bhupalarya@gmail.com

Abstract—Digital image is one of the most actively trans- mitted types of data in modern communication systems which include email services, social media networks, cloud stores, and web-oriented applications. Although image files are generally considered harmless, they can also be used to cover silently hidden information by using steganography methods. Hidden information may include confidential information, unwarranted messages, or malicious software and pose a possible security threat.

The paper presents an empirical and explainable system, which is named as SecuredImage, a method to detect concealed data in digital images using statistical and image analysis approaches and controlled machine learning approach. The designed solution focuses on simplicity and realism with maintaining the efficient detection. The system is trained using a controlled set of regular images and LSB steganographic images. The inputs to a logistic regression classifier are extracted statistical features mean pixel intensity, variance, Shannon entropy, skewness, kurtosis, file size, among others. Experimental testing proves that SecuredImage can achieve reliable detection safety and computational efficiency, which prove that feature-based machine learning is a promising baseline approach to performing image steganalysis.

Index Terms—component, formatting, style, styling, insert

Introduction

The high-rate development of digital communication tech- nologies has ignited the magnified growth of multimedia information production, transfer, and storage. Among the multimedia forms, digital images have taken the approach of becoming one of the most common mediums of transmission, through information exchange, due to their easy acquisition, compactness and wide applicability in diverse, heterogeneous communication platforms. Images are therefore dispatched regularly through email services, social media networks, in- stant messaging application, cloud storage architectures and web based services and thus represent a basic unit of modern digital ecosystem.

Image files, due to their inherent non-executable nature, are often viewed as harmless by the end users as well as traditional security protocols. The inspection of the executable files, scripts, and network traffic are often taken into account by security infrastructures, but image files are discussed

as inoffensive material. The implicit trust of image formats has brought about a possibility of using images as a form of hidden communication by enemies. In this respect, one method worth mentioning is that of steganography, which involves storing in digital media a hidden information in such a way that the presence of the hidden data can go unnoticed.

Steganography is radically different in nature to cryptog- raphy. Whereas cryptographic strategies strive to secure the content of a message such that a third party cannot easily read it because it is too complicated and coded, steganographic strategies aim at covering up the existence of a message to such an extent that a third party is not likely to notice it. Images are particularly appropriate vectors of steganography since they are characterised by large amounts of redundant information, and can accept a large amount of pixel-based modifications without producing any discernible visual effects. With a number of pixel values changed, the resulting image often does not visually strike any difference than the original image to the human viewer.

Whereas steganography has a justifiable purpose (as, e.g., in secure communication, digital watermarking, and copyright protection) it also has an evil side. There is a chance that attackers will be storing sensitive data, rogue messages, or harmful commands inside the image files in order to bypass traditional security measures. Using these hidden data enables covert data exfiltration or illicit communication once placed therein, as the recipient may later extract such hidden data with deserted specialized tools. This is a serious threat to the current cybersecurity systems as a result of this abuse of steganography.

Least Significant Bit (LSB) embedding is one of the most commonly used spatial-domain algorithms of the many steganographic techniques. In LSB steganography the $B:s of the pixel values are modified to represent a hidden message. These changes are visually incomprehensible but inject small scale statistical distortions in pixel distributions. In spite of simplicity, the LSB-based steganography is still efficient in avoiding detection by amateurs and level 1 security checks.

In order to cope with this threat, steganalytic methods have been developed to reveal the existence of concealed infor- mation over digital media. The initial steganalytic methods were based on statistical analyses of images by hand, and they included methods such as histogram analysis, entropy, and pixel correlation analysis. Nevertheless, manual analysis is not feasible in the face of the large volume of image collections
that one would have to handle in a real-world scenario, which leads to the urge to pursue automated methods of detection that have a machine learning foundation.

Machine learning provides a powerful architecture of ste- ganalysis by training on experience by learning trends and decision conformities, instead of following rules. Machine learning models can be used to tell the difference of innocent images and those with concealed data by extracting salient statistical features of their images and training a classifier. Machine learning methods based on features provide a balance between the accuracy of detection, computing efficiency and interpretability making them appropriate to both research and academic purposes as well as detecting baseline machine learning system.

