International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-14 Issue-2, July 2025

Comprehensive Comparison of Image Steganography Techniques with Security Enhancement

Hessah Alshamrani, Samah Alajmani, Raneem Yousif Alyami, Ben Soh

Abstract: ***This paper presents an extensive comparative analysis of several image steganography methods, examining their efficiency in terms of capacity, media quality, resistance to detection, and computational efficiency. Steganography, the science of hiding sensitive data within a larger image, is vital for secure data transmission. The research compares five of the most used techniques: Least Significant Bit (LSB), RGB, Pixel Value Differencing (PVD), Feature-Based Optimised Steganography, and the VisionStego AI System. The introduction emphasises the importance of cryptography and steganography in concealing data. Cryptography encrypts the data, whereas steganography hides data within multimedia content. Image steganography conceals information by distorting cover images in a way that makes the information difficult to retrieve. Steganalysis is crucial in the retrieval of concealed information. LSB, RGB, and PVD are traditional steganography methods that suffer from drawbacks such as low capacity, media degradation, and detectability. This study will contrast and compare the performance of LSB, RGB, PVD, Feature-Based Optimized approaches, and the VisionStego AI System. A literature review explains various methods in steganography and their evolution. Scientists have discovered that combining encryption and steganography provides enhanced data security. Advanced techniques, such as CNN-based and GAN-based methods, have replaced traditional approaches. Hashing techniques and robust linked list steganography have been proposed to offer greater protection. Generative adversarial networks (GANs) and invertible steganography networks (ISNs) have emerged as methods to enhance capacity, security, and robustness. The methodology section compares five steganography techniques: LSB, RGB, PVD, Feature-Based Optimized Steganography, and VisionStego AI System. The performance of each method is based on capacity, media quality, detection resistance, and computational complexity. The comparison metrics are Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), Mean Squared Error (MSE), embedding time, and extraction time. The LSB technique substitutes the least significant bit of the cover image with secret information. It is simple and fast, but has low capacity and is detectable. The test results indicate that LSB offers high-speed embedding and good quality, but has low capacity and security. The RGB technique disperses the secret data in the red, green, and blue components of the cover image. It offers better data hiding quality and fewer visual distortions compared to LSB, but with a reduced extraction rate; hence, it is not suitable for applications that require rapid data retrieval. The PVD technique conceals information by looking for pixel value differences in the cover image. It is less detectable to manipulation and reduces visual noise. But it is more complicated to operate and can be identified when image enhancement techniques are applied. Feature-Based Optimized Steganography uses information embedding based on some features of multimedia, i.e., image corners and edges. It incorporates data encryption and compression before information embedding, lowering PSNR, SSIM, and MSE. The scheme offers satisfactory security and minimum storage space, but increases extraction and embedding times due to compression and encryption. The VisionStego AI System utilises artificial intelligence to automatically calculate effective places within the image where data must be embedded. It embeds text data in a digital format and calculates areas of importance in the image through saliency detection. It offers good security, optimised storage size, does not distort the image, and provides simple retrieval, along with outstanding security. The outcomes of the performance test reveal that the VisionStego AI System achieves a satisfactory compromise between data concealment quality, storage efficiency, and processing efficiency. The discussion and results section demonstrate that the VisionStego AI System outperforms other systems in preserving image quality after embedding. It achieves high PSNR and SSIM, which are metrics for zero and imperceptible distortion. Feature-Based Steganography maximizes the spreading of data, thereby enhancing concealment performance with no impact on visual coherence. Low measures of MSE confirm that the embedding procedure ensures a subtle and almost imperceptible modification of the image. The VisionStego AI System can offer hiding capacity preservation while maintaining image quality, providing large-scale data embedding in a lossless, imperceptible form. VisionStego AI is furthermore less vulnerable to steganalysis attacks compared to conventional LSB-based methods. With the addition of encryption and compression processes, this further enhances its security. The conclusion and future work focus on how the projected VisionStego AI System exhaustively surpasses LSB-based techniques in terms of concealment capability and confidentiality, while retaining higher image fidelity and resilience against steganalysis attacks. The system's ability to perform optimal data embedding without distorting the structural integrity of the image is evident from the high values of PSNR and SSIM. Future research could focus on optimising the embedding process according to other image characteristics, conducting additional experiments on different types of images, and enhancing detection resistance and extraction resistance using higher-level encryption and obfuscation techniques.***

Keywords: Image Steganography, Least Significant Bit, Pixel Value Differencing, Feature-based Optimise & VisionStego AI.

Manuscript received on 01 May 2025 | First Revised Manuscript received on 09 May 2025 | Second Revised Manuscript received on 17 June 2025 | Manuscript Accepted on 15 July 2025 | Manuscript published on 30 July 2025.

*Correspondence Author(s)

Hessah Alshamrani*, Department of Cyber Security, Taif University, Taif, Saudi Arabia. Email: H.alsh14@hotmail.com, ORCID ID: 0009-0008-2927-5194.

Dr. Samah Hazzaa Alajmani, Assistant Professor, Department of Information Technology, Taif University, Taif, Saudi Arabia. Email ID: s.ajmani@tu.edu.sa, ORCID ID: 0009-0000-7152-9559

Dr. Raneem Yousif Alyami, Assistant Professor, Department of Information Technology, Taif University, Taif, Saudi Arabia. Email ID: Rayami@tu.edu.sa, ORCID ID: 0000-0002-3711-5106.

Dr. Ben Soh, Associate Professor, Department of Computer Science and Information Technology, La Trobe University, Melbourne, Australia. Email ID: b.soh@latrobe.edu.au

Abbreviations:
LSB: Least Significant Bit
RGB: Red, Green, Blue
PVD: Pixel Value Differencing
PSNR: Peak Signal-to-Noise Ratio
SSIM: Structural Similarity Index
MSE: Mean Squared Error
EMD: Exploiting Modification Direction
MBNS: Multiple-Based National System
CNN: Convolutional Neural Network
GAN: Generative Adversarial Network
DCT: Discrete Cosine Transform
RSA: Rivest-Shamir-Adleman
RLL-SWE: Robust Linked List Steganography Without Embedding
ISN: Invertible Steganography Network
MNMI: Modified Neighbour Mean Interpolation
3DES: Triple Data Encryption Standard
MD5: Message Digest Algorithm 5
AES: Advanced Encryption Standard
IMStego: Image Steganography Tool

I. INTRODUCTION

Steganography and cryptography are two essential techniques for securing information, but they serve different purposes. While cryptography focuses on encrypting data to make it unreadable without a decryption key, steganography conceals sensitive multimedia data within a larger image, ensuring covert communication. Image steganography specifically manipulates the cover image to hide data, making it difficult to detect. However, steganalysis plays a crucial role in extracting concealed information and determining whether an image contains hidden messages.

Steganography is widely used for secure data transmission across public networks, with traditional methods relying on pre-selected cover images [1]. These techniques can be categorized into transformation domain and spatial domain approaches, with the least significant bit (LSB) method being the most common. Various embedding techniques exist, including exploiting modification direction (EMD), pixel value differencing (PVD), least significant bit (LSB), and multiple-based national system (MBNS). LSB, RGB, and PVD are widely used but face challenges such as limited capacity, degradation in media quality, susceptibility to detection, and reduced computational performance. While individual techniques have been studied, there is a lack of comprehensive research comparing their effectiveness. The increasing need for steganography techniques that balance capacity, media quality, detection resistance, and computational efficiency highlights a critical gap in understanding the performance differences between LSB, RGB, and PVD methods. The absence of a thorough comparative study makes it difficult to select the optimal technique for various applications. Addressing this gap will help improve existing processes and foster the development of more efficient data-hiding technologies [2]. This research aims to address key questions: How efficient are LSB, RGB, PVD, and feature-based optimised techniques, as well as the VisionStego AI system, in terms of capacity, media quality, and detection resistance? Which of these techniques is most suitable for different applications based on metrics such as capacity, quality, security, and performance? What are the strengths and weaknesses of these methods when evaluated across different scenarios? The main objective of this study is to recommend the most suitable technology for various practical applications based on comparative results. This involves analyzing the working principles of LSB, RGB, PVD, feature-based enhancement, and the VisionStego AI system.

The comparison will focus on key performance aspects, including capacity, media quality after embedding, resistance to detection, and computational efficiency. Understanding the benefits and limitations of these techniques in different scenarios will help refine existing methods and guide future research. A comparative study of data-hiding techniques has some significant advantages. It makes the selection of an appropriate technique for specific applications easier. For example, LSB is apt for quick and simple data hiding, RGB offers increased storage capacity, PVD provides a compromise between high capacity and image quality, and feature-based optimization ensures high security and minimal visual distortion. The VisionStego AI system has been suggested to achieve maximum protection and make detection hard. Second, performance analysis provides information on changes in capacity, security, stegoimage quality, and computational efficiency.

PVD and RGB methods are secure against attacks such as histogram analysis, while feature-based optimization offers better security with minimal image impact. VisionStego AI is highly effective at guarding sensitive information within images. PVD and feature-based optimisation provide a suitable compromise between image capacity and data distortion in this work, while LSB offers high quality but with limited capacity. Security functions, such as the use of RGB or feature-based optimization, introduce complexity which renders hidden information more difficult to locate. Some techniques, such as feature-based optimization, scale better for larger images and applications, while LSB is better suited for simpler applications. A comparison aids in selecting the best approach based on individual requirements, whether the goal is to achieve maximum capacity, enhance security, or preserve image quality. This research will make significant contributions to the field in several ways. It will contrast the real-world performance of all methods on images with varying sizes and quality. A security analysis will contrast their resistance against the most frequent attacks. Novel performance metrics in terms of distortion-to-capacity ratio and the impact of methods on colour and fine details will be proposed. Experimental simulations will assess capacity, PSNR, SSIM, MSE, embedding time, and extraction time. A key innovation in this study is the development of AI-based technology to identify optimal hiding locations in images before data embedding, thereby enhancing both security and data concealment. This paper is organized as follows: Section 2 provides a detailed description of related studies. Section 3 outlines the proposed methodology, detailing the experimental setup, datasets used, and practical applications, followed by the results and their analysis. Section 4 presents the conclusions drawn from this study and discusses future directions for work in this domain. Finally, Section 5

lists the references that supported this research.

II. LITERATURE REVIEW

The rapid development of multimedia technologies has enabled the widespread transmission of images over public channels. Consequently, much attention has been drawn to the secure transmission of such images.

Encryption methods are often used to protect multimedia data; however, when images are encrypted, they appear random and meaningless, which could potentially make it even easier for attackers to suspect that concealed information is present. To overcome this challenge, information concealment techniques such as digital watermarking and insertion have been established.

Digital image concealment refers to a mechanism that conceals hidden information within a cover picture, making the embedded content invisible or undetectable to the naked eye. It is intended to render the image containing the hidden data in a way that does not reveal the presence of the secret information, thereby enhancing transmission security.

Statistical image models play a crucial role in concealing information in less perceptible pixels, thereby enhancing the security of concealed data. Despite the numerous advantages of steganography techniques, challenges exist in the process of hiding information. The challenges range from strengthening the capacity of concealed data to making it immune to detection using various attack tools.

Here, a summary of the available literature on methods for hiding information in images, with a focus on image steganography techniques, is provided. There shall also be a reflection on the improvement measures used to ensure the non-detectability of the hidden information, as well as debates on how methods have evolved, including the challenges faced in their application and the solutions offered to further improve their application. The research paper "A comparative study and literature review of image steganography techniques" reviews the use of steganography methods to embed information into digital images. The paper elaborates on the strengths and weaknesses of each technique, comparing various data hiding methods. The study highlights the combined use of encryption and steganography for enhanced data security and recommends future studies in this area. However, it needs improvement, i.e., incorporating experimental steps and comparing each technique in actual scenarios. The article also identifies the need to avoid using steganalysis procedures, but does not include advanced techniques to counter them. Overall, the research contributes significantly to data hiding by examining various methods, but might require additional deeper security analysis and implementation in practice [3]. The 2022 research presents a new steganography technique for digital images based on the Least Significant Bit Substitution Method. The method embeds a hidden message into the blue channel of a cover image, mixes it with a magic matrix, and uses a multi-level encryption algorithm to encrypt the difference between the two channels. The method outperforms the current LSB-based embedding algorithms in terms of PSNR, imperceptibility, capacity, and robustness [4]. The 2021 article categorized image-hiding techniques as traditional, CNN-based (Convolutional Neural Network), and GAN-based approaches. The deep learning methods outperformed traditional methods, producing high-quality, camouflage images that are resistant to reverse engineering. The challenges encountered included the lack of benchmark data, the trade-off between capacity and security, and stability issues. Quantum artificial intelligence, hybrid technology, and GAN model stability are to be explored in the future [5]. The 2024 paper "A Review of Image Steganography Based on Multiple Hashing Algorithms" explains how hashing algorithms can be used for enhancing security. It provides an overview of image steganography, a technique that conceals secret information within images. The paper utilises the Discrete Cosine Transform (DCT) for decomposing images into frequencies, the RSA (Rivest-Shamir-Adleman) and Blowfish algorithms as encryption methods, and the Hash-LSB Approach for data hiding. The article suggests a comparison among various hashing algorithms, increasing the strength against steganalysis attacks, and the scope of application in cybersecurity, digital proper protection, and secure communication [6].

An article published in 2024 proposed the RLL-SWE (Robust Linked List Steganography Without Embedding) technique for concealing information in intelligent networks, rendering the hidden communication immune to cyberattacks. It utilises image features to select relevant lists, thereby enhancing security. Methods include extracting robust features, reconstructing them as a multi-head linked list, making it increasingly attack-resistant, and exploring whether an optimal list can be identified.

The study concludes that RLL-SWE is a crucial development in information concealment, offering high security against detection and intrusion [7]. The research paper "StegaStyleGAN: Towards Generic and Practical Generative Image Steganography" aims to develop a secure image hiding system using generative technology. It utilises StyleGAN2, a high-definition image generation platform, and incorporates a differential privacy data modifier and a secret data extractor. The constructed StegaStyleGAN (Generative Adversarial Network) model significantly outperforms the current system in terms of security, capacity, and robustness [8]. The 2021 paper titled "High-Capacity Image Steganography Based on Reversible Neural Networks" introduces the Invertible Steganography Network (ISN), a novel steganography network with enhanced payload capacity, high-quality image recovery, and state-of-the-art performance with strong detection avoidance. The ISN (Invertible Steganography Network) employs a single invertible network for both forward and backwards passes, sharing all parameters and ensuring the high-quality generation of both containers and exposed hidden images. Adjusting parameters can improve the quality of the container image while maintaining the revealed image quality above 38 dB [9]. A 2023 study investigated enhancing the performance of reversible data hiding (RDH) by integrating the Modified Neighbour Mean Interpolation (MNMI) method with logarithmic transformation. The technique enhances pixel accuracy and minimises distortion, achieving an embedding capacity of

1,300,000 bits while maintaining a peak signal-to-noise ratio (PSNR) of 28.5 dB. The study concludes that combining Modified Neighbour Mean Interpolation (MNMI) with a logarithmic transformation enhances data capacity and image quality, proving its effectiveness in RDH applications. To improve the paper's impact, it is recommended to include more experimental results, user research on perceptual quality, and comparisons with state-of-the-art techniques [10]. The study "Evaluation of LSB Steganography on Image File Using 3DES (Triple Data Encryption Standard) and MD5 (Message Digest Algorithm 5) Key" emphasizes the importance of data security in digital communications. It evaluates the combination of steganography and encryption techniques, highlighting the Triple DES (3DES) algorithm's resistance to computational attacks. The study also emphasizes diversification of significant relevance in the 3DES algorithm for enhanced security [11].

The 2021 textual steganography research highlights the need to safeguard data and documents. The study explains encoding, encryption, and embedding procedures, and how they are used to secure individual information against forgery and counterfeiting. The article categorises text encryption approaches into linguistic, format-based, and random and statistical generation, and recommends security improvements and the adoption of new technologies, and some proposals for research improvement.

More information on which method has been used, and an additional description of the more intricate data collection and analysis. It is preferable to specify the software or tool used and describe how it contributed to the research, including case studies or experiments, with a primary focus on providing a valuable assessment of the proposed approach.

The relevance of the study can be enhanced by highlighting the potential applications of the proposed method across various industries. To further enhance the findings and discussion section, a more precise explanation of the findings, along with a comparison to existing hypotheses or studies, would be beneficial. By elucidating the method's accuracy or effectiveness in comparison to alternative methods [12], the 2024 study explores a secure file-sharing system using image steganography and cryptography techniques. It combines encryption with image hiding to enhance the security of data transmission. Techniques include AES (Advanced Encryption Standard) encryption, LSB steganography, XOR techniques, and the IMStego tool. The combination of encryption and concealment enhances security, increases stealth capability, and improves resistance to attacks that rely on image analysis and the extraction of hidden data. But there were some restrictions: the current method only works with PNG and BMP images, which reduces its flexibility with other image formats. A public key was not used in the encryption, which may reduce the flexibility of data sharing with multiple parties [13]. The 2019 article "A Brief Review of Image Steganography Techniques" provides a comprehensive analysis of image steganography methods, with a focus on Transform Domain techniques. The study determines that frequency domain techniques offer better security as they conceal information within the image and cannot be detected or accessed unauthorized. Techniques used to hide information are cryptography, watermarking, fingerprinting, and compression. The study finds that frequency domain techniques are more effective than spatial domain techniques, as they conceal data in frequency coefficients, making them less noticeable and more difficult to detect. The study recommends ongoing development and improvement of frequency domain technologies, data scrambling techniques, and comparing algorithm performance in real-world applications [14]. The 2023 report "Steganalysis of Steganography Based on Chat" discusses timing steganography techniques in chat applications. The report analyses user behaviour in chat, which includes reading, writing, and editing before sending. The method identifies unusual behaviour by measuring writing and reading speeds. The study identified some anomalous temporal trends but encountered challenges such as establishing effective detection criteria, categorising errors, and applying the findings to other media. It performs best on text debates. The study proposes a promising, utilitarian approach to identifying temporal cover-ups in chat, but it requires further development to measure most instances accurately. Enhancing algorithms with artificial intelligence methods to improve trend identification. Extending the study to other modes, such as voice calls and video, and measuring the response times accordingly. Identifying alterations over time correlated to hiding from those naturally occurring using machine learning techniques.

III. METHODOLOGY

In ancient times, an intriguing method of secret communication involved shaving the head of an enslaved person, tattooing a hidden message on his scalp, and allowing the hair to grow back. When his hair had grown over the message, he was transported to his destination. Upon arrival, his head was shaved again, and the message appeared. This technique, employed by Aristagoras for sending secret messages, is one of the oldest steganographic methods discovered. Encryption techniques have since evolved into the level of data hiding technology used today. Steganography is widely used today for the secure storage and transmission of confidential data. Extensive research has shown that data can be hidden within various types of media, including images, videos, and audio files. These advancements have made steganography a vital tool in fields that require secure communication and data protection. In this research, we will focus on the field of hiding a secret message in an image, highlighting some spatial hiding techniques. Such as (LSB, RGB, PVD) in addition to Feature-based Optimized techniques with compression and encryption, VisionStego AI technique. A practical comparison was conducted among these five techniques, in addition to enhancing the Feature-based Steganography technique through encryption and compression before data hiding, and developing a new technique (VisionStego AI system) to improve security levels and increase resistance to unauthorised exploitation operations. Python and specialised image processing packages, such as OpenCV

and NumPy, were used to design the studies. The performance of each technique was evaluated using criteria such as extraction resistance and image quality. This section outlines the detailed steps for conducting the research, beginning with data preparation, proceeding through the application of various techniques, and concluding with the evaluation of the results.

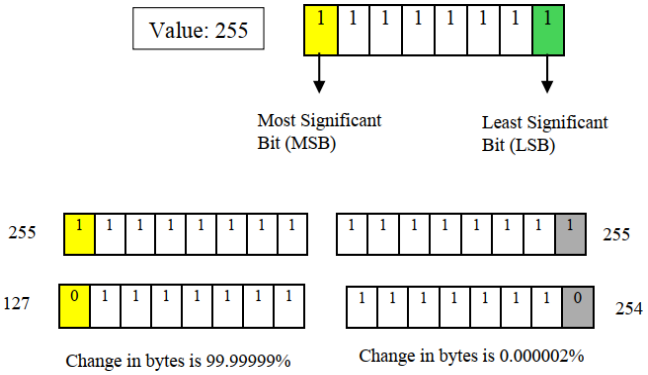
A. LSB (Least Significant Bit) Technique

Steganography is an effective technique for concealing the presence of secret data within a digital object carrier. Images are the most common elements covered in steganography applications. The process of embedding secret information within the image requires intensive calculations and high skills in application programming. As is well known, the rightmost bit has the least significant value in the binary code and is referred to as the "Least Significant Bit (LSB)." LSB is one of the main techniques used in image hiding. The level of precision in image formats falls short of the perceptual capabilities of the human eye. Making a slight change in the least significant bit (LSB) value of the colour components in the image will not be noticeable to the human eye. This subtle change in the bit values of the colour components of the image can be made using the LSB technique. The idea behind the LSB process is not complicated, as it involves making bit value changes in this manner. Tests have also proven that the LSB technique is a suitable method for embedding secret information into carrier objects, such as images, videos, and audio files. In this method, the least significant bit in the host file object is replaced with the bits of secret data to be embedded.

The most familiar carrier object is images. The image that carries embedded secret data is called a hidden image. The goal of steganography is to make the hidden image appear identical to the original image without any distortion caused by the insertion of secret data. The image file on the computer displays different colours and varying concentrations of light in other areas of the image. A 24-bit BMP image is the best type of image file for hiding secret data within it. When the image is of high quality and resolution, it is more suitable for hiding more information within the image. In general, the eighth bit (the farthest to the right) of the colour byte is considered the least important among the other bits and is called the least significant bit. Therefore, the eighth bit of each colour byte can be used to insert one bit of secret information.

When using a 24-bit depth image, you can store three bits of secret information in each pixel of the image by replacing the least significant bits in each colour component (red, green, and blue).

We will need three pixels from the image to hide one byte of secret information, where we modify the least significant bit in the colour components of the image with the corresponding bit of the secret information. The rest of the bits in three pixels remain unchanged. We let the three consecutive pixels be "pixel (i), pixel (i+1), and pixel (i+2)," with the three RGB components.



[Fig.1: Explanation of the LSB (right) and the MSB (left) Concept]

i. Steps to Implement the LSB Technique for Hiding Messages within Images:

The image is loaded, read, and then mapped to RGBA to extract the colour data of each pixel. Each letter of the message is converted into an 8-bit binary digit, and a stop sequence (00000000) is added to indicate that the message is complete. The least significant bit (LSB) of each pixel's red channel (R) is replaced with binary message data. The image is altered once edited and stored with a new extension that carries the encrypted message.

To extract the hidden text from an image, it begins by opening the image and then translating it to RGBA, allowing for the viewing of pixel colour values. The operation proceeds by pulling out the binary data, where the LSB is extracted from the red channel (R) of every pixel and placed in a binary string. The binary data is then split into sets of eight bits, which form a character, and decoded into text that can be read. Extraction continues until it encounters a stop code defined, i.e., the first occurrence of "00000000" (like \x00 in text), indicating the end of the concealed message. The extracted message is then printed after decryption, showing the concealed data.

As evident from Table 1, LSB has good quality and fast embedding but poor capacity and security. The technique is ideal for applications in which small amounts of data are to be hidden without compromising image quality. Still, it is not suitable for applications that demand robust protection against attacks or require large hiding capacities.

Table- 1: Evaluation Results of LSB Steganography

Data set	Capacity (bpp)	PSNR	SSIM	MSE	Embedding Time	Extraction Time
Image 1.png (2000,3000)	0.0002	92.7526	1	3.45e-05	2.71476	2.72595
Image 2.png (460, 736)	0.00354442	80.4972	0.999999	0.000579907	0.144985	0.0989935
Image 3.png (168, 299)	0.0238892	72.0943	0.999993	0.00401471	0.0199969	0.0160437
Image 4.png (578,870)	0.00238635	82.0918	1	0.000401702	0.187292	0.154325
Image5.png (720, 1280)	0.00130208	85.0346	1	0.000203993	0.459533	0.271211
Image6.png (724,1280)	0.00129489	84.7683	1	0.000216894	0.414461	0.28346

B. RGB

The RGB (Red, Green, Blue) model is based on colour generation by mixing the three primary colours —red, green, and blue — in varying proportions. Pixels in digital images and screens are specified in terms of numeric values between 0 and 255 for each of the three colour components. The relationship of the RGB model with the Least

Significant Bit (LSB method: The Least Significant Bit (LSB) method uses the RGB model for hiding information within digital images. This is done by manipulating the least significant bits of either the red, blue, or green component. Mainly, this alteration is applied to the least significant bits of the red component (R). This modification enables data insertion without affecting the visible change in image colours, making it a suitable technique in the field of data hiding (Steganography).

i. Steps to Hide Text using RGB:

- Loading the Image and Converting it to RGBA Format: When the image is opened, it is loaded and converted into RGBA format, allowing access to the colour values of each pixel, including the three-colour channels: Red (R), Green (G), and Blue (B).
- Converting Text to Binary Format: Each character in the text to be hidden is converted into an 8-bit binary representation. This is followed by adding an end-of-message symbol, represented by 00000000 repeated three times, to ensure the identification of the hidden data's termination.
- Hiding Data in the Image: The Least Significant Bit (LSB) in the three-colour channels (R, G, B) is modified to conceal the data within the image. Each 3 bits of the message are distributed across the RGB components of each pixel, ensuring a more balanced and less noticeable insertion of information.
- Saving the Modified Image: Once all the data has been embedded within the image, the modified version is saved under a new name, preserving the original image unchanged.

ii. Advantages of This Method Compared to Traditional LSB (in the R Channel Only):

- Reduced Visual Alterations: Distributing the data across all three colour channels (R, G, B) makes modifications in the image less noticeable compared to altering a single channel.
- Increased Data Hiding Capacity: Utilising all colour channels enables the concealment of a larger amount of data compared to the traditional method, which modifies only one channel.
- Harder to Detect Hidden Data: Since the information is spread across three channels, it becomes difficult to notice the changes with the naked eye, enhancing data security.

The Text extraction from the encoded image of the RGB model by using the Least Significant Bit (LSB) data hiding technique is carried out by following a sequence of consecutive steps. The first step is to open the image and convert it to RGBA format, which allows access to the colour values of all pixels, including the three-channel colours: red (R), green (G), and blue (B). Then, the least significant bits (LSB) of each of the distinct colour channels of each pixel are extracted and concatenated into a sequence of binary numbers. Once the binary string has been formed, it is grouped into sets of 8 bits per character and is converted to readable text. The data extraction continues until the end-of-message code (\x00), ensuring that unwanted data is not read. Finally, the extracted text is displayed once the process has been completed, allowing information hidden in the image to be accessed without compromising its quality or design.

The RGB technique offers superior data hiding quality by preserving the original image with minimal distortion, as evidenced by high PSNR values and an SSIM of 1. It also provides an acceptable embedding speed but lacks support for high data hiding capacity, such as the Least Significant Bit (LSB) technique. The primary disadvantage of this technique is its slow extraction rate, particularly when working with large images; therefore, it is less suitable for applications that require high extraction speed. Overall, the RGB technique is a satisfactory choice for providing good image quality with an average ability to conceal, but not necessarily the best, where rapid extraction speed is required. While this style offers a combination of excellence and visual balance, it is not as usable when capacity is a large extent or quick information retrieval is the main requirement.

Table-II: Evaluation Results of RGB Steganography

Data set	Capacity (bpp)	PSNR	SSIM	MSE	Embedding Time	Extraction Time
Image 1.pn (2000,3000)	0.0002	92.5278	1	3.63333e-05	1.88304	13.7677
Image 2.png (460, 736)	0.00354442	80.5491	1	0.000573015	0.116113	0.228858
Image 3.png (168, 299)	0.0238892	72.0656	0.999995	0.00404125	0.0163214	0.0349994
Image 4.png (578,870)	0.00238635	81.9438	1	0.000415623	0.157616	0.376433
Image 5.png (720, 1280)	0.00130208	84.5609	1	0.000227503	0.333817	0.81395
Image6.png (724,1280)	0.00129489	84.8777	1	0.000211499	0.276946	0.913907

The RGB technique provides exceptionally high quality in hiding data with minimal distortion in the original image, as indicated by extremely high PSNR values and an SSIM value of 1. It also achieves good embedding speed; however, it is not much better in data hiding capability compared to the Least Significant Bit (LSB) approach. The key disadvantage of this technique is its long extraction time, particularly for big images, which makes it ineffective in applications where fast data retrieval is required. In general, the RGB technique is a sufficient method for obtaining good image quality with a medium hiding capacity. Still, it is not always the ideal choice for applications that prioritise fast extraction time. While this strategy is well-balanced in terms of quality and visual stability, it fares poorly if high capacity or rapid data access are the paramount requirements.

C. PVD (Pixel Value Differencing)

Instead of modifying the Least Significant Bit (LSB) as in the conventional method, the Pixel Value Differencing (PVD) method conceals information by utilising pixel value differences within an image. It involves dividing the image into non-overlapping blocks of adjacent pixels and analysing the changes in pixel values within these blocks. By examining these differences, the method determines the

amount of data that can be concealed, with a more responsive and secure steganographic operation.

i. Steps for Practical Application:

Hiding capacity for any difference of pixels between the nearest neighbours relies on pre-defined ranges. The larger the difference in pixel values, the more data can be hidden without loss of image quality. Input text is first written as a sequence of bits (binary mode) and has an end tag (00000000), after which the data enters complete termination. This sequence of the image is processed in horizontal sequences of double consecutive pixels (p1, p2) as they traverse horizontally independently throughout the image. Data for each colour channel (B, G, R) is handled separately to ensure proper data embedding. For a given pair of pixels, the difference between pixel values is computed by the equation: diff = |p1 - p2|… (3.1), and the number of bits hidden is determined based on this difference.

The difference is deliberately manipulated to include hidden information. Pixel values are modified in a manner that p2 contains hidden information without significantly altering the values from the image boundary [0, 255]. Once all the data is embedded, the modified image, now containing the steganographic data, is saved with a different name (stego_PVD.png), maintaining the visual integrity and quality of the embedded data. To reveal the hidden message, the process begins by opening the stego picture (stegoimage.png) and converting it to RGB mode. A binary string is created in advance for storing the extracted data. The image is scanned by processing adjacent pixel pairs (p1, p2) from left to right, and for each colour channel (R, G, B), the pixel value difference is computed using formula (3.1). Based on this difference, the number of hidden bits is calculated by using the get capacity(diff) function. To read the hidden data, the AND operation is applied to the difference with a mask. The extraction continues until the end-of-message marker (00000000) is encountered, which signifies the end of the hidden data. The binary string composed of the extracted bits is converted into readable text.

It is broken into groups of 8 bits, each of which represents an ASCII character. Each group of 8 bits is then converted to a character using the expression chr (int (byte, 2)). Lastly, the extracted text is returned and printed, ending the data extraction process.

GBA format, such that the colour of every pixel can be accessed. The Pixel Value Differencing (PVD) technique shows remarkable efficiency in both image quality and process performance. The method achieves a high Peak Signal-to-Noise Ratio (PSNR) of 71.98-92.80 dB, indicating that the image quality remains unaffected after data embedding.

Moreover, the SSIM value of 1 also reveals that the visual distortion is nearly zero, and the Mean Squared Error (MSE) also confirms that the changes imposed on the images are negligible. In terms of performance, the embedding time and extraction time are minimal compared to other data hiding techniques, making PVD highly suitable for applications that require fast processing.

However, the approach does not offer a significant enhancement in data hiding capacity compared to techniques such as LSB or RGB, and it may limit its application when concealing large amounts of data. In general, while PVD experiences an acceptable quality-speed compromise, it might not be ideal when high capacity is the prime consideration.

Table-III: Evaluation Results of PVD Steganography

Data set	Capacity (bpp)	PSNR	SSIM	MSE (Mean Squared Error)	Embedding Time	Extraction Time
Image 1.png (2000,3000)	0.0002	92.8018	1	3.41111e-05	0.269534	0.0970109
Image 2.png (460, 736)	0.00354442	80.388	0.999999	0.000594675	0.0245733	0.00999951
Image 3.png (168, 299)	0.0238892	71.9879	0.999986	0.00411424	0.00735116	0.00399876
Image 4.png (578,870)	0.00238635	82.0277	1	0.000407668	0.0303035	0.0119996
Image 5.png (720, 1280)	0.00130208	84.8169	1	0.000214482	0.0441952	0.0159976
Image6.png (724,1280)	0.00129489	84.7111	1	0.000219772	0.0460331	0.017

IV. PROPOSED METHODOLOGY

A. Features-Based Optimized

Feature-based steganography is a technique of data concealment that utilises specific features of digital media, such as images, sound, or video, to conceal data, as opposed to modifying pixel or sample levels. It operates by exploiting features such as edges and corners in images, unique sound frequencies, or basic visual and kinetic features in video, where changes are less noticeable. It is widely used in covert communications, such as hiding private data in media files, embedding watermarks for intellectual property protection, and transmitting encrypted data for cybersecurity.

In this paper, we propose a method that integrates data compression and encryption into the feature-based optimisation process for embedding information. This approach demonstrates significant improvements in terms of PSNR, SSIM, and MSE, as well as reduced embedding and extraction times, compared to conventional methods. Furthermore, the proposed approach enhances security against attacks by employing a secret key for data recovery, thereby providing greater security even after the concealed data is detected.

i. Steps for Practical Application:

In this technique, initially, a compression algorithm is applied to compress the text. For an additional level of security, the compressed data is converted to Base64 format and encrypted with the Caesar Cypher. To identify suitable regions for embedding data into the image, the edges are detected using the Canny filter. The encrypted text is transformed into binary bits and embedded within the colour channels of the image. The modified image that contains the secret data is referred to as the Stego Image. During data extraction, the same edge detection algorithm is used on the Stego Image to retrieve the embedded binary data. The binary bits are retrieved

and transformed into encrypted text, which is decrypted and decompressed to get the original message. To verify the quality of the Stego Image, several parameters, including PSNR (Peak Signal-to-Noise Ratio), SSIM (Structural Similarity Index), and MSE (Mean Squared Error), are compared with the original image. Extraction time, embedding time, and capacity (bits per pixel, bpp) are also determined to analyse the method's performance.

The Feature-Based technique, combined with compression and encryption, demonstrated excellent performance in terms of image quality. The method achieved a high PSNR of between 85.59 and 108.92 dB, and an SSIM of 1, meaning that there was no noticeable visual distortion. The MSE was very low, indicating that the alterations made to the original image were minimal. In terms of performance, the extraction and embedding times were typical compared to techniques such as LSB and PVD, due to the compression and encryption added to the process. However, this approach offers high security and reduced storage due to the compression step taken, making it suitable for use when both data security and small storage are of top priority.

Table-IV: Evaluation Results of Feature-Based Optimized Steganography

Data set	Capacity (bpp)	PSNR	SSIM	MSE	Embedding Time	Extraction Time
Image 1.png (2000,3000)	0.0002	108.923	1	8.33333-07	6.0118	6.29218
Image 2.png (460, 736)	0.00354442	92.6353	1	3.54442e-05	0.346749	0.387552
Image 3.png (168, 299)	0.0238892	85.5982	1	0.000179169	0.0598764	0.0613611
Image 4.png (578,870)	0.00238635	95.1453	1	1.98863e-05	0.506239	0.555655
Image 5.png (720, 1280)	0.00130208	96.0153	1	1.6276e-05	0.907612	0.92139
Image6.png (724,1280)	0.00129489	96.339	1	1.5107e-05	0.93589	1.06316

B. Visionstego AI system

This is an algorithm applied in a steganography system, where a specific text is hidden in an image without producing noticeable changes. The system ensures that the text can be extracted later without losing any data. To enhance the imperceptibility of the changes, artificial intelligence is employed to identify the most suitable locations in the image where the data can be hidden, thereby making the concealed information even more difficult to locate.

i. Steps for Practical Application:

- Transcoding Text into Digital Data. Before inserting text into an image, the text is first transcribed into digital form. The text is encoded using the zlib library to compress it for optimised storage. Then, the compressed text is converted into a binary form, represented as a stream of zeros and ones (bits), since digital images operate in terms of binary data. For example, the text "Hello" is converted into its binary equivalent, where each letter is represented by 8 bits.
- Identifying Key Areas in the Image Using Artificial Intelligence. Not all regions of an image are suitable for hiding text, as certain areas may be more noticeable or prone to distortion. To address this, the saliency detection technique is utilized, an algorithm that identifies regions within the image that attract more visual attention. This is achieved using cv2.saliency. Static Saliency Spectral Residual_create () function. A mask is then generated, highlighting areas with significant visual features, such as edges and high-detail regions. This technique is critical because it ensures that the text is concealed in less conspicuous areas, reducing the likelihood of detecting changes in the image.
- Hiding Data Within the Image Once the text has been converted into bits and the key regions of the image identified, the data is embedded into the blue channel of the image using the least significant bit (LSB) technique.

By changing the least significant bit, the change is not visible to the naked eye. The process begins with saving the text length (32 bits) so that the extraction process can know when to stop. Then the bits are embedded individually in the image. For example, if a pixel's colour value is (120, 200, 155) and the hiding bit is '1', only the blue channel is changed to provide the pixel value (121, 200, 155). Due to the slight change, it becomes imperceptible.

To recover the hidden text, the saliency detection algorithm is used once more to identify the same significant regions used in the embedding process. The first 32 bits are read to define the length of the hidden text. The remaining bits are then recovered from the blue channel, and the binary data is converted back into text using zlib decompression. With the proper extraction, the original material is produced without loss as far as the conditions of the detection of saliency are retained. Such parameters are fundamental to the appropriate release of hidden information and should be safeguarded, as they comprise the master key to correct extraction.

ii. Features of the Algorithm:

- Smart hiding using artificial intelligence: the best hiding spots are identified to avoid detection.
- Effective storage size: The text is compressed to save more space.
- No impact on image quality: adjustments are made to the smallest possible portion of the pixels.
- Ease of extraction: The text can be retrieved with 100% accuracy

without data loss.

- High security: Because the concealment is done in places that are difficult to detect even with traditional analysis methods.

Table-V: Evaluation Results of VisionStego AI System Steganography

Data set	Capacity (bpp)	PSNR	SSIM	MSE	Embedding Time	Extraction Time
Image 1.png (2000,3000)	0.000152	94.1999	1	2.47222e-05	0.445559	0.442285
Image 2.png (460, 736)	0.00269376	81.5992	1	0.000449945	0.05001	0.0361168
Image 3.png (168, 299)	0.0181558	73.4576	1	0.00293306	0.0125248	0.0142202
Image 4.png (578,870)	0.00181363	83.4329	1	0.000294979	0.0548823	0.0459878
Image 5.png (720, 1280)	0.000989583	85.7897	1	0.000171441	0.101076	0.0809684
Image6.png (724,1280)	0.000984116	85.7863	1	0.000171573	0.1752	0.179139

iii. Analyses of Visionstego AI System Results:

The steganography quality assessment confirms that the proposed technique yields good Peak Signal-to-Noise Ratio (PSNR) values, ranging from 73.45 to 94.19 dB, indicating that the quality of the extracted images remains intact with only minor distortion. Additionally, the Structural Similarity Index (SSIM) is always 1, indicating that the generated images are practically indistinguishable from the original photos in terms of structural perception. The Mean Squared Error (MSE) values are minimal, indicating very slight alterations to the original image, thereby rendering the hiding process imperceptible visually. In terms of embedding capacity, measured in bits per pixel (bpp), the method has a medium to high capacity, meaning it can embed a substantial volume of data without significantly impacting image quality. In terms of performance efficiency, the extraction and embedding times vary with the image features but are highly acceptable. All the values indicate low processing times, demonstrating the system's high efficiency in data extraction and hiding. The VisionStego AI System provides balanced performance, featuring high-quality steganography, sufficient data storage capacity, and an overall acceptable processing rate. This renders it particularly well-positioned for use in applications that require high visual quality, acceptable embedding capacity, and the highest computational efficiency.

V. DISCUSSION AND RESULTS

A comprehensive evaluation was conducted to analyse the performance of various steganographic techniques, including Least Significant Bit (LSB), RGB, Pixel Value Differencing (PVD), Feature-Based optimised Steganography, and the proposed VisionStego AI System. The evaluation focused on key performance metrics, including image quality, storage, attack resistance, and processing efficiency.

A. Concealment Quality: The VisionStego AI System demonstrated superior performance in preserving image quality post-embedding. It achieved a high Peak Signal-to-Noise Ratio (PSNR) ranging from 73.45 to 94.19 dB, indicating minimal and imperceptible distortion. Additionally, the Structural Similarity Index (SSIM) consistently reached a value of 1, signifying that the stego image remained nearly identical to the original. The Feature-Based Steganography technique played a crucial role in optimising data distribution, thereby enhancing concealment effectiveness while maintaining visual fidelity.

B. Mean Squared Error (MSE) Analysis: The low Mean Squared Error (MSE) values obtained confirm that the embedding process introduced subtle and nearly undetectable changes to the image, reinforcing the effectiveness of the proposed approach in maintaining image integrity.

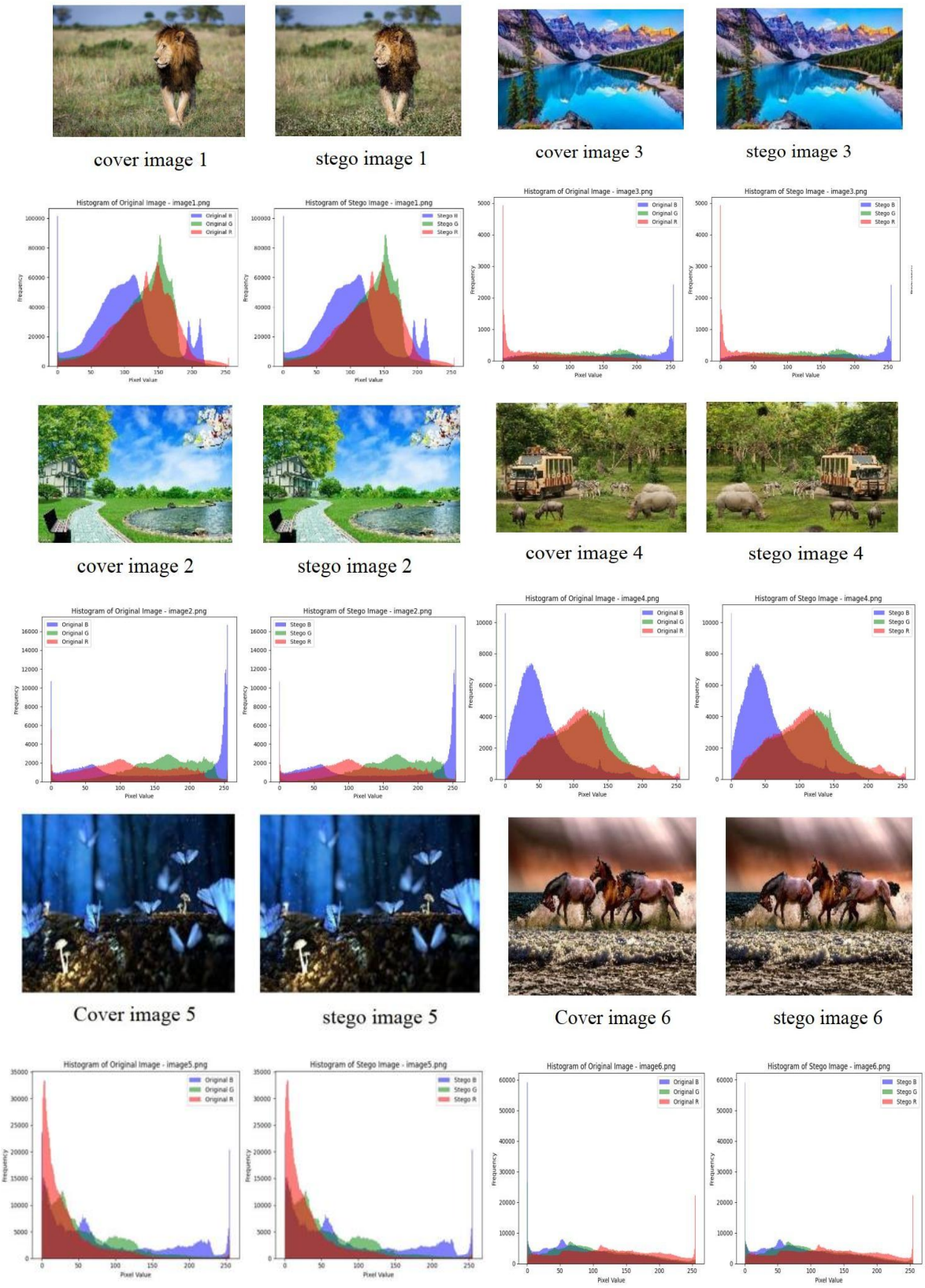
C. Storage Capacity (bpp): While the embedding capacity

D. varied across different techniques, the VisionStego AI System successfully balanced hiding capacity and image quality, ensuring that a significant amount of data could be embedded without perceptible degradation in image clarity.

E. Attack Resistance and Security: Compared to conventional LSB-based methods, VisionStego AI demonstrated greater resilience to steganalysis attacks, including histogram analysis and statistical detection techniques. The integration of encryption and compression mechanisms further strengthened its security, making the detection and extraction of hidden data significantly more challenging.

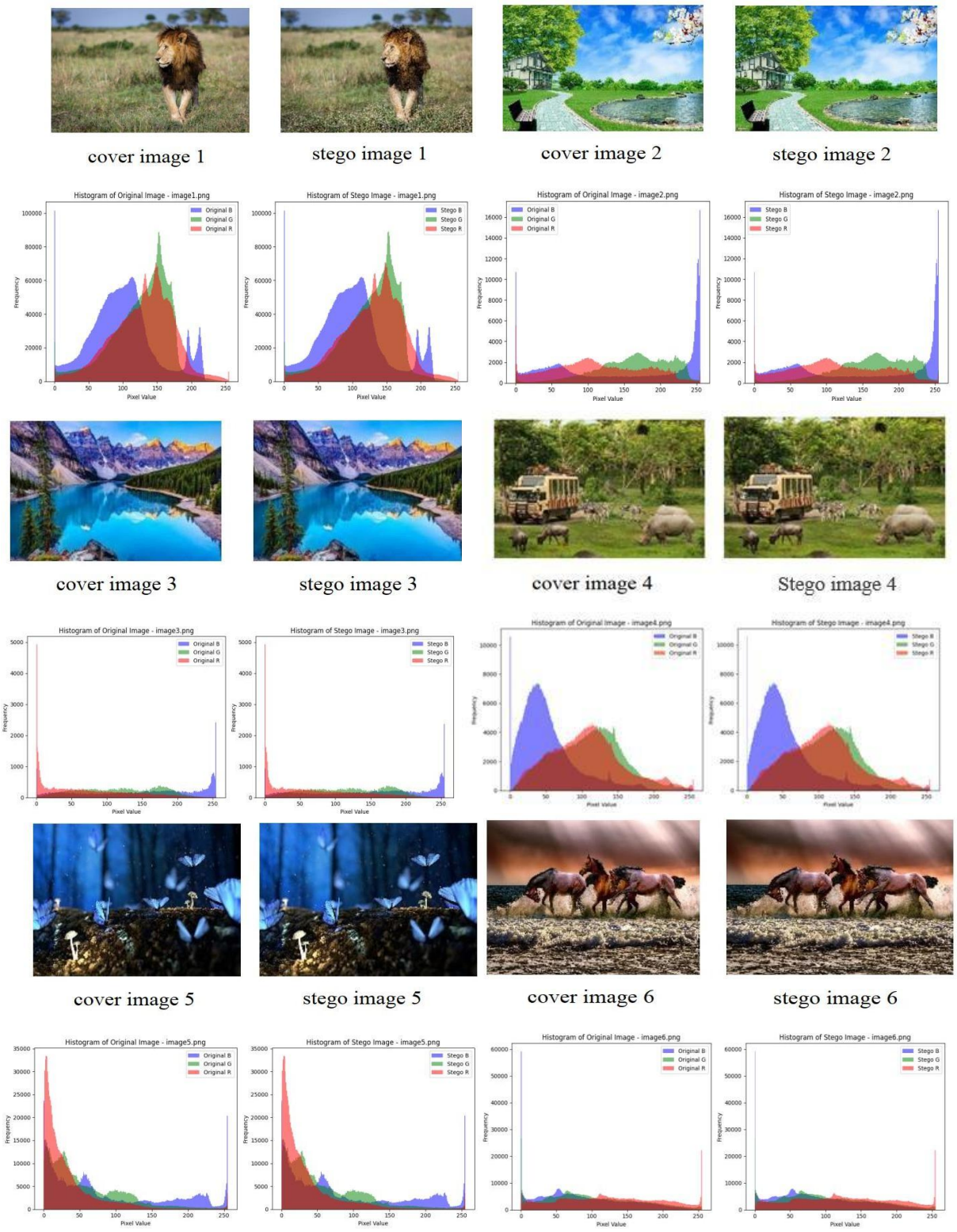
F. concealed data was well-distributed across the image, ensuring that no visible patterns or anomalies were introduced, which could otherwise be exploited for steganalysis detection.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)



[Fig.2: Comparison of RGB Cover and Stego Images Histogram of Feature-Based Optimized]

The feature-based optimised algorithm creates minor variants of the colour distortion but does not create significant distortions in the images. The histogram is varied, but with variations not sufficiently substantial to raise suspicion easily. The outcome of these results indicates that the method yields an optimal trade-off between capacity and imperceptibility.



[Fig.3: Comparison of RGB Cover and Stego images Histogram of VisionStego AI system]

Although there are distribution shifts, no pattern is visible that can be easily exploited for detection. The stego images are remarkably like the original cover images, indicating that the technique is effective in maintaining image quality. The changes are evenly distributed, which complicates the detection of hidden data using simple statistical analysis. The method strikes a good balance between preserving image quality and concealing data. VisionStego AI technology offers superior performance compared to traditional methods, striking a balance between concealment quality, storage capacity, analysis resistance, and processing speed. The primary security feature of the proposed system is the utilisation of artificial intelligence in identifying the optimal locations within images where data can be hidden; hence, it is more complex to detect with traditional analytical methods. Augmenting the Feature-Based Steganography technique with encryption and compression has led to improved resistance to attacks and improved image quality after hiding.

Table-VI: Comparison Between Steganography Techniques

Method Used	Advantage	Disadvantage
LSB	-Ease of implementation. -Difficulty in detecting the change in the image.	-Prone to detection when using image compression methods (such as JPEG). -Data may be lost if the image is modified.
RGB	-More complex hiding compared to LSB. -Reducing noticeable changes in the image.	- It can affect colour quality. -More prone to detecting manipulation compared to more advanced methods.
PVD	-Better resistance to manipulation detection compared to LSB. -Reduces visual clutter.	- Greater complexity in execution. - It may be detected if image enhancement processes are applied.
Feature-based optimized	-Improving the quality of concealment. -increase in steganalysis resistance. -Achieving balance between capacity and image quality. -High speed in hiding and extraction.	- The complexity of implementation and programming. -Need for higher computational resources. -The possibility of losing some data when pressing. - Need for an encryption key to retrieve the data.
VisionStego AI system	-Increase in steganalysis resistance. -Integration with encryption and compression technologies. -Efficiency in performance and speed. -The ability to adapt to different types of images.	-Sensitivity to substantial image edits. -Complexity in data sharing and retrieval. Higher development costs (developing and training AI models require additional expenses compared to traditional methods).

VI. CONCLUSION AND FUTURE WORK

This paper conducted a comparative study of an extensive nature, comparing the proposed technique with conventional Least Significant Bit (LSB)-based steganography techniques, in terms of several performance attributes, including embedding capacity, imperceptibility, security, and Peak Signal-to-Noise Ratio (PSNR). The experimental results concluded that the proposed technique significantly outperforms LSB-based techniques in terms of hiding capacity and secrecy, while achieving higher image fidelity and defence against steganalysis attacks. Among the most substantial advantages of the method described is that it allows for optimising the data embedding without compromising the structural integrity of the image, as evidenced by the high values of PSNR and SSIM scores. Coupled with the use of sophisticated embedding techniques and encryption, better resiliency to attacks has also been achieved, making it less likely for attackers to detect or extract hidden information using statistical or visual examination methods. This improvement is particularly significant for applications with high-security demands, such as digital watermarking, secret communication, and cybersecurity.

To further amplify the contribution of this study and increase the efficacy of the proposed steganographic technique, some paths for future research can be considered. Firstly, future upgrades could include optimising the embedding process by utilising other image characteristics, such as disparate colour channels beyond the blue channel, to enable more flexible data hiding techniques without compromising image quality and imperceptibility. Second, to obtain a more comprehensive comparison of the algorithm's efficiency, additional experiments should be conducted on various image formats, including coloured, grayscale, textural, and aerial images. Since different types of images have unique statistical characteristics, using a larger dataset for testing will help assess the generalizability and strength of the proposed methodology. Additionally, the detection resistance and extraction resistance of the algorithm can be further improved by incorporating more advanced encryption techniques and obfuscation technologies, such as adaptive encryption models, chaotic encryption methods, and deep learning-based hiding techniques, to render the hidden data even more challenging to identify. The proposed method can also be applied to real-world data hiding applications that are both secure and efficient, including digital rights protection, cybersecurity, medical image security, and forensic intelligence applications. The conclusions of this study indicate the promise of the proposed VisionStego AI System in realizing high-quality, secure, and imperceptible steganography. By combining optimised embedding techniques with encryption algorithms, the system offers a robust solution for applications that require high security and imperceptibility. Future research will focus on enhancing the method's adaptability, efficiency, and anti-detection capability, so that it can be used in most digital security, data protection, and confidential communication scenarios.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/Competing Interests:** Based on my understanding, this article does not have any conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted with objectivity and without any external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Kahn, D. (1996). The history of steganography. In *Lecture Notes in Computer Science* (pp. 1–5). DOI: https://doi.org/10.1007/3-540-61996-8_27
2. Darwis, D., Pamungkas, N. B., & Wamiliana, N. (2021). Comparison of the least significant bit, pixel value differencing, and modulus function on steganography to measure image quality, storage capacity, and robustness. *Journal of Physics Conference Series*, *1751*(1), 012039. DOI: https://doi.org/10.1088/1742-6596/1751/1/012039
3. Alhomoud, A. M. (2021). Image Steganography in the spatial Domain: status, techniques, and trends. *Intelligent Automation & Soft Computing*, *27*(1), 69–88. DOI: https://doi.org/10.32604/iasc.2021.014773
4. Rahman, S., Uddin, J., Khan, H. U., Hussain, H., Khan, A. A., & Zakarya, M. (2022). A novel steganography technique for digital images using the least significant bit substitution method. *IEEE Access*, *10*, 124053–124075. DOI: https://doi.org/10.1109/access.2022.3224745.
5. Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A (2021). Image Steganography: A Review of Recent Advances. *IEEE Access*, *9*, 23409–23423. DOI: https://doi.org/10.1109/access.2021.3053998
6. Alenizi, A., Mohammadi, M. S., Al-Hajji, A. A., & Ansari, A. S. (2024). A review of image steganography based on multiple hashing algorithms. *Computers, Materials & Continua/Computers, Materials & Continua (Print)*, *80*(2), 2463–2494. DOI:https://doi.org/10.32604/cmc.2024.051826
7. Zhao, P., Zhou, Y., Ijaz, S., Khan, F., Chen, J., Alshawi, B., Qin, Z., & Rahman, M. A. (2024). RLL-SWE: A Robust Linked List Steganography Without Embedding for intelligence networks in bright environments. Journal of Network and Computer Applications, 234, 104053. DOI: https://doi.org/10.1016/j.jnca.2024.104053
8. Su, W., Ni, J., & Sun, Y. (2024). StegaStyleGAN: Towards Generic and Practical Generative Image Steganography. *Proceedings of the AAAI Conference on Artificial Intelligence*, *38*(1), 240–248. DOI: https://doi.org/10.1609/aaai.v38i1.27776
9. Lu, S., Wang, R., Zhong, T., & Rosin, P. L. (2021). Large-Capacity Image Steganography Based on Invertible Neural Networks. *2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 10811–10820. DOI: https://doi.org/10.1109/cvpr46437.2021.01067
10. Sharma, R. P., Malik, A., Singh, S., Agarwal, S., & Kumar, R. (2023). High-Payload Lossless Steganography Using Image Interpolation. *Security and Communication Networks*, *2023*, 1–14. DOI: https://doi.org/10.1155/2023/2068813
11. Ashari, I. F., Nugroho, E. D., Andrianto, D. D., Yusuf, M. a. N. M., & Alkarkhi, M. (2024). Evaluation of LSB steganography on an image file using 3DES and MD5 keys. *JITCE (Journal of Information Technology and Computer Engineering)*, *8*(1), 8–18. https://www.researchgate.net/publication/383306535
12. Majeed, M. A., Sulaiman, R., Shukur, Z., & Hasan, M. K. (2021). A review of text steganography techniques. *Mathematics*, *9*(21), 2829. DOI: https://doi.org/10.3390/math9212829
13. BhanuRajeshNaidu, K., Manikanta, J., Vaseem, S., Adnan, S., & Kumar, C. N. (2024). Secure file-sharing system utilising image steganography and cryptography techniques. In *CRC Press eBooks* (pp. 120–124). DOI: https://doi.org/10.1201/9781003559092-21
14. U. Ghanekar, "A Brief Review on Image Steganography Techniques." [Online]. Available: DOI: https://ssrn.com/abstract=3579269

AUTHOR'S PROFILE

Hessah Alshamrani, I hold a Bachelor's degree in Information Systems from King Khalid University and am currently pursuing a Master's degree in Cybersecurity at Taif University, Saudi Arabia. My professional experience includes working effectively in diverse and high-pressure environments. I am skilled in analysis, problem-solving, and collaborating with multidisciplinary teams. Passionate about the field of information security and the protection of data and systems, I continually seek to explore and learn about the latest innovations in this ever-evolving field. Committed to continuous learning, I stay updated on the latest trends and developments in cybersecurity and learn advanced and sophisticated methods to protect data and systems.

Dr. Samah H. Alajmani received the B.Sc. degree in Computer Science from King Abdulaziz University, Jeddah, Saudi Arabia. She earned the M.Sc. degree in Information Technology from the Queensland University of Technology, Brisbane, Australia. She is currently an Assistant Professor at Taif University, Taif, Saudi Arabia. Her Research interests include Cybersecurity, AI, Machine learning, Deep Learning, and IoT.

Dr. Raneem Yousif Alyami is an Assistant Professor of Information Technology at Taif University, specialising in human-computer interaction, artificial intelligence, and cybersecurity. She earned her Ph.D. in Human Computer Interaction from the University of Reading, United Kingdom, with a focus on designing interactive and assistive technologies. Her research interests include deep learning, IoT, and AI-driven security solutions, with an emphasis on bridging the gap between technology and human needs. Dr. Alyami is actively working on publishing research in high-impact journals and developing AI-based solutions for accessibility and cybersecurity. She has led interdisciplinary research projects that integrate machine learning models into real-world applications to enhance usability and system security. With expertise in both theoretical and applied computing, she plays a key role in advancing digital innovation, fostering industry collaborations, and mentoring the next generation of IT professionals.

Dr. Ben Soh, Associate Professor, obtained his PhD in Computer Science and Engineering (in Secure and Fault-Tolerant Computing under the tutelage of Prof. TS Dillon) from La Trobe. Since then, he has successfully supervised 14 PhD students and published more than 200 peer-reviewed research papers. He has made significant contributions in the following research areas: Fault-Tolerant and Secure Computing, Cloud Computing, Information Systems Research, Pervasive Wireless Network Communications, Educational Technology and Business Process Management. Currently, he serves as La Trobe's cybersecurity programs advisor and coordinator.