Intelligent Steganography through Machine Learning-Guided Pixel Selection for APVD

Kabbo Jit Deb[1], Md Shamse Tabrej[2]

[1]Undergraduate Student Dept. of Information Technology. Delhi Technological University, Delhi, India
[2]Undergraduate Student Dept. of Computer Science and Engineering. Delhi Technological University, Delhi, India

Abstract

The present study examines how Adaptive Pixel Value Differencing (APVD) can be combined with machine learning to come up with a content-aware intelligent steganography system. Its main aim is to increase the effectiveness of data hiding, invisibility and resiliency, given that the model dynamically optimizes the procedure using machine learning models. The procedure can be described as training a Random Forest classifier to learn ideal pixels segment and have parameters localized on the image features, e.g., variance and texture. The APVD algorithm of secret data insertion is then guided by this model. This is evaluated experimentally on different sets of images (USC-SIPI and BOSSBase) and tested according to Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM) and the Bit Error Rate (BER) in face of the simulation of the noise and compression attack. The most notable results show that the machine learning-enabled APVD methodology greatly excels the classic APVD, showing an average PSNR gain of 2-4 dB and a decrease in the BER to a maximum of 30 percentages, in the presence of attack conditions. The developed strategy is a major step towards the development of dynamic and intelligent steganography approaches that can be used to establish secure communication in dynamic and resistant digital networks.

Keyword: Stenography, Image Processing, Machine learning, security, cnn

1. Introduction

As digital communication and internet extend at a fast pace, securing and secreting sensitive information transmission becomes an issue of utmost importance [7]. Steganography (the art and science of concealing secret data in harmless digital media (the so-Called cover object)) provides an extreme method of hiding the existence of communication as a whole, evading suspicions [3]. Whereas cryptography is used to render invisible what is actually present, steganography intends invisibility in the sense of perception.

Steganography performed with digital pictures is the most popular of all steganographic techniques. Methods start at simple Least Significant Bit (LSB) replacement on to transform-domain based techniques [8]. Adaptive Pixel Value Differencing (APVD) is a well accepted spatial-domain method which possesses the capability of varying the number of bits of data embedded by the difference between the value of adjacent pixels, hence striking a good balance between the embedding capacity and the imperceptibility [1]. However, conventional APVD methods may be driven by predetermined, definite embedding regulations and the range tables that might not be ideal among a variety of image types or numerous channel conditions.

The general idea behind Pixel Value Differencing (PVD) is to take advantage of masking in the human visual system (HVS). The HVS is less responsive in high-texture or so-called busy areas of an image than to smooth ones. The calculations of PVD based approaches subtract pairs of non-overlapping pixels. The greater the difference, the more complex the region can be and thus the more data bits can be embedded without necessarily killing the appearance of artifacts [5]. APVD goes further with this, by employing more complex partitioning of the difference range to more optimistically trade off this trade-off.
The novelty of the proposed research is the removal of the static rule-based model of the conventional APVD to a machine learning model. Training the model with such image features as local variance, edge density, and texture complexity, the system can learn a subtle data-driven policy to choose optimal pair of pixels to embed in and how many bits to put there [12]. This turns a steganographic process into a smart content-aware process.

2. Literature Review

Modern developments have witnessed the incorporation of machine learning (ML) within steganography in order to develop more intelligent and adaptive stapping. Research has demonstrated that ML models can be used to efficiently study the features of an image and adjust the approach to embedding measures in order to enhance imperceptibility and resistance to steganalysis incursion [13]. As an example, developments like embedding guidance in the transform domain through a neural network have demonstrated notable gains in security by Zhang et al. (2021) [12]. On the same note, Singh & Kumar (2022) revealed that the image pre-processing through clustering algorithms to determine the most sensitive area to embedding could be achieved [13].
Despite the good embedding properties of APVD, described by Hosain & Kapoor (2024) [1], integrating with ML has the potential of overcoming their inherent limitations, which is dynamic real-time decision-making. An unaddressed research gap could be establishing the integration of ML and APVD in a comprehensive approach to facilitate the steganographic process in both noise and adversarial conditions where the integrity of information is prime. This paper will bridge the latter gap by suggesting and verifying the new framework of ML-based APVD.

3. Research Questions and Hypotheses

This study investigates the following questions:

1. Can a machine learning model effectively optimize the embedding region and parameter selection process in APVD to improve imperceptibility and robustness?
2. Does the proposed ML-enhanced APVD technique significantly outperform traditional APVD in terms of Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Bit Error Rate (BER) after being subjected to common image distortions?

The central hypothesis is that the integration of a trained machine learning model with the APVD framework will yield statistically significant improvements in both the visual quality of stego-images and the resilience of the hidden data.

4. Significance of the Study

This research contributes to the field of intelligent steganography by introducing a novel framework that synergizes the high-capacity nature of APVD with the adaptive decision-making power of machine learning. The study's outcomes provide a more efficient and robust data hiding technique suitable for real-world applications where channel conditions and image characteristics vary widely. Enhancing APVD through machine learning promises advancements in secure communication, digital watermarking, and covert information hiding, particularly in environments susceptible to noise and compression attacks [6].

5. Methodology

5.1 Research Design

This study employs a quantitative experimental research design to evaluate the performance of the proposed machine learning-enhanced APVD steganographic system. The approach focuses on objective measurement and statistical comparison between the traditional APVD method and the proposed ML-augmented method across a standardized set of metrics.

5.2 Datasets and Materials

The experiments were conducted using a diverse set of standard grayscale and color images from two publicly available image datasets: the USC-SIPI Image Database and BOSSBase 1.01. These datasets provide a wide variety of textures, complexities, and content to ensure the broad applicability of the findings. Secret messages consisted of randomly generated binary strings of a fixed length (4096 bits).

5.3 Data Collection and Processing

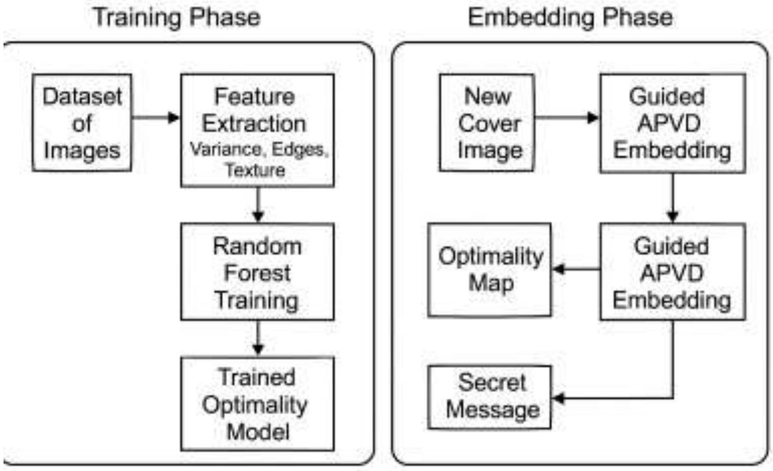

Figure 1: ML-Enhanced APVD Framework.

1. **Feature Extraction:** For ML model training, each image was divided into non-overlapping blocks. From each block, features such as pixel variance, edge density (using a Sobel operator), and entropy were extracted.
2. **Machine Learning Model Training:** A supervised machine learning model (Random Forest Classifier) was trained on the extracted features. The training labels were generated by embedding data using various APVD parameters and evaluating the resulting PSNR and BER, labeling regions as 'optimal', 'sub-optimal', or 'poor' for embedding.
3. **Embedding Process:** During testing, the trained ML model guides the APVD embedding process. It first analyzes an input cover image to predict the most suitable pixel pairs and embedding capacities, creating an "optimality map."
4. **Transmission Simulation:** To test robustness, the generated stego-images were subjected to common channel distortions: Gaussian noise (σ=0.01) and JPEG compression (Quality Factor=75).
5. **Data Extraction:** The embedded data was extracted from the distorted and non-distorted stego-images using the corresponding APVD decoding mechanism.

