Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

Saliency-Aware Steganography with a Hybrid AES and RSA with LSB Embedding

Abdullah S. AL-Malaise Alghamdi[1*] and Rana Alrawashdeh[2]

1 *Computer Science Department, School of Engineering, Computing and Design, Dar Al-Hekma University, Jeddah 34801, Saudi Arabia*
2 *Faculty of Computer Studies, Arab Open University, Amman 11953, Jordan*

ARTICLE INFO

Article History

Received: 17-01-2026
Revised: 28-05-2026
Accepted: 11-06-2026
Published: 19-06-2026

Vol.2026, No.2

DOI:

**Corresponding author.*
Email:
aghamdi@dah.edu.sa

ABSTRACT

Image steganography hides secret data within digital media, such as images, without detection. Traditional stenographic methods struggle with three major problems including limited data capacity, susceptibility to attacks, and compromised visual quality. In this work, we propose a new framework, based on the BossBase dataset, that combines hybrid encryption with saliency-based adaptive embedding to select the most effective regions for data concealment in cover images. We encrypt the secret image in the first step using a hybrid encryption approach, Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) algorithm, where AES is first used to encrypt the secret image and the AES key is then RSA-encrypted for dual layer encryption. Bitwise triplication technique and majority voting are incorporated to protect the encrypted key from bit errors. Then, we generate a hybrid histogram equalization (HE) map from the cover image's saliency map to embed the secret image. During the embedding process, we use the Least Significant Bit (LSB) technique, which selects areas in the hybrid map derived from the cover image with low visual sensitivity for embedding data. The system evaluation includes multiple performance metrics, including Peak-to-Signal Ratio (PSNR), Structural Similarity Index Measure (SSIM), Mean Squared Error (MSE), Bit Error Rate (BER), payload capacity, and execution time. The experimental results show excellent imperceptibility for all secret image sizes (64×64, 128×128, 192×192) with PSNR values above 58 dB and SSIM values above 0. 9995.The system succeeded in reconstructing completely imperceptible content with BER = 0. The reconstructed contents had infinite PSNR and SSIM = 1.0000 against any image Perturbations(including noise, blurring, compression, and cropping) . All the conventional steganalysis and the deep-learning–based steganalysis (RS, CRM, Xu-Net, Ye-Net) failed to detect the embedded signals.

Keywords: Image Steganography, RSA, Advanced Encryption Standard (AES), Saliency Map.

How to cite the article

1. Introduction

As we have entered the digital era, secure communication has become more important because public networks are handling more multimedia content at higher speeds. Encryption methods protect message content from disclosure, but they fail to hide the fact that a message exists [1]. The inability to hide the presence of data has sparked growing interest in image steganography, which enables the secure embedding of secret information into innocuous cover images [2]. The widespread adoption of image steganography stems from the redundancy and high pixel capacity of digital images. Current stenographic methods face the challenge of finding the right balance between security, imperceptibility, high payload capacity, and resistance to attacks. Most stenographic methods fail to account for the human visual system (HVS)'s perceptual characteristics, leading to noticeable stego-image distortions and increased vulnerability to steganalysis [3].

In this work, we propose a solution that addresses these constraints through a secure, adaptive image steganography framework that combines hybrid cryptographic encryption with saliency-guided LSB embedding. The secret image is protected using a hybrid encryption method that employs AES for content security and RSA for secure key distribution. In order to improve robustness against random bit errors, the AES key is repeated three times and the steganalysis signatures are majority voted. This means that one of three instances of the same key could have an error of up to one bit still allowing the correct key to be voted most often. We have conducted a saliency map analysis of the cover image to select the least visible areas of the image to use as the carriers for the least significant bits (LSB) that are replaced in the steganographic experiments reported in this work. The objectives of this research are to investigate methods and techniques to detect steganographic content, to measure the hiding capacity of images, and to analyze the tradeoffs between imperceptibility and capacity [7]. This work has the following objectives:

- **Objective-1**: To unite hybrid encryption methods with spatial domain adaptive saliency-based embedding techniques.
- **Objective-2**: To combine AES encryption for content protection with RSA encryption for secure key exchange through its stenographic design.
- **Objective-3**: To improve system robustness against bit-level errors by applying a triplicate encoding strategy and triplicate encoding with majority voting for key recovery.
- **Objective-4**: To generate a saliency map from the cover image to select embedding locations in perceptually neutral areas, which reduces visible distortion.
- **Objective-5**: To use adaptive LSB embedding in low saliency areas to securely hide the encrypted payload while maintaining imperceptibility.
- **Objective-6**: To evaluate the system through quantitative metrics, including PSNR, SSIM, MSE, BER, BPP, and execution time for embedding and extraction.

Figure 1 illustrates the typical steganography process structure which will be modified later in the proposed mechanism in Figure 2. The enhanced mechanism includes hybrid encryption, saliency-obtained stego image and histogram equalization for achieving better imperceptibility and security. This study aims to address the following research questions:

- **RQ1-1:** How can a secure stenographic system be designed using hybrid encryption (AES + RSA) to ensure high confidentiality?
- **RQ1-2:** Can the use of a saliency map improve stego image quality by guiding embedding to perceptually less sensitive regions?
- **RQ1-3:** To what extent does adaptive LSB embedding help in balancing hiding capacity and imperceptibility?
- **RQ1-4:** How does the proposed system perform in terms of image quality, payload capacity, and error rate compared to traditional approaches?

In this paper, we present an efficient image steganography system that incorporates hybrid encryption technique with saliency-based and HE-based adaptive spatial domain reversible data-hiding technique. The adaptive steganography technique achieves the dual goals of secure communication and disturbance obfuscation with imperceptible quality. The enciphers encrypt the secret image, and secure key exchange is achieved by different encryption and secure key exchange techniques, namely, Advanced Encryption Standard (AES) and RSA. The deciphers can recover the encryption key from bit error contaminated stego-key using technique of bitwise triplication followed by majority voting technique. Adaptability of data-hiding capacity in the adaptively designed system is achieved by utilizing saliency map of the cover image for selecting appropriate low-visual distortion areas for reversible data-hiding. Optimal capacity is also achieved by embedding

LSBs (Least Significant Bits) in low-saliency regions of the cover image to achieve high-quality stego-image with imperceptible visual distortion. The approach not only maintains high quality of original cover image but also embeds hidden data with desired level of security and very low distortion errors.

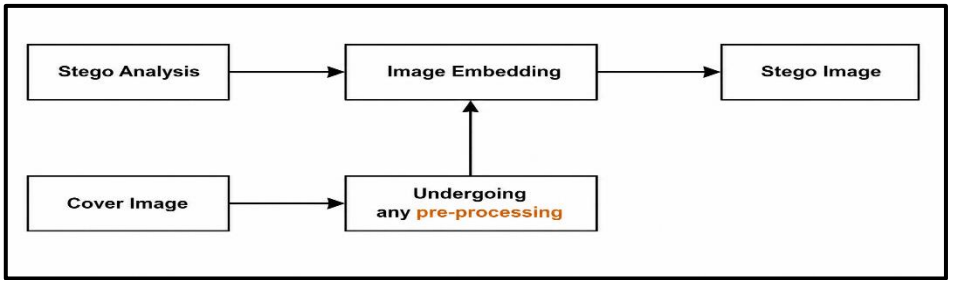


Figure 1. Basic Steganography Pipeline.

The paper has been organized as follows. Section 2 covers the work related to this work. Section 3 covers the proposed methodology. Section 4 discusses the experiment results, and Section 5 presents the conclusion.

2. Literature Review

Image steganography in spatial domain has attracted significant attention in recent years from numerous researchers, due to its capability to embed hidden information into image in a visually imperceptible way. Most of existing steganographic techniques attempted to improve steganographic security in terms of imperceptibility, embedding capacity and resistance to steganalysis detection. In addition to steganographic quality, researchers have also explored techniques that combine steganography with encryption and developed adaptive spatial steganography methods that select high quality cover objects. In this paper, we provide a comprehensive overview of state-of-the-art steganographic approaches, followed by a discussion on their limitations and shortcomings.