Convolutional Neural Network (CNN) paradigms of deep learning have become increasingly popular in steganalysis during the last several years due to their ability to acquire the complicated feature representations and learn to do so independently. However, these methods require large labelled datasets, expensive computing resources and complex model architectures. Such requirements can be restrictive in either a research-based environment or a resource-constrained one.

The present paper presents SecuredImage, a small but effective steganalytic system based on the notion of statistical analysis of images and supervised machine learning. The suggested system is focused on identifying unknown data smuggling through LSB steganography that involves deriving a highly careful set of statistical features of digital pictures. These features then provide training of a Logistic Regression classifier, which is binary classification to determine whether there is covert information in an image.

The main value of the work lies in the fact that it shows how a lightweight and easily understandable machine learning paradigm can be used to achieve dependable steganalysis. The system proposed can ensure transparency, reproducibility and easy implementation, even though it achieves acceptable

detection performance, by avoiding overly complex models. The rest of this paper will be organized as follows: Section II will be a review of related literature, Section III will outline the proposed methodology, Section IV will provide experimental results and discussion, and finally Section V will provide a conclusion of the paper and research directions.

Related Work

Steganography and steganalysis are some of the research areas that are old in information security field. Early research work was largely focused on the ways that hidden information can be drawn into digital media and then retrieved. Images have been the most widely studied forms of media, owing to their ubiquitous use, and due to the large volume of data redundancy.

The first steganographic schemes worked in the spatial domain, and the Least Significant Bit (LSB) substitution was the most widely used one. In steganography of LSB, the tiniest bits of the pixel intensities are manipulated to convey hidden information. Although all these changes are not perceivable by the eye they distort the statistical properties of the image. Empirical work has demonstrated that LSB embedding remarkably entails discernible artistically patterns among distributions of pixel-values, which can be used in steganalytic methods.

The steganalytic techniques developed during the early years were largely based on image statistical analysis. An analysis of the histograms was typically used to detect the characteristics of abnormalities caused by embedding the data, including the presence of anomalous peaks or the asymmetry of pixel-value distributions. After the choice of entropy-based methods was also explored, based on the motive that the addition of concealed information is likely to increase the unpredictability of pixel values. These techniques proved that even primitive statistical measures could be used to provide useful hints at steganographic information.

As the field of research continued developing, it was established that more advanced methods of statistics could be developed to increase the precision of detection. Neigh- borhood pixel correlation analyses and co-occurrence matrix derived feature extraction were proposed to manifest inter- pixel relationship. These techniques looked at the effects that steganographic embedding had on intrinsic spatial relation- ships in pictures. Although these techniques worked, often they required manual domain expertise and feature engineering.

Machine learning introduced a massive paradigm shift to steganalysis. Instead of steadily relying on manual crafted heuristics, machine-learning-based methods allowed acquiring decision boundaries in an automated manner using data. The researchers started to derive statistical features of images and present them to such classifiers as Support Vector Machines (SVM), Logistic Regression, k -Nearest Neighbors (k -NN) as well as Random Forests. Such models provided better detection performance and better generalization as compared to purely statistical methods of detection.

The Logistic Regression is one of the traditional classifiers that have received specific interest due to its simplicity, interpretability, and ability to classify two classes. Several tests have proved that Logistic Regression could achieve competitive performances in situations of being trained using well-chosen statistical features particularly in detecting LSB- based steganography. Random Forests together with ensemble techniques further benefited by combining different decision trees though at the cost of a more complex model.

At the same time, the frequency-domain steganographic methods, including those that are based on Discrete Cosine Transform (DCT) coefficients used in JPEG images, were stud- ied. In line with this, the advances of steganalytic techniques were to examine frequency-domain characteristics, including DCT coefficient allocation and spectral energy candidature. Although frequency-domain analysis increased resistance to some embedding measures, it also increased the calculated loads.

Steganalysis using deep learning has gained a lot of popu- larity in the recent years. CNNs have been applied to automati- cally acquire hierarchical feature representations directly learnt directly on the image data. There has been state-of-art per- formance onbenchmark datasets with CNNbased techniques including BOSSBase and ALASKA. However, the approaches involve huge volumes of labeled data, time-consuming training times, and high computing expenses. As well, deep-learning models are not easily interpretable, which makes the rationales of classifications difficult to explain.

Although there are achievements related to the use of deep- learning methods, feature-based machine-learning techniques are relevant, particularly in the academic domain as well as developing a baseline system. Some of the benefits of feature- based approaches include explainability, reproducibility, and low resources. They are also relatively easy to institute and analyze making them appropriate in controlled experimental studies.

According to the available literature, this paper employs a statistical image steganalysis feature based machine-learning technique. The proposed system will focus on steganography using LSB, and a small classifier to prove that favorable results can be obtained without using sophisticated deep-learning networks. This method gives a thick foundation upon which to build alternative research and is a practical solution in a situation where complexity and comprehensibility are of high values.

Proposed Methodology

The proposed system for the SecureImage is a statistical image analysis through supervised machine learning to find the hidden data in digital images. The methodology adheres to a pipeline which is structured and interpretable and leads to consistency, reproducibility, and computational efficiency. The system takes steganalysis as a binary type of classification where all input images undergo analysis after which they are considered to be either a normal image or one that has hidden information. The general flow of work can be described as a sequential movement, where the preparation of the dataset will be the first step and the final one will be performance evaluation.

A managed dataset will be developed to test the usefulness of the approach being proposed. The records will contain about four hundred digital images which will be categorized equally into two groups normal image and steganographic image. Normal images are taken in open-source image repositories, personal image collections to ensure the diversity of images content, texture and illumination conditions. These images are benign image data, and they are the standard class of the images in classification.

That is created as steganographic images whereby the textual information is implanted in the normal images through the least significant bit (LSB) steganography method. The reason behind LSB embedding is the simplicity and wide use of the method as well as established behavior in the literature. In the process of embedding, pixel values are altered to enclose hidden information as the least significant bits. These modifications produce changes in statistics of the distributions of pixels, despite the fact that the visual characteristics of the

picture remain unchanged. The dataset has a valid experimen- tal setup of assessing detection performance because of the control forms of embedding.

As a preprocessing phase to the statistical analysis, all of the images are subjected to a preprocessing stage to ensure consistency in each dataset. Images are downsized at a fixed resolution and changed to a fixed color format. The value of the pixels is normalized to a standard range to ensure that numerical stability is achieved in terms of calculating the features. This step is a preprocessing step which reduces variation due to dissimilarity in image resolution and format and extracted features relate mostly to influence of data embedding and not likeness of other picture traits.

The main part of the given methodology is feature extrac-tion. The task of this step is to obtain statistical features of images which are affected by steganographic interference. The use of a couple of statistical indicators is done on each image such as the mean intensity of each pixel, the variance, entropy, as well as skw, and kurtosis and file size. The mean pixel in- tensity is an overall brightness of an image and variance is the distribution of the pixel values and can be used to have an idea about noise caused by the concealed information. The Shannon entropy quantifies the unpredictability of the pixel values and is more likely to rise when some hidden information is being installed. Skewness and kurtosis characterize the asymmetry and the concentration of the pixel distributions respectively, and thus permit the preservation of small distributional shifts. Even the file size is taken into account, because in case of embedding hidden information, there will be a change of size by a marginal margin. The obtained statistics are assembled to create a numerical feature vector of every image. The entire data is then stored in a feature matrix whereby each row is represented as an image and each column is represented as a statistical feature. The features with large numerical ranges are avoided

by scaling them to features with smaller numerical ranges when these values are found to dominate the learning process. The structured representation of machine learning models allows the efficient training and testing of machine learning models. To do the classification, a Logistic Regression model is used to differentiate between normal and steganographic images. Logistic Regression is selected because of its simplicity, interpretation and binary classification issues. The model gives an estimation of whether a particular image has the hidden data depending on the extract feature vector. Another benefit of the Logistic Regression is that it allows giving an idea of the relative significance of individual features and thus making
the process of detection more explainable.

The dataset is separated into the training and testing subsets according to seventy to thirty ratio. The classification model parameters are learned on the training set and the test set is meant to be used in checking the generalization ability of the model on the images that it had not seen before. Such a division is required to keep performance indicators close to actual detection ability. Cross-validation can also be implemented in the training phase in order to enhance thevigor and minimize overfitting.

The standard classification measures are used to determine the performance of the system based on such measures as ac- curacy, precision, recall and confusion matrix analysis. These measures give a detailed picture of the behavior of detection through the measurement of correct and incorrect classifica- tions. The effectiveness of the proposed approach is analyzed using the results of evaluation and potential limitations are identified.

Computationally, the proposed methodology is very efficient since the number of features is low as it uses a low dimensional representation and as it makes use of a lightweight classi- fication model. Standard computing equipment can be used to extract popular features and classify the extracted features quickly without having to rely on specialized equipment. This efficiency has been what makes the system applicable both in the large scale image processing as well as the real-time situation of detection.

Altogether, the suggested methodology indicates that a hybrid of statistical features generation and supervised ma- chine learning could bring a good solution to identify the concealed information in digital pictures in an effective and understandable way. The simplicity of the system with the ability to provide dependable performance in steganalysis of images makes the SecuredImage a robust base in steganalysis framework and a platform on which the future developments can build on.

Experimental Results and Discussion

The trial analysis of the SecuredImage system was con- ducted to determine the effectiveness of the system in un- earthing hidden information in digital images. The experiment design was meant to confirm that statistical image features used together with supervised machine learning could be used in steganalysis in rigorously controlled conditions. All of the experimental operations were done on a built dataset of normal images and steganographic images which were produced by Least Significant Bit embedding.

The data was divided into a training and testing sample in a seventy to thirty proportion. The parameters of a Logistic Regression classifier were estimated with the help of the training set, but the testing set was to be used only to assess the work of the system on the previously unknown images. This decoupling allowed the results that were reported to be an accurate representation of the capability of the model to make predictions out of the data used in the process of training it. The experiments have been conducted using normal computing hardware and no specialized acceleration was employed and thus it proved the efficiency of calculation of the proposed methodology.

To measure the performance of the system, the generally accepted metrics of the classification, such as accuracy, preci- sion, recall, and confusion-matrix analysis, were used. Correct- ness was taken as the main measure of general defectiveness, which is the percentage of images that had been classified correctly in the test set. Precision and recall were also used to
shed more light on the classification performance, to measure the system capability within recognizing steganographic im- ages, whilst reducing the false classifications. The confusion- matrix analysis explained the rate of the correct and incorrect predictions of both classes.

Based on the experimental results it can be seen that the proposed system has a total detection accuracy of between eighty to eighty-five percent on the test data. Such performance shows that machine learning using statistical features can be effectively used to identify normal and steganographic images, even when no complicated deep-learning models are used. The current level of accuracy carries the expected level of perfection of a baseline steganalysis system when working in controlled experimental conditions.

Broadening the scope of classification behavior analysis reveals that statistical characteristics in terms of randomness and pixel distribution are very crucial in the performance of detection. Precisely, the entropy and variance became powerful factors that indicated the existence of hidden data. Images with embedded text tended to have high values of entropy, which can be explained by the greater value of randomness which data embedding brings. Similarly, the magnitude of the vari- ance measurement was mirrored by delicacies of noise patterns due to the alteration in pixel values. These results support the hypothesis behind the use of the statistical characteristics on steganalysis.

Although the overall results are positive, there were some cases of misclassification when the tests were being conducted. There are also some normal images with an intrinsically large noise level or stylized textures, which were sometimes identified as steganographic. On the other hand, the small set of steganographic pictures combined with low density of em- bedding or images with smooth visual features was incorrectly directive as normal. These misclassifications indicate the very nature of the limitations inherent in the use of purely statistical methods and refer to the possible ways of improvement.

The analysis of the confusions matrices also shows the equilibrium between the true positives, the true negatives, the false positives, and the false negatives. The false-positive rate of the system is quite low implying that most of the normal images are detected correctly. This feature is favorable in real life situation because it minimizes unnecessary alerts and those alarms generated. At the same time, the system has a sufficient level of detecting steganographic images, thus establishing its the effectiveness in detecting concealed information.

Computationally, the suggested system is efficiently per- formed. The image processing time is very short to come up with feature extraction and classification which makes the system applicable in real-time processing of images or in large image analysis applications. This efficiency is ensured by the use of low-dimensional feature vector and a low end classifier such that the system can be used with a standard hardware without performance becoming a bottleneck.

Altogether, the experimental findings can support the ef- fectiveness of the SecuredImage system as a steganalysis- based baseline. It is a testament to the feasibility of the approach because of the achieved detection performance, which is combined with low computational complexity and high interpretability. Although there is no specific intent of the system to identify highly advanced methods of steganography, the system provides a strong base that can be strengthened by new features and other working classifiers or bigger and varied data sets.

Discussion and Analysis

The empirical findings provided by the system of Secured- Image provide substantive information on the effectiveness of machine learning based on statistical features to perform the image steganalysis task. The detection rates which are noted suggest that the even the parsimonious and explainable modeling structures may be successfully used to obtain the insight into the covert information concealed in the digital im- ages as long as appropriately discriminative features are used. In its turn, these results support the argument according to which complex deep-learning designs do not necessarily play a critical role in achieving a reliable baseline performance, at least in highly controlled experimental contexts.

The results of observation can be explained by the increased sensitivity of statistical image features to the perturbation created by steganographic embedding. Keeping the process unnoticeable yet in a systematic and organized way, the least significant challenge of-bit embedding makes subtle adjustments to pixel values, transforming the global statistical characteristics, such as entropy, variance, and distributional shape. Though these changes are not detectable by the naked eye, these

changes are effectively measured using the strict statistical test, thus proving that determinants of randomness and pixel dispersion are good signals in the detection of signs of hidden data that have been stenciled employing spatial - domain methods.

The use of the Logistic Regression paradigm of classifica- tion to classify contributes to the increased intelligibility of the system, as well as the stability. As opposed to other more detailed models, the Logistic Regression provides a transparent probabilistic decision boundary which is based on extracted features thus allowing a full analysis of what the classifier does which is a critical requirement when doing academic or security focused work. The homogeneity of the results on the variety of test samples also shows that the model starts generalizing satisfactorily within the inherent limitations of the data the model is tested on.

Despite the promising results, certain constraints did occur in the course of the analysis. Normal images that had a high level of natural noise or complex texture were incidentally erroneously identified as steganographic. This has been ex- plained by the fact that such images tend to have a higher entropy and variance value and thus end up being statistically identical to the steganographic images. Steganographic images that had a low embedding density or whose visual contents were smooth at times were considered to be normal, since the statistical perturbations that embedding caused were minimal.

These results shedding light on these inherent trade-offs of the statistical feature-based approaches.

The confusion matrix analysis also serves to highlight the trade-off that is achieved between the detection accuracy and the false-alarm rate. The relatively low false-positive rate allows gravitating towards conservative labeling of suspect images, which is desirable in real life application of this system where unnecessary alarms can hamper system usability. At the same time the system has a satisfactory true-positive rate which affirm its ability to detect in images hidden data. This equilibrium testifies to the fact that the chosen features and classification plan are best suited to the detection goal in general.

The proposed methodology has significant benefits in the computational sense. The parsimonious feature set in brief dimensions coupled with a simple classification system results in both fast processing of the features and low resource consumption. This efficiency makes the system appropriate to be used in systems that are limited in their computational capabilities or when a large set of images has to be processed. Besides, the lack of sophisticated model training and inference further increases the feasibility of the method used.

Secured Image system enables a slightly higher absolute accuracy at the expenses of more interpretability, simplicity, and ease to implement as compared to the deep-learning based steganalysis methods that have been reported in the literature. Deep-learning models will continue to require large datasets and massive computing power on an ongoing basis, which might not be tenable in some situations. Contrarily, the Secured Image system provides clear and replicable solution that could be used as a baseline or preliminary screening tool in image-security processes.

Overall, the discussion shows that the presented methodology balances the performance of detection, interpretability, and computational efficiency in a competent way. Even though the system is not designed to address highly advanced or evolving steganographic plans, it is sufficiently good to perform its function of steganalysis as a baseline steganalysis framework. The knowledge gained out of this analysis gave a solid base of potential improvements, such as adding additional features, involving alternative classifiers, or even coming up with hy- brid paradigms, which combines the statistical approach and learning-based approach.

The information obtained during this analysis provides a solid basis of further improvements, including the incorpora- tion of new functionalities, the embrace of new classifiers, and the design of the hybrid approaches consolidating the methods of statistics and learning.

Conclusion: The current paper introduces the example of Secured Image which is a detailed and interpretable approach to discovery of hidden data in digital images based on the analysis of statistic images and the process of supervised machine learning. This is given the drive to work by the increasing abuse of digital images as the covert vessels of concealed messages that

emerges as a significant threat to traditional security systems that often characterize image files as harmless. The proposed system will help in the strengthening of digital communication channels by filling this neglected attack scenario.

The main focus of the study was to determine the possibility of using a lightweight and feature-based machine learning architecture to be able to detect steganographic messages hidden in images without the complexities of using deep- learning based architectures. Formalized experiments prove that well-chosen statistical properties can be used to represent fine changes borne by data embedding. Such characteristics as randomness, pixel dispersion, and so-called distribution shape were proved to be especially effective in differentiating normal and steganographic images created through Least Significant Bit embedding.

Logistic Regression classifier was a good design choice that can work with the proposed system. Its openness to interpretation made it easy to give a clear explanation of the classification behaviour and gain a clear picture on how vari- ous disparate statistical features are utilised in making detec- tion decisions. It proves particularly useful in educational and security-sensitive scenarios, where clarifying what automated decisions are and having confidence in them is the highest priority. The attained detection rate, with a fairly low value of false-positive rate, legitimizes that the proposed methodology is a credible baseline answer to image steganalysis in under experimental conditions.

Another added value of this work is its ability to be fast at calculations. The feature representation in low dimensions and lightweight classification model draw up the short processing time and the consummation of small resources. In compar- ison with steganalysis systems that rely on deep-learning, the system tends to utilize a big dataset along with special hardware and long training times to achieve good results, the SecuredImage system fits on regular computing platforms. This makes the methodology appropriate in a large image analysis case, classroom context, and when pre-screens are needed and prompt decision-making is required.

The encouraging outcomes are not enough, despite which the limitations of the offered system also have to be mentioned. The detection system is more geared towards the spatial- domain steganography methods that are LSB-based embedding in particular. This means that it can lose its efficiency in the more advanced steganographic techniques by using frequency domain operation or by using adaptive embedding techniques. In addition, pictures with high levels of natural noise or com- plicated textures can sometimes produce statistical features of the steganographic pictures resulting in a misidentification. These limitations reflect the nature of trade-offs with methods of statistics based on pure features.

The results of the current research provide an avenue to potential research and improvement in the future. A possible avenue is further developing the system in the future to be able to identify frequency-domain steganography systems that are commonly used in compressed image formats like JPEG. Features frequency based like Discrete Cosine Transform
coefficients would make it more resistant to a wider range of embedding techniques. The other avenue that can offer hopeful future is the incorporation of texture and structural features, which can contribute to distinguishing the natural image complexity and steganographic changes.

Future research can also include the study of hybridization classification methodology, which uses statistical elements with lightweight deep-learning models. These hybrid systems have the potential to be able to make higher detection accuracy and, at the same time, maintain some interpretation and computer performance. Increasing the dataset to more compre- hensive and diverse image set, as well as different embedding rates and payloads, would also better equip the system with generalisation capacity, and provide more information about its practical viability in the real world.

Besides, the suggested system may be enveloped beyond single experimentation by integrating it into the real-world processes. They can be used in websites and email systems to scan images as part of email security, in web platforms to filter the content in real time, and in forensic tools to analyze a specific computer crime. Testing the system under these real-life conditions would provide the system with important input on the effectiveness and usefulness in practice.

To sum up, the system SecuredImage proves that a sta- tistically based well-designed machine-learning solution can be efficient in terms of detecting any hidden information within the digital image

without compromising the ease, understandability, and efficiency. The suggested methodology would form a solid base about image steganalysis and offer a strong foundation in terms of future research. This work contributes substantially to the overall effort of achieving the security of digital media against disguised covert methods of data-hiding.

References

1. N. Provos and P. Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE Security Privacy, vol. 1, no. 3, pp. 32–44, May–June 2003.
2. J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications, Cambridge, U.K.: Cambridge University Press, 2009.
3. R. Chandramouli and N. Memon, "Analysis of LSB Based Image Steganography Techniques," in Proc. IEEE Int. Conf. Image Processing, Vancouver, BC, Canada, 2000, pp. 1019–1022.
4. T. M. Cover and J. A. Thomas, Elements of Information Theory, 2nd ed. Hoboken, NJ, USA: Wiley, 2006
5. M. Johnson and S. Katzenbeisser, "A Survey of Steganographic Tech- niques," in Information Hiding Techniques for Steganography and Digi- tal Watermarking, Norwood, MA, USA: Artech House, 2000, pp. 43–78.
6. J. Fridrich and M. Goljan, "Practical Steganalysis of Digital Images: State of the Art," in Proc. SPIE Security and Watermarking of Multi- media Contents, vol. 4675, 2002, pp. 1–13.
7. Tiwari, M., & Darbari, S. (Eds.). (2023). Emerging trends in computer science and its application (p.11). BhupalArya.Routledge. https://www.routledge.com/Emerging-Trends-in- Computer-Science-and-Its-Application/Tiwari-Darbari/p/book/9781032999012.
8. Bhupal arya. "Design a wireless network scenario using CBR." Scope Journal 13, no. 3 (2023): 22-30, https://scope/journal.com/publication/2023/September/33/14/3?token=9b40895f80cac539822676c5788f086a&da=01250116182223
9. . Arya, Bhupal,"Simulation-based Evaluating AODV Routing Protocol Using Wireless Networks." In Applied Data Science and Smart Systems chapter 49. Taylor & Francis,(2023).
10. . B. Arya, A. Kumari, and J. Kumar, "Comparative analysis of wireless routing protocols for security threat—A review," in *Emerging Trends in Computer Science and Its Application*, pp. 60–64, 2021.
11. B. Arya and J. Kumar, "Design a wireless network scenario using CBR," *SCOPE*, vol. 13, Sep. 2020. [Online]. Available: https://scope-journal.com/publication/20
12. Kumari and J. Kumar, "Intelligent detection of cyber threats in wireless networks using machine learning algorithms," *International Journal of Environmental Sciences*, vol. 11, no. 14s, pp. 1783–1794, 2025.
13. J. K. Bhupal Arya and A. Kumari, "Wireless network with machine learning and deep learning techniques," in *Emerging Trends in Computer Science and Its Application*, vol. 1, pp. 71–79, 2021.
14. Bhupal Arya and A. Kumari, "Advanced IDS architecture for threat analysis in modern wireless networks," *Journal of Information Systems Engineering and Management*, vol. 10, no. 4, pp. xx–xx, 2024.
15. R. Chaudhary, B. Kinkar, and B. Arya, "Zero Waste Chain: A Smart Platform for Bridging Food Waste and Food Need," American Journal of Education and Evaluation Studies, vol. 3, no. 1, pp. 1–Jan. 2026, E-ISSN: 2997-9439.
16. R. Chaudhary, B. Kinkar, and B. Arya, "Zero waste chain: A smart platform for bridging food waste and food need," *American Journal of Education and Evaluation Studies*, [vol. __, no. __], pp. -, [year]. [Online]. Available: **https://semantjournals.org/index.php/AJEES**
17. S. Kumar, S. Kumar, and B. Arya, "Real-time deployment of AI-based predictive maintenance in a manufacturing plant using edge computing and streaming sensor data," *J. Appl. Bioanal.*, vol. 11, no. 6s, pp. 1-11, Nov. 2025, doi: 10.53555/jab.v11i8.1730.