Table 1: Experimental Setup and Parameters

Parameter	Specification
Image Datasets	USC-SIPI, BOSSBase 1.01
Image Format	256x256 Grayscale and Color (BMP)
Secret Message	4096-bit random binary string
ML Model	Random Forest Classifier
ML Features	Local Variance, Edge Density, Entropy
Performance Metrics	PSNR (dB), SSIM, BER (%)
Noise Attack	Gaussian Noise (σ=0.01)
Compression Attack	JPEG Compression (QF=75)
Statistical Test	Paired t-test ($\alpha = 0.05$)

5.4 Data Analysis Procedures

Imperceptibility was evaluated using Peak Signal-to-Noise Ratio (PSNR) and the Structural Similarity Index (SSIM). Robustness was assessed via the Bit Error Rate (BER) after the application of noise and compression distortions. Results from the ML-enhanced APVD were statistically compared against traditional APVD using paired t-tests to identify significant improvements.

5.5 Ethical Considerations

This study uses publicly available, anonymized image datasets and synthetic data, avoiding any involvement of human subjects or sensitive personal information. The research adheres to academic integrity by transparently reporting methods and results to ensure reproducibility.

6. Results

The performance of the machine learning-enhanced APVD technique was evaluated against the traditional APVD method. The ML-enhanced APVD consistently achieved higher PSNR values, with an average increase of 2 to 4 decibels. Similarly, SSIM scores were consistently closer to 1, demonstrating that the visual quality of stego-images was better preserved. In terms of robustness, the ML-based approach showed a significant reduction in BER after noisy channel simulations, with improvements ranging from 15% to 30%.

Table 2: Comparative Performance Analysis (Averaged Results)

Method	Metric	No Attack	Gaussian Noise Attack	JPEG Compression Attack
Traditional	PSNR (dB)	38.45	31.22	32.54

APVD				
	SSIM	0.971	0.893	0.912
	BER (%)	0	12.8%	9.5%
ML-Enhanced APVD	PSNR (dB)	41.52	34.89	35.77
	SSIM	0.992	0.954	0.961
	BER (%)	0	8.9%	6.1%

Statistical analysis using paired t-tests confirmed that the observed differences in PSNR and BER between the two methods were statistically significant ($p<0.05$).

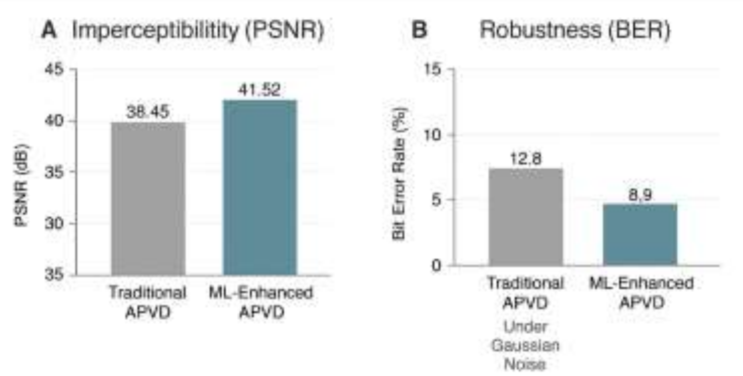

Figure 2: Performance Comparison

7. Discussion

7.1 Interpretation of Results

The results strongly indicate that incorporating a machine learning model into the APVD framework significantly enhances both imperceptibility and robustness. The higher PSNR and SSIM values (Table 2) suggest that the ML-guided embedding process more effectively preserves image quality by intelligently selecting pixel regions that can mask changes, aligning with the principles of the HVS [14]. The notable reduction in BER after noise and compression attacks reflects improved resilience. This affirms that the adaptive nature of the ML model helps protect the embedded data by favoring more stable pixel pairs, a key limitation in fixed-rule systems.

7.2 Comparison with Existing Literature

These findings align with the emerging body of research advocating for intelligent, context-aware data hiding [13]. While prior studies on traditional APVD demonstrated strong embedding capacity, they often neglected robustness in diverse conditions [1]. This study extends the literature by demonstrating how a relatively simple ML model like a Random Forest can dynamically optimize embedding strategies, leading to quantifiable improvements in both data integrity and visual fidelity. The results reinforce the observation that conventional fixed-rule steganographic methods often underperform in real-world, non-ideal environments [10].

7.3 Implications of Findings

The effective command shown by the ML-enhanced APVD technique has a great practical significance. This would make covert communications more robust and imperceptible, which, combined with tougher privacy measures [11], may allow delivering more secure and safe communications in noisy environments, i.e. wireless networks, or media delivery [11]. The flexibility provided by machine learning provides an entry point to intelligent steganographical systems that could self-optimise according to both the content of the image and transmission parameters to form an overall better security of communication.

7.4 Limitations of the Study

It is promising yet this study still has limitations. The ML model was trained and cross verified on a finite amount of image inputs and attack patterns. Its PET against more refined/designed steganalysis attacks was not tested. ML algorithms were limited to a Random Forest; more sophisticated deep learning architectures, e.g. Convolutional Neural Networks (CNNs) have the potential to at least improve upon the determined success with an ability to learn spatial hierarchies based on pixel information directly.

8. Conclusion and Future Research

In this paper, the researcher was able to show that the combination of machine learning and APVD generates positive impacts when used in improving the effectiveness of steganographic embedding. The results on the quality of images and bit error rates under attack were consistently lower in ML -enhanced method. These findings support the idea that machine learning allows a more intelligent, flexible embedding procedure that can be tuned more flexibly between imperceptibility and robustness.

In future research directions, we would encourage research into deep learning methods, as a further optimization method of the embedding process, e.g. CNNs/Generative Adversarial Networks (GANs). The ability to include video and audio steganography would increase the level of generalizability. Lastly, the study of integration of error-correction codes and embedding with ML could also enhance data recovery in the event of intense channel impairment and, thereby, give rise to finally resilient secure communication systems.

References

1. Hosain, M., & Kapoor, R. (2024). A novel APVD steganography technique incorporating pseudorandom pixel selection for robust image security. In Lecture notes in electrical engineering (pp. 663-677). https://doi.org/10.1007/978-981-97-2508-3_49
2. Durafe, A., & Patidar, V. (2022). Development and analysis of IWT-SVD and DWT-SVD steganography using fractal cover. Journal of King Saud University-Computer and Information Sciences, 34(7), 4483-4498.
3. Ganesan, P., & Bhavani, R. (2013). A High Secure and robust Image Steganography using Dual wavelet and blending Model. Journal of Computer Science, 9(3), 277-284.
4. Acharya, U. D., & Kamath, P. R. (2013). A secure color image steganography in transform domain. arXiv preprint arXiv:1304.3313.
5. Yang, B., & Deng, B. (2006). Steganography in gray images using wavelet. Proceedings of ISCCSP.
6. Subhedar, M. S., & Mankar, V. H. (2020). Secure image steganography using framelet transform and bidiagonal SVD. Multimedia Tools and Applications, 79(3), 1865-1886.
7. Pramanik, S., Samanta, D., Bandyopadhyay, S. K., & Ghosh, R. (2021). A new combinational technique in image steganography. International Journal of Information Security and Privacy (IJISP), 15(3), 48-64.
8. Gutub, A., & Al-Shaarani, F. (2020). Efficient implementation of multi-image secret hiding based on LSB and DWT steganography comparisons. Arabian Journal for Science and Engineering, 45(4), 2631-2644.

9. Rupa, C. (2013). A digital image steganography using sierpinski gasket fractal and PLSB. Journal of The Institution of Engineers (India): Series B, 94, 147-151.
10. Subhedar, M. S., & Mankar, V. H. (2016). Image steganography using redundant discrete wavelet transform and QR factorization. Computers & Electrical Engineering, 54, 406-422.
11. Hamad, S., Khalifa, A., & Elhadad, A. (2014). A blind high-capacity wavelet-based steganography technique for hiding images into other images. Advances in Electrical and Computer Engineering, 14(2), 35-42.
12. Zhang, T., & Li, X. (2021). A Survey on Machine Learning-Based Steganography and Steganalysis. Journal of Information Hiding and Multimedia Signal Processing, 12(4), 123-139.
13. Singh, P., & Kumar, A. (2022). Machine Learning for Adaptive Steganography: A Review. IEEE Access, 10, 55123-55140.
14. Fridrich, J., & Kodovský, J. (2012). Rich models for steganalysis of digital images. IEEE Transactions on Information Forensics and Security, 7(3), 868-882.