Moumen and Sissaoui [8] proposed a secure transmission method for secret images in medical image area. In this paper, secret images are encrypted by secret image encryption methods using AES (Advanced Encryption Standard) for symmetric encryption, RSA (Rivest, Shamir and Adleman) algorithm for asymmetric encryption, and LSB (Least Significant Bit) steganography. Firstly, secret images are encrypted with AES methods to increase transmission efficiency. Secondly, the encrypted AES key is encrypted with RSA algorithm. The encrypted AES key is embedded into the encrypted image by LSB method. Thus, no direct key exchange is needed between the sender and the receiver. Simulation results reveal that the proposed scheme is secure and can resist common steganalysis techniques. Some real medical grayscale images are used to test the proposed method. The decrypted images from the proposed system have achieved PSNR higher than 50 dB, on average. The correlation and entropy analysis results show a sharp decrease in pixel correlation and a corresponding increase in true randomness in stego images and decrypted images.

A balance between security and imperceptibility is maintained through a novel approach which allows secure transmission of images via conventional insecure channels. Abdel Wahab et al. in [9] presented a hybrid approach to enhance the security, efficiency and capacity of steganographic methods. In this work, a message is first encrypted using RSA cryptographic technique. The encrypted message is then subjected to Huffman coding technique for achieving efficient compression. The coded message is then invisibly embedded into an image cover using spatial domain steganography technique based on Least Significant Bit (LSB) technique after applying Discrete Wavelet Transform (DWT) on the cover image. The cover image is also compressed to increase the efficiency of storage and transmission. A few experiments have been conducted to evaluate the performance of proposed methods through several quality metrics such as PSNR, SSIM, MSE, BPP, CR and Compression Time. Experimental results demonstrate that the system processes images with high image quality (PSNR > 40dB) and small error probability and is robust to compression and tampering. Compared with existing algorithms and methods, the approach provides better visual quality and higher coding efficiency. The results demonstrate good data reduction capability and provide secure encryption and covert transmission capability simultaneously. The approach is suitable for secure multimedia transmission applications that require low bandwidth.

Barnwal et al. in [10] proposed concept of secret pixel as steganography technique which embeds data by covering it securely with strong encryption. Secret Pixel encompasses dual layer encryption. AES-256 symmetric key encryption is

used for session key and encryption of actual message is done by RSA-4096. Randomized embedding is achieved by seeded pseudo random number generator and data is scattered in non-sequential pixels of image. This technique provides better imperceptibility and secure hiding of data as compared to classical LSB technique which can be easily tracked by statistical methods. Moreover, embedding process is made further imperceptible and efficient by compressing the payload using techniques like zlib compression (DEFLATE: LZ77 + Huffman coding). Simulation results show excellent visual quality with high visual fidelity up to 48 dB PSNR and 0.98 SSIM. It can embed up to 50 KB secret data into 1080p image and has low computational overhead. Suitable for real-time secure data communication applications.

Security and privacy in cloud environment have become a very important issue to secure the data which is stored in the cloud as well as being transmitted over the network. There is an increasing trend in cloud computing to apply hybrid of classical and emerging cryptographic techniques along with steganography to secure data from unwanted eyes. In this research, Badhan and Malhi [11] discuss and review different techniques and mechanisms that can be employed to provide end-to-end security especially data confidentiality and integrity in cloud-based scenario by using hybrid approach of classical and emerging cryptography along with steganography. Classical methods such as AES, RSA and DES along with emerging methods such as ECC are discussed in the paper. Comparison of different security mechanisms is discussed which includes their individual implementations as well as hybrid implementations along with known steganography techniques including image and video-based steganography. The results of comparison indicate vast improvement in security when hybrid approach of cryptographic techniques and steganography is employed over traditional security techniques. Literature review is also presented that includes hybrid technique of AES-RSA along with spatial domain technique of LSB substitution method and ECC-AES along with transform domain technique of DWT. Also, mechanisms for incorporation of error correction and data compression are discussed to enhance security and throughput.

Shmueli et al. [13] recently proposed spatial-domain image steganography technique that embeds data in natural locations within an image. In their technique, the Maximum Energy Seam (MES) with the highest cumulative energy on each iteration is selected for embedding. The cumulative energy is approximated by a gradient operator. A saliency map is computed to highlight high-energy regions (namely, texture regions). Dynamic thresholding is applied to the resulting stego-image to ensure natural degradation. Message bits are embedded along the MES path by flipping the least significant bit of RGB values, repeatedly embedding along all seams (with no overlap between adjacent seams). Experimental results showed that the achieved PSNR and SSIM are very high (up to 70 dB and 1.0) for different images and different data sizes. The PSNR and SSIM are even better than those of LSB replacement and random insertion methods. The high capacity embedding and very good visual quality preservation are obtained in this work. The data are embedded into content-sensitive positions; however, no additional positions need to be sent to the decoder.

3. Research Methodology

To achieve adaptive steganography, our proposed technique illustrated in Figure 2 adopts hybrid encryption followed by hybrid saliency-based LSB substitution in the spatial domain. The embedding approach includes histogram equalization followed by Gaussian-based residual salience map, and insensitivity-based secret data embedding. The decryption approach includes hybrid encryption scheme of both advanced encryption standard (AES) and AES in CBC mode, and secure decryption of tripled encrypted triple des (3E3DES) ciphertexts. The approach includes tripled encryption of 3DES and RSA (1024-bit) hybrid encryption for securing the transmitted tripled decryption keys, and a tripled decryption method. Majority voting is used to extract the encrypted keys. Tripled key bits are then embedded into cover image pixels by substituting the LSBs of low-saliency intensity regions. These tripled and triple-encrypted keys are merged to form a triple-layered payload. Results illustrated excellent stego-image imperceptibility and high-quality secret image extraction.

3.1 Dataset

BossBase 1.01 is a standard benchmark dataset for image steganography and steganalysis research. The dataset contains 10,000 fully uncompressed grayscale images, each being 512×512 pixels in size. The images used in BossBase were taken by digital cameras at high quality and then resized and converted to grayscale to create uniform samples. The standardized high-quality images are suitable for generating cover-stego (cover object-stego object) pairs to test various embedding algorithms, as well as for training deep-learning-based steganalysis networks [15][16].

3.2 Image preparation and preprocessing

In the preprocessing phase, we first import the cover image. The image is preprocessed by first converting it to grayscale, then normalizing the image and embedding at a resolution of 256×256 pixels. Histogram Equalization (HE) is then performed on the image. This enhances the visual contrast so that more structure in the image can be seen. Then, a Gaussian-based residual approach is then applied to generate a saliency map. The image is then processed through these defined regions of interest. The enhanced cover image reveals more distinct structural and intensity details which are perceptible to human vision. The resulting saliency map distinguishes between visually meaningful and meaningless regions more clearly enabling the low-saliency regions for effective data embedding. Embedding data in such regions results in minimal perceptible distortion and embedding artifacts leading to improved stego image imperceptibility. In our proposed framework, the secret image is encrypted using the well-known AES (Advanced Encryption Standard) cipher, employing a randomly generated symmetric key. Then the AES key is encrypted with a publicly known RSA algorithm to secure the transmission of the encryption key. The resulting encrypted AES key, and the encrypted secret image, are then embedded into the cover image.

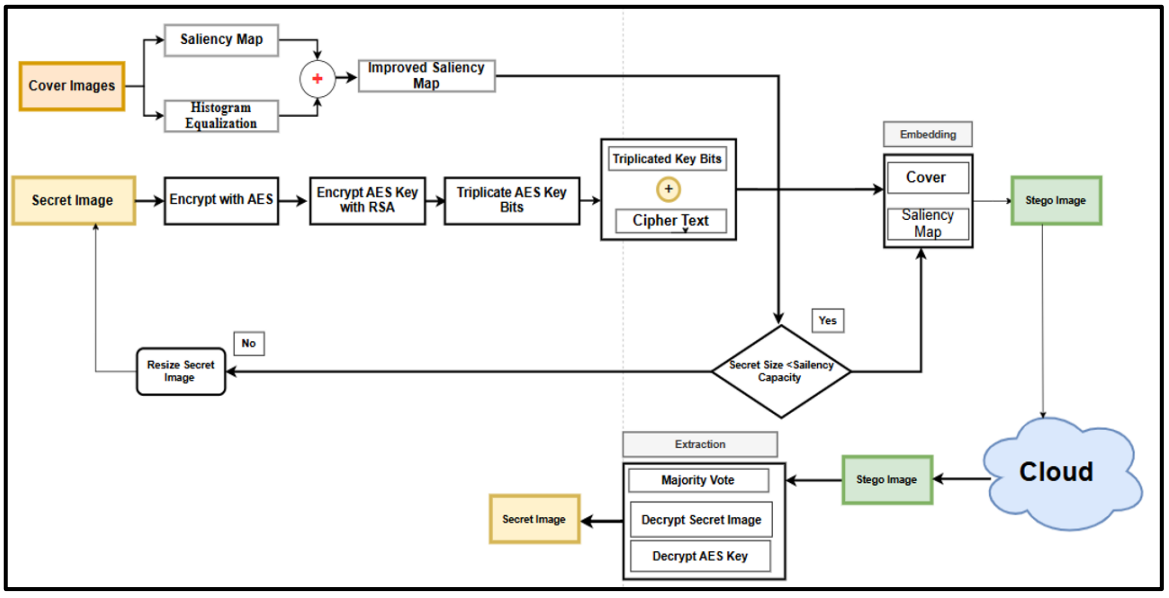


Figure 2. Proposed Approach

Algorithm 1. AES Encryption in CBC Mode

Require: plaintext (split into 128-bit blocks), key, IV
Ensure: ciphertext

```
round_keys ← KeyExpansion(key)
previous_block ← IV
for each plaintext_block in plaintext do
    xor_block ← plaintext_block ⊕ previous_block
    encrypted_block ← AES_Block_Encrypt (xor_block, round_keys)
    Append encrypted_block to ciphertext
    previous_block ← encrypted_block
end for
return ciphertext
```

Algorithm 2. AES Block Encryption

Require: 128-bit block, round_keys
Ensure: encrypted_block

```
state ← block
AddRoundKey (state, round_keys [0])
for r = 1 to Nr − 1 do
    SubBytes(state)
```

```
        ShiftRows(state)
        MixColumns(state)
        AddRoundKey(state, round_keys[r])
    end for
    SubBytes(state)
    ShiftRows(state)
    AddRoundKey (state, round_keys [Nr])
    return state
```

The provided pseudocode (Algorithm 1 and Algorithm 2) demonstrates how AES encryption functions when using CBC mode. The process starts by dividing the plaintext into 128-bit blocks, which are then XORed with either the previous ciphertext block or an initialization vector for the first block before AES encryption. The AES block encryption process includes the standard operations of SubBytes, ShiftRows, MixColumns, and AddRoundKey, which are repeated throughout multiple rounds. The pseudocode provides an abstract representation of encryption operations, which helps developers reproduce secure data-hiding system operations [17]. The RSA cryptographic process in Algorithms (3, 4, and 5) is described in pseudocode, including key generation, encryption, and decryption steps. The key generation process requires two large prime numbers to calculate encryption and decryption keys. The public key can be used to encrypt data by anyone, but the private key serves as the decryption key for the intended recipient only. The encryption process begins by converting the original message to an integer before applying the public key. The private key decrypts the message back to its original form. The structured pseudocode makes RSA easier to understand while demonstrating its function for secure asymmetric encryption.

Algorithm 3 RSA Key Generation

Require: Security parameter k (e.g., 1024 bits)
Ensure: Public key (e, n) and Private key (d, n)

```
    Choose two large distinct primes p and q
    Compute n ← p × q
    Compute φ(n) ← (p − 1)(q − 1)
    Choose integer e such that 1 < e < φ(n) and gcd(e, φ(n)) = 1
    Compute d such that d ≡ e^−1 mod φ(n)
    return Public key (e, n) and Private key (d, n)
```

Algorithm 4 RSA Encryption

Require: Message M, Public key (e, n)
Ensure: Ciphertext C

```
    Convert message M to integer m such that 0 ≤ m < n
    Compute c ← m^e mod n
    return c
```

Algorithm 5 RSA Decryption

Require: Ciphertext c, Private key (d, n)
Ensure: Original message M

```
    Compute m ← c^d mod n
    Convert integer m back to message M
    return M
```

3.3 Embedding process

The embedding procedure begins with the concatenation of a unified binary payload consisting of the encrypted secret image (denoted by 'ciphertext') followed by a triplicated form of the AES key used for steganography. In the second step, the generated payload is distributed throughout the least significant bits (LSBs) of the cover image. The positions where bits are replaced are not random and are determined by a saliency map derived from a saliency-based image preprocessing. This saliency map highlights the visually less relevant regions of an image according to the properties of the human visual

system. We exploit visually weak areas in images to covertly embed large amounts of data, thus maximizing tolerance to loss and ensuring that any resulting changes are perceptually indistinguishable. Once an image has been embedded with, the resulting image is known as the stego image. The stego image looks to the human eye (viewer) like the original cover image. Therefore, it can be sent via normal channels. The stego image carries the encrypted secret data and the encryption key within the pixel intensity values of the image [18].

D. Extraction and decryption

Similarly, in the extraction stage, the same saliency map that was generated in the embedding phase (see Figure 3) is employed to accurately determine the exact locations where the embedded data is dispersed in the stego image. In the extraction phase, the focus is placed on the low-saliency regions, specifically on the least significant bits (LSBs) of the image. The payload consists of an encrypted payload (ciphertext) followed by multiple copies of an encrypted AES key. Majority voting is performed on the repeated segments to possibly correct for bit errors before decryption of the key. After embedding, the encrypted AES key is decrypted back with the corresponding RSA private key. The original AES key recovered is then used to decrypt the encrypted payload (secret image) using the same AES in CBC mode for decryption.In the presented approach, both RSA and AES are used. Because of the dual level encryption (decrypted key with RSA and encrypted data with AES), the scheme provides robust protection to the data against bit level alterations. Protected data becomes transmissible over open networks or can be imperceptibly embedded in other multimedia objects.

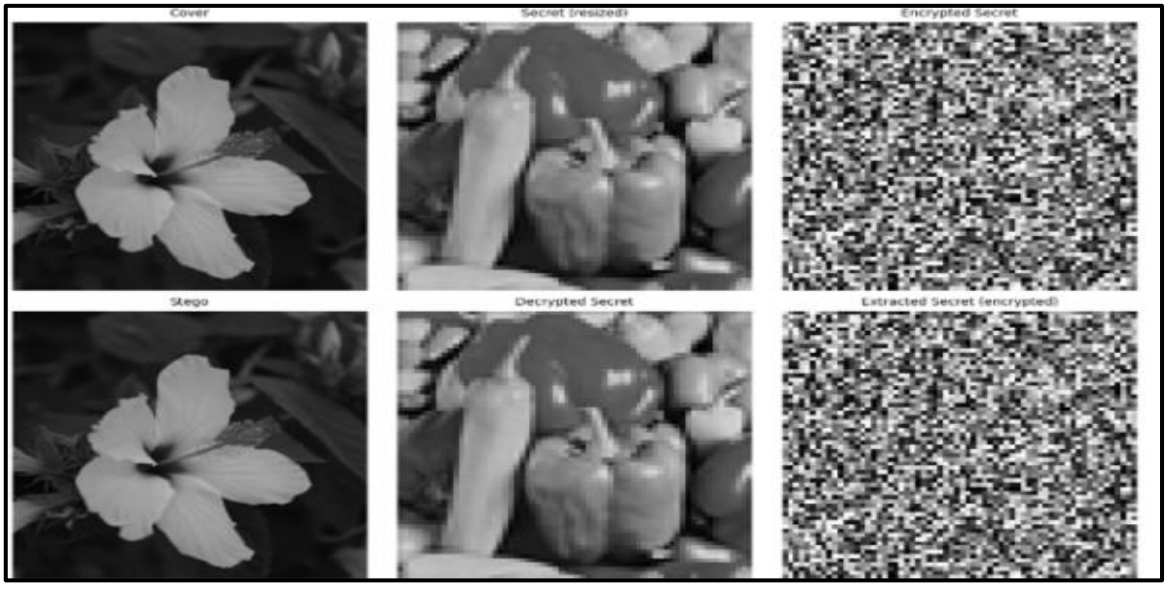


Figure 3. Embedding and Extraction Process

4. Analysis and Findings

The proposed strategy demonstrates its performance through three measures: imperceptibility, capacity, and security or robustness. Imperceptibility is evaluated using MSE, RMSE, PSNR, SSIM, and IF. The capacity of the proposed strategy is measured by Payload Capacity (PC) and Bits Per Pixel (BPP). Security performance is evaluated using RS analysis, Xu-Net, and Ye-Net, Convolutional Residual Model (CRM), and Histogram analysis as steganalysis methods. Robustness is measured using Histogram Distortion (Re) and Bit Error Rate (BER). The following subsection describes the performance metrics in detail.

4.1 Imperceptibility

Mean Squared Error (MSE): represents the average squared difference between the pixels of the cover image and the stego image. Lower MSE values indicate better imperceptibility and are closer to zero. MSE is defined as [10]:

$$\text{MSE} = (1/\text{mn}) \times \Sigma_{\text{i}}^{=1\text{m}} \Sigma_{\text{j}}^{=1\text{n}} \left(\text{I(i, j)} - \text{K(i, j)} \right)^2 \quad (1)$$

Where
MSE: Mean Squared Error
m, n : Image dimensions
I(i, j) : Pixel value of the original image
K (i, j): Pixel value of the stego image
Root Mean Squared Error (RMSE): is obtained by taking the square root of MSE and is expressed as [12]:

$$RMSE = \sqrt{MSE} \quad (2)$$

Peak Signal-to-Noise Ratio (PSNR): evaluates the quality of the stego image according to the Human Visual System (HVS). PSNR values greater than 30 dB indicate imperceptible embedding. PSNR is calculated as [14]:

$$PSNR = 10 \times log^{10}(MAX^2/MSE) \quad (3) \text{ where:}$$

PSNR : Peak Signal-to-Noise Ratio
MAX : Maximum possible pixel value
MSE: Mean Squared Error

Structural Similarity Index Measure (SSIM): evaluates structural similarity between the cover and stego images. SSIM values range from 0 to 1, with values close to 1 indicating high similarity. SSIM is defined as:

$$SSIM(I, K) = ((2\mu I\mu K + C1)(2\sigma IK + C2)) / ((\mu I^2 + \mu K^2 + C1)(\sigma I^2 + \sigma K^2 + C2)) \quad (4)$$

Where:
I, K: Two different images
μI , μK : Mean intensity of images I and K
σI, σK: Standard deviation of images I and K
σIK: Covariance between images I and K
C1, C2: Stabilization constants
Image Fidelity (IF): measures the similarity between two images at the pixel level [7]. IF values closer to 1 indicate higher similarity and are computed as:

$$IF(I, K) = (1 / N) \times \Sigma_{\text{i=1}}^{\text{N}} (1 - |Ii - Ki| / max(Ii, Ki)) \quad (5)$$

Where:
IF(I, K) : Information Fidelity
N : Total number of pixels
Ii , Ki : Pixel values at position i

B. CAPACITY
Payload Capacity (PC): measures the amount of data that can be hidden within the cover image by the proposed steganographic method. The payload capacity depends primarily on the size of the cover image [11]. Equation (6) defines the payload capacity:

$$Payload\ Capacity = T \times N \times 8 \quad (6)$$

where:
T: Total number of pixels in the cover image
N: Bytes per pixel (1 for grayscale images, 3 for color images)
Bits Per Pixel (BPP): represents the average number of embedded bits per pixel across the entire image [2]. BPP is calculated using Equation (7):
BPP = Payload Capacity (bits) / N (7)
where:
BPP: Bits Per Pixel
Payload Capacity (bits): Total payload capacity in bits
N: Total number of pixels in the image
Bit Error Rate (BER): measures the proportion of incorrectly extracted bits relative to the total number of embedded bits [13]. BER is a key metric for evaluating data extraction accuracy and system reliability in stenographic systems:
where:

$$BER = Ne / Nt \quad (8)$$

Where:
Ne: Number of erroneous bits
Nt: Total number of embedded bits
Histogram Distortion (Re): quantifies the statistical difference between the histograms of the cover and stego images. It indicates the degree of detectable changes caused by data embedding and is used to assess the imperceptibility of the stenographic system:

$$Re = 1 - (Hs / Hc) \quad (9)$$

Where:
Hs : Histogram of the stego image
Hc: Histogram of the cover image

Table 1 simulates embedding a 64×64 secret image into a 256×256 grayscale cover image. As can be seen from the table, the steganographic system developed in this paper performs outstandingly in all the measurements. The PSNR (Peak Signal to Noise Ratio) measurement between the cover image and stego image are as high as 58.75 dB. It is therefore clear that the stego images have good visual quality and are hard to be perceived. The SSIM (Structure Similarity) measurement is 0.9995 and the MSE (Mean Squared Error) is 0.09. The Image Fidelity (IF) measurement is also high with value 0.9133. The PSNR, SSIM and MSE of the original secret image and the decrypted image are infinite, 1.0000 and 0 respectively. The error bits (BER) is 0.000000, thus there is no embedding error or extraction error in the system. The histogram distortion (Re) is 0.0000. The system has a huge payload capacity of 11520 bits. The capacity normalized by image size, i.e. bit rate (BPP), is 0.1758. The system has a fast-processing time for data embedding and extraction. The average time for data embedding is 1.61 seconds, while the average time for decrypted image extraction is 0.11 seconds.

Table 1. Steganography Evaluation Metrics Using 64×64

Metric	**Value**
PSNR (Cover vs Stego)	58.75 dB
SSIM (Cover vs Stego)	0.9995
MSE (Cover vs Stego)	0.09
Image Fidelity (IF)	0.9133
PSNR (Secret vs Decrypted)	∞ dB
SSIM (Secret vs Decrypted)	1.0000
MSE (Secret vs Decrypted)	0.00
Bit Error Rate (BER)	0.000000
Histogram Distortion (Re)	0.0000
Bits Per Pixel (BPP)	0.1758
Payload Capacity	11520 bits
Embedding Time	1.6149 sec
Extraction Time	0.1127 sec

The evaluation results for the proposed stenographic system that embeds a 128×128 secret image into a grayscale cover image are presented in Table 2. The results show excellent imperceptibility, perfect reconstruction, and high computational efficiency. The PSNR between the cover and stego images is 58.71 dB, well above the acceptable threshold (typically 40 dB), indicating that the embedded modifications are visually imperceptible. This is corroborated by an SSIM of 0.9995, indicating near-identical structural quality between the cover and stego images. The MSE is extremely low (0.09), further confirming minimal pixel-level distortion. Similarly, the IF is reported as 0.9125, indicating high pixel-level agreement. Regarding data recovery, the system achieves perfect reconstruction of the secret image, as demonstrated by infinite PSNR, SSIM = 1.0000, and MSE = 0.00 between the original and decrypted secret images. The Bit Error Rate (BER) is 0.000000, confirming error-free extraction of the embedded payload. The histogram distortion (Re) value is negligible (0.0000), indicating no significant change in statistical entropy between the cover and stego images, suggesting high security and undetectability. In terms of capacity, the system supports embedding 11,520 bits at a bit rate of 0.1758 bits per pixel (BPP). The embedding process is completed in just 0.7897 seconds, while extraction takes 0.0446 seconds, highlighting the algorithm's computational efficiency.

Table 2. Comprehensive Steganography Evaluation Metrics 128×128

Metric	Value
PSNR (Cover vs Stego)	58.71 dB
SSIM (Cover vs Stego)	0.9995
MSE (Cover vs Stego)	0.09
Image Fidelity (IF)	0.9125
PSNR (Secret vs Decrypted)	∞ dB
SSIM (Secret vs Decrypted)	1.0000
MSE (Secret vs Decrypted)	0.00
Bit Error Rate (BER)	0.000000
Histogram Distortion (Re)	0.0000
Bits Per Pixel (BPP)	0.1758
Payload Capacity	11520 bits
Embedding Time	0.7897 sec
Extraction Time	0.0446 sec

Table 3 demonstrates the efficiency and stability of the proposed steganographic scheme when embedding a 192×192 secret image into a given cover image. The table clearly indicates high imperceptibility, perfect retrieval, and fast processing. An extremely high PSNR of 58.65 dB implies negligible distortion between the original cover image and resulting stego image. The SSIM value of 0.9995 and average MSE of 0.09 indicate excellent structure similarity between original and stego images. The Image Fidelity (IF) of 0.9113 indicates good visual similarity between the original cover image and stego image. The secret image recovery process achieves perfect recovery. The PSNR is infinite and SSIM = 1.0000 and MSE = 0.00. The BER is zero, which means no error occurred during the secret image extraction process. So, the Re value is zero, which means there is no statistical difference between the cover image histogram and the corresponding stego image histogram. The maximum embedding capacity is 11,520 bits. Thus, the average bits per pixel (BPP) is 0.1758. The average running time for the embedding process is 0.2782 seconds, and the average running time for the secret image extraction process is 0.0404 second.

Table 3. Comprehensive Steganography Evaluation Metrics Using 192×192

Metric	Value
PSNR (Cover vs Stego)	58.65 dB
SSIM (Cover vs Stego)	0.9995
MSE (Cover vs Stego)	0.09
Image Fidelity (IF)	0.9113
PSNR (Secret vs Decrypted)	∞ dB
SSIM (Secret vs Decrypted)	1.0000
MSE (Secret vs Decrypted)	0.00
Bit Error Rate (BER)	0.000000
Histogram Distortion (Re)	0.0000
Bits Per Pixel (BPP)	0.1758
Payload Capacity	11520 bits
Embedding Time	0.2782 sec
Extraction Time	0.0404 sec

4.2 Security analysis

A security evaluation of the proposed stenographic method required implementing both traditional and deep-learning-based steganalysis techniques. The evaluation of learned models for detecting hidden content in cover–stego image pairs was performed using Xu-Net, Ye-Net, RS, and CRM. These models detect spatial anomalies arising from data embedding through their design, and their performance is evaluated using classification accuracy, ROC curves, and false-positive and false-negative rates. The Confusion Residual Mapping (CRM) technique was used to visualize and highlight the spatial regions in the stego image where the model's prediction confidence is altered. CRM provides neural steganalysis with interpretability by visualizing the embedding's impact on image regions, helping explain the model's detection logic. The

deep learning approach was combined with RS analysis (regular–singular analysis) as a statistical steganalysis method. The technique determines the embedding rate by analyzing fluctuations in pixel pairs between regular and singular groups before and after flipping the function. RS analysis continues to work effectively against LSB-based methods while providing lightweight yet reliable detection In steganalysis evaluation, detection accuracy values close to 50% indicate behavior like random guessing, which suggests that the steganalysis is unable to reliably distinguish between cover and stego images (good results).

4.2.1 Ye-Net Analysis

The system shows accuracy = 0.4875, and the ROC curve from the steganalysis model evaluation is shown in Figure 4. The ROC curve shows the relationship between the true positive rate (sensitivity) and the false positive rate to evaluate how well the classifier separates stego images from cover images at different threshold settings. The Area Under the Curve (AUC) is 0.35 in this case, which falls below the random-guessing threshold of 0.5. The model demonstrates poor performance with good impact, with an AUC of 0.35, indicating it frequently confuses stego images with cover images and vice versa. The specific model fails to detect the embedded payload, demonstrating the security and imperceptibility of the proposed stenographic approach under the evaluated conditions. The confusion matrix of the Ye-Net is demonstrated in Figure 5. It can be observed that all the 39 cover images (class 0) were correctly classified as cover images. On the other hand, all the 41 stego images (class 1) were misclassified as class 0. Hence, the Ye-Net exhibits a perfect specificity of 100%, but zero sensitivity, i.e., it correctly classified no true positive samples and generated many false negative samples. This said, the detection ability of the proposed approach is weak since the used steganographic system provides very difficult spatial distortions to images. The confusion matrix in Fig. 5 shows very poor generalization capability, thus the developed feature embedding technique is resistant to standard classification-based steganalysis methods such as hidden content detection. Lower detection accuracy in steganalysis means better security for the stenographic system. As detection accuracy is getting closer to the random-guessing performance, the embedded modifications do not introduce sufficient discriminative features that can be effectively learned and used by a steganalysis model, thus the stenographic system becomes more secure.

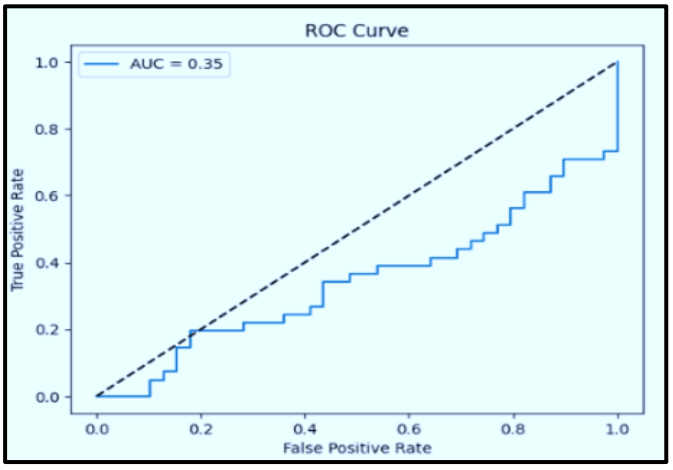


Figure 4. Ye-Net ROC

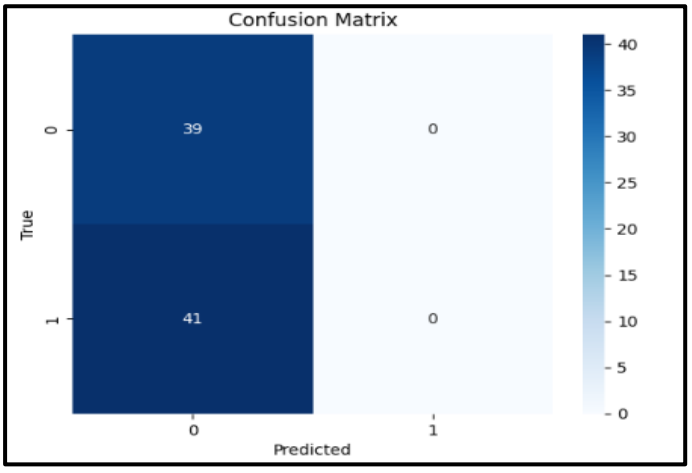


Figure 5. Ye-Net Confusion Matrix

4.2.2 Xu-Net Analysis

The accuracy of Xu-Net was 0.4250. Figure 6 is the ROC curve of the steganalysis model. It illustrates true positive rate (sensitivity) against the false positive rate for different thresholds. The area under the curve (AUC) was 0.53. The AUC value is greater than the random-guess value of 0.50. However, the detection performance is very weak and merely marginal over chance. This detection performance may indicate that the method (Xu-Net) is resistant to detection by even statistical learning-based steganalysis. In Figure 7, as shown in the confusion matrix, 34 of the 50 cover images were correctly classified as covers (true negatives) and the remaining 16 images were misclassified as stego images. On the other hand, all the 46 stego images were classified as covers, therefore there were 0 true positives. This results in 100% specificity and 0% sensitivity (recall). This result clearly shows that there is an extreme bias toward the negative class and it is possible that the employed steganographic method is very weak and does not disturb images sufficiently or the detection method employed here is very weak and underfitted.

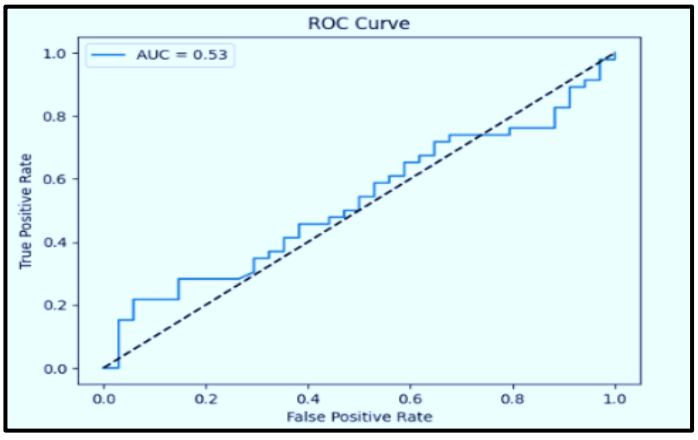


Figure 6. Xu-Net ROC

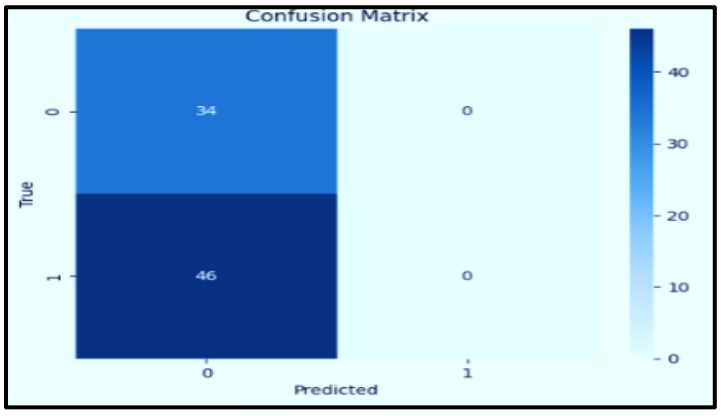


Figure 7. Xu-Net Confusion Matrix

4.2.3 CRM Analysis

The accuracy of the developed CRM for the testing image subset was 0.4250. The corresponding ROC curve in Figure 8 shows that as the threshold is increased, the true positive rate (sensitivity) improves. However, the false positive rate increases also. The calculated AUC value of 0.42 is less than that of the random classification line (0.50) and indicates that the steganalysis model fails to classify between cover and stego images, producing many incorrect classifications. This could be because the images in the training set lacked discriminatory features or because the employed image distortion technique is highly imperceptible. The ROC analysis demonstrates the quality of the stenographic method used, which embeds visually imperceptible content. The results of the classifier-based steganalysis (Fig. 9) show that such content cannot be distinguished from cover content, or misclassified as stego content (class 0), i.e. always classified as class 1. In the test, there were zero true negatives and 46 false negatives (all cover images classified as stego images), and 34 true positives. The best achieved result for stego image detection has a 100% recall rate and 0% specificity. This high false-positive rate is due to a strong bias of the model to the positive class. It is possible that this high bias is caused by overfitting, strong class imbalance in the training set or the lack of discriminative features in the cover's images.

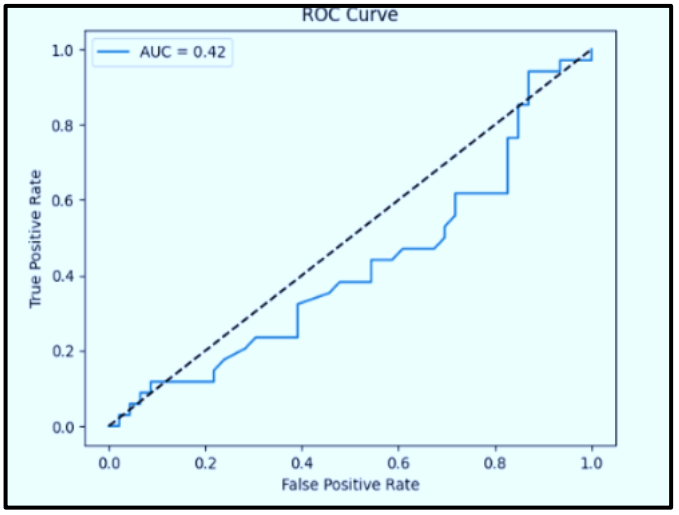


Figure 8. CRM ROC

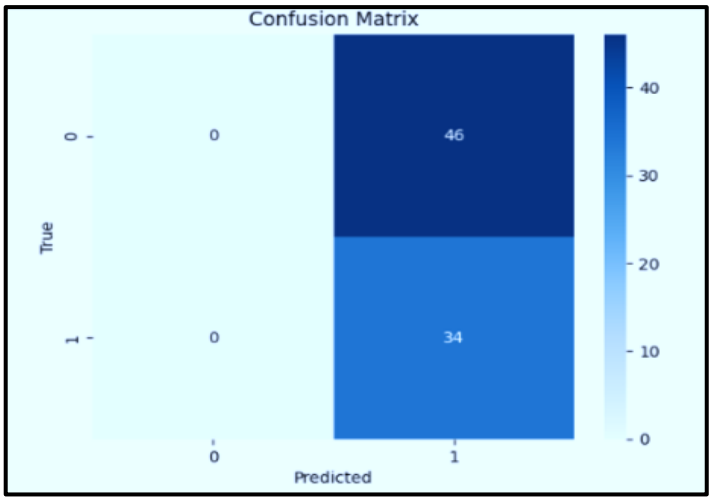


Figure 9. CRM Confusion Matrix

4.2.4 RS Analysis

The RS analysis determined the statistical detectability of the proposed stenographic method. The results show that in Figure 10, the cover and stego images have the same payload estimation of 1.0000 and a security value of 0.0000. The payload estimate of 1.0 indicates that the image has the maximum embedding capacity under the flipping function test. However, since both images cover and stego produce the same result, it indicates that the embedding process does not introduce any distinguishable statistical patterns detectable by RS analysis. The security score of 0.0000 indicates that there is no statistical difference between regular and singular groups before and after flipping, meaning that the RS detector is unable to distinguish between stego and non-stego images. This outcome highlights the strong resistance of the proposed method against RS steganalysis, as it preserves the statistical structure of the cover image even after embedding. Consequently, the method demonstrates a high degree of imperceptibility and statistical undetectability under RS-based detection frameworks. The RS analysis results, shown in Figure 11, reveal consistent patterns across the two image sets (cover and stego). The proposed method demonstrates strong resistance to RS-based statistical steganalysis because the equal payload and zero security scores remain consistent despite the different counts of regular (R), singular (S), and unusable (U) groups, such as (R=2587, S=8388, U=5409) versus (R=11142, S=32364, U=22030).

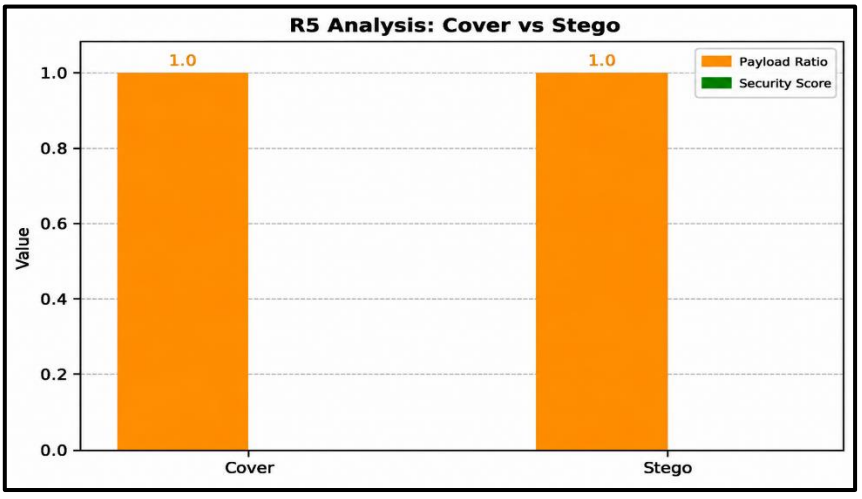


Figure 10. RS Analysis for Cover and Stego image.

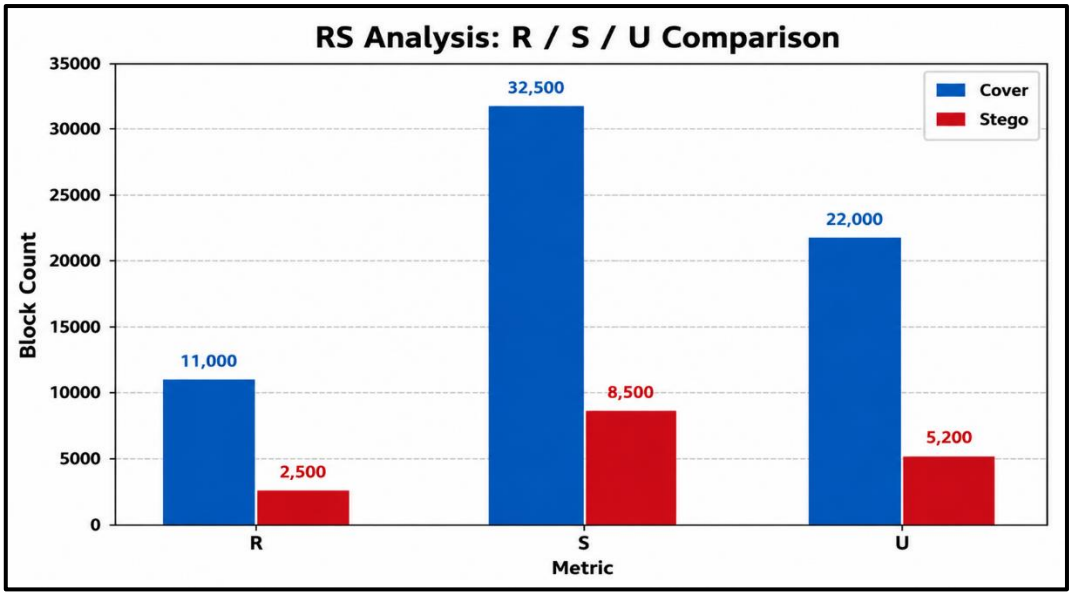


Figure 11. R-S-U Analysis for Cover image and its Stego image

4.3 Robustness analysis

Figure 12 demonstrates visual distortions on the stego-image caused by five common image attacks such as Gaussian noise, salt and pepper noise, JPEG compression, Gaussian blur and cropping. Most common image attacks cause quality degradation of image by adding noise. In the spatial domain, Gaussian noise attack and salt and pepper noise attack are the most common image noise attacks, which spread noise to images by modifying pixel values. Table 4 shows the experimental results, which indicate that our proposed steganographic method is resistant to five typical image attacks. In our experiments, the system was able to recover all the hidden contents for any of the attack scenarios we performed. The results are infinite for PSNR and SSIM values of 1.0000. The results indicate that the embedding and extraction processes are highly distortion resilient, for both imperceptibility to normal usage and robustness to adversary or degraded environments. The results also demonstrate high resilience to real-world applications where stego images are required to be compressed, noisy or have part of the stego image lost during usage.

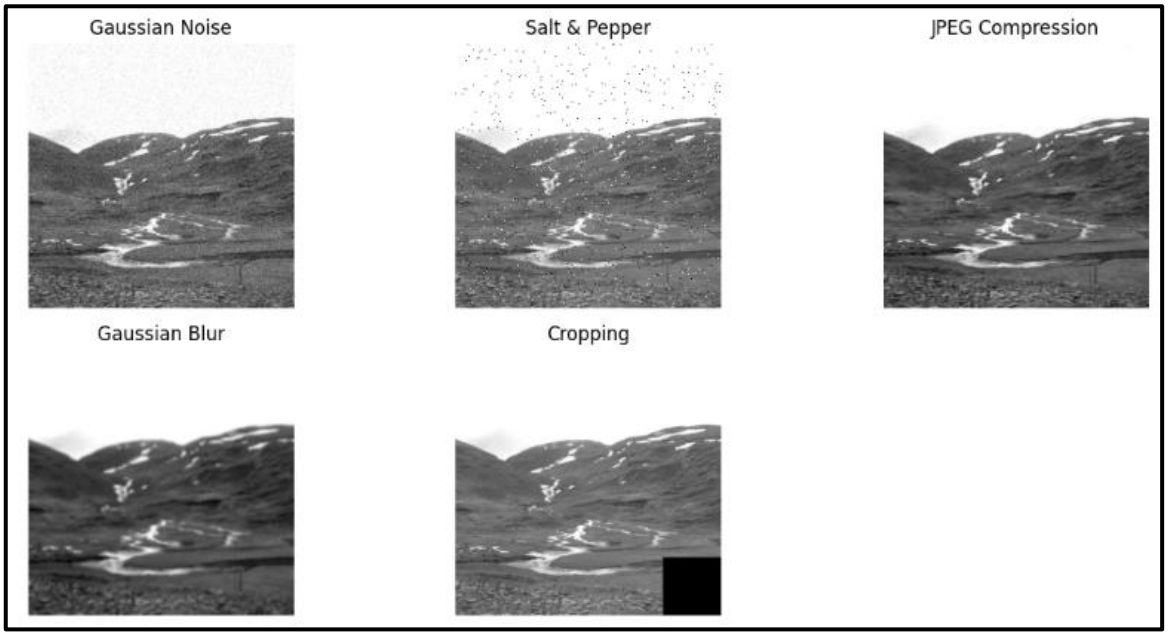


Figure 12. The visual effects of five common image attacks

Table 4. Robustness Evaluation Results under Different Attacks.

Attack Type	PSNR (dB)	SSIM
Gaussian Noise	∞ (Perfect reconstruction (MSE = 0)	1.0000
Salt & Pepper	∞ (Perfect reconstruction (MSE = 0)	1.0000
JPEG Compression	∞ (Perfect reconstruction (MSE = 0)	1.0000
Gaussian Blur	∞ (Perfect reconstruction (MSE = 0)	1.0000
Cropping	∞ (Perfect reconstruction (MSE = 0)	1.0000

The evaluation results in Table 5 demonstrate how the proposed method performs against multiple existing stenographic techniques using the BOSSBase dataset to assess stenographic security, payload capacity, robustness, and imperceptibility. The current methods focus either on achieving high embedding rates or on protecting against specific steganalysis techniques, yet they compromise either image quality or security against various types of attacks. The previous methods [20], [19], and [21] produced acceptable imperceptibility results, as indicated by their PSNR values, which ranged from 35 dB to more than 52 dB, while maintaining embedding capacities of 0.01-0.5 bpnz/AC. The methods show immunity to traditional feature-based steganalysis methods, including DCTR and GFR, but their resistance has been tested only with JPEG compression at specific quality levels (Q75–Q90), without testing against contemporary deep learning-based steganalysis systems. The approach from [22] enables users to embed up to 0.5 bpnz/AC of information while performing SRNet-based security assessments, yet it lacks specific results for imperceptibility metrics, which hinders the evaluation of visual effects during embedding. The security-oriented approach described in [23] reduces the detection performance of multiple steganalysis models (SRM, Deng-Net, SRNet, and Ye-Net) but fails to provide quantitative metrics for both imperceptibility and robustness, thereby preventing a full assessment. The system described in [10] provides the maximum payload capacity, reaching 1,572,864 bits at a BPP of 8, while achieving excellent imperceptibility (SSIM = 0.99, IF = 0.99). The system shows average security capabilities against deep-learning steganalyzers, as detection accuracy scores range from 0.45 to 0.67 for Xu-Net and Ye-Net. The proposed work provides a better equilibrium between all assessment criteria. The system operates with perfect stealth, achieving a PSNR of 58.7 dB, an SSIM of 1.0, and an MSE of 0, indicating no visible image degradation. The method achieves an embedding capacity of 0.17 BPP, which is lower than that of high-capacity methods, yet it offers sufficient security for payload transmission while preserving visual quality. The proposed method provides effective protection against both traditional and deep learning-based steganalysis detection systems, including Xu-Net and Ye-Net, as well as CRM and RS analysis, because it maintains detection accuracy at random-guess levels. The system demonstrates its ability to withstand typical image attacks through robustness experiments, demonstrating its effectiveness for a real-world secure stenographic implementation. The comparison shows that the proposed method addresses the weaknesses of the previous method by optimizing all three performance criteria simultaneously rather than focusing on a single metric.

Table 5. Comparison between our work and related works based on BOSSBase Dataset.

Paper	Dataset	Imperceptibility	Capacity	Security	Robustness
[20]	BOSSBase	PSNR ≥ 35	0.05–0.5 bpnz/AC	DCTR-secure GFR-secure	Error rate from JPEG compression Q75, Q90
[19]	BOSSBase	PSNR ≥ 50	0.01–0.1 bpnz/AC	DCTR-secure GFR-secure	Error rate from JPEG compression Q75, Q90

[21]	BOSSBase	PSNR ≥ 52	0.05–0.3 bpnz/AC	DCTR-secure GFR-secure	Error rate from JPEG compression Q75, Q90
[22]	BOSSBase	NA	0.1–0.5 bpnz/AC	DCTR-secure SRNet-secure	Error rate from JPEG compression Q70
[23]	BOSSBase	NA	NA	Lowest detection accuracy in SRM, Deng-Net, SRNet, YU-Net Improved security up to 5.39%	NA
[10]	BOSSBase	MSE = 0.0000 PSNR = up to 39.83 dB SSIM = 0.99 IF = 0.99	Max = 1,572,864 bits BPP = 8	Xu-Net: 0.45–0.67 secure YU-Net: 0.43–0.67 secure	Robust
Proposed Work	BOSSBase	MSE = 0.0000 PSNR = 58.7 SSIM = 1.0 IF = 0.99	Max = 11520 bits BPP= 0.17	Xu-Net: Secure Ye-Net: Secure CRM=Secure RS=secure	Robustness

5. Conclusion

The research develops an image steganography framework that protects information through hybrid encryption and saliency-guided embedding methods to maintain both confidentiality and imperceptibility. The system protects the secret image through AES encryption in CBC mode and RSA encryption of the AES key followed by a bitwise triplication and majority voting scheme to improve resistance against bit-level errors. The system uses histogram-equalized cover images to create saliency maps, which identify areas for embedding through adaptive LSB substitution. The experiments using three different secret image dimensions (64×64, 128×128, 192×192) show excellent imperceptibility results with PSNR values above 58 dB and SSIM values reaching 0.9995. The secret image reconstruction achieved perfect recovery (BER = 0) while keeping the computational cost low. The proposed method successfully resisted detection by traditional (RS) and learning-based (XU-Net, YU-Net, CRM) steganalysis techniques, which failed to detect the embedded content. The proposed system achieves an optimal balance between payload capacity and security and visual quality to provide a strong solution for secure covert communication.

Corresponding author
Abdullah S. AL-Malaise Alghamdi
aghamdi@dah.edu.sa

Acknowledgements
The authors appreciate Dar Alhikma for supporting this paper.

Funding
NA.

Contributions
Authors work together on researching, investigating and writing up the article.

Ethics declarations

The authors have not used any human subjects for research.

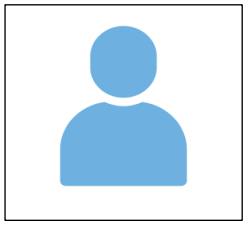
Consent for publication
Authors have their consent for publication.

Competing interests
The authors have not any competing interest.

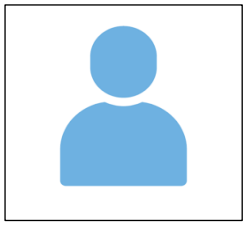
References

[1] Ji, P., Zhang, Y., & Lv, Z. (2025). Edge-guided dual-stream U-Net for secure image steganography. *Applied Sciences, 15*(8), 4413.
[2] Wang, M. (2025). AttnEdge: An enhanced edge detection method based on self-attention mechanism. In *Proceedings of the Fourth International Conference on Computer Vision, Application, and Algorithm (CVAA)* (Vol. 13486, pp. 438–446). SPIE.
[3] Sanjalawe, Y., Al-E'mari, S., Fraihat, S., Abualhaj, M., & Alzubi, E. (2025). A deep learning-driven multi-layered steganographic approach for enhanced data security. *Scientific Reports, 15*(1), 4761.
[4] Verma, A. K., Sarkar, T., et al. (2024). Utilizing imaging steganographic improvement using LSB & image decoder. In *Proceedings of IC3SE* (pp. 144–150). IEEE.
[5] Panigrahi, R., & Padhy, N. (2025). An effective steganographic technique for hiding the image data using the LSB technique. *Cyber Security and Applications, 3*, 100069.
[6] Yusuf, H. S., & Hagras, H. (2020). High payload image steganography method using fuzzy logic and edge detection. *International Journal of Computer Science Trends and Technology, 8*(4), 123–134.
[7] Duan, X., Liu, N., Gou, M., Wang, W., & Qin, C. (2020). SteganoCNN: Image steganography with generalization ability based on convolutional neural network. *Entropy, 22*(10), 1140.
[8] Moumen, A., & Sissaoui, H. (2017). Images encryption method using steganographic LSB method, AES and RSA algorithm. *Nonlinear Engineering, 6*(1).
[9] Domathoti, M., Ayyalasomayajula, S. K., Karri, V. K., & M, L. (2025). Hiding data using efficient combination of ECC and compression steganography techniques. *International Journal of Scientific Research in Engineering and Management, 9*(3), 1–9.
[10] Barnwal, A., Sah, A., R, S., Khera, N. U., Srivastav, R., & Sivasankar, A. (2024). SecretPixel: Advanced steganography with seeded random embedding and AES-RSA encryption. In *Proceedings of IEEE INSPECT* (pp. 1–6). IEEE.
[11] Badhan, A., & Malhi, S. S. (2024). A review on hybrid cryptography approach with steganography. In *Proceedings of IEEE IEMECON* (pp. 1–7). IEEE.
[12] Zhao, J., Wang, S., & Sun, F. (2025). Saliency map construction for adversarial image steganography. *Chinese Journal of Electronics, 34*(3), 816–827.
[13] Shmueli, R., Mishra, D., Shmueli, T., & Hadar, O. (2024). A novel technique for image steganography based on maximum energy seam. *Multimedia Tools and Applications, 83*(28), 70907–70920.
[14] Kumar, A., Singla, P., & Yadav, A. (2024). StegaVision: Enhancing steganography with attention mechanism. *arXiv preprint arXiv:2411.05838*.
[15] Bayar, B., & Stamm, M. C. (2016). A deep learning approach to universal image manipulation detection using a new convolutional layer. In *Proceedings of the ACM Workshop on Information Hiding and Multimedia Security* (pp. 5–10).
[16] Ray, B., Mukhopadhyay, S., Hossain, S., Ghosal, S. K., & Sarkar, R. (2021). Image steganography using deep learning based edge detection. *Multimedia Tools and Applications, 80*(24), 33475–33503.
[17] Setiadi, D. R. I. M., Rustad, S., Andono, P. N., & Shidik, G. F. (2024). Graded fuzzy edge detection for imperceptibility optimization of image steganography. *The Imaging Science Journal, 72*(6), 693–705.
[18] Wang, M. (2025). AttnEdge: An enhanced edge detection method based on self-attention mechanism. In *Proceedings of CVAA* (pp. 438–446). SPIE.
[19] Bai, J., Chang, C.-C., Nguyen, T.-S., Zhu, C., & Liu, Y. (2017). A high payload steganographic algorithm based on edge detection. *Displays, 46*, 42–51.
[20] Sukumar, A., Subramaniyaswamy, V., Ravi, L., Vijayakumar, V., & Indragandhi, V. (2021). Robust image steganography approach based on RIWT-Laplacian pyramid and histogram shifting using deep learning. *Multimedia Systems, 27*(4), 651–666.
[21] Wang, Y., Tang, M., & Wang, Z. (2020). High-capacity adaptive steganography based on LSB and Hamming code. *Optik, 213*, 164685.
[22] Alattar, A. (2004). Reversible watermark using the difference expansion of a generalized integer transform. *IEEE Transactions on Image Processing, 13*(8), 1147–1156.
[23] Setiadi, D. R. I. M., et al. (2023). Digital image steganography survey and investigation. *Signal Processing, 206*, 108908.

Biographies



Abdullah Saad Al-Malaise Al-Ghamdi is a professor of software \& systems Engineering and AI, associated with Faculty of Computing and Information Technology (FCIT) at King Abdulaziz University (KAU), and Dar Al-Hekma University, Jeddah, Saudi Arabia. Currently, he is working as a ``Collaborated Faculty Professor'' at Jeddah International College, University of Business and Technology. He received his PhD. degree in computer science from George Washington University, USA, in 2003. He has worked as a member of the Scientific Council and as a Secretary General of the Scientific Council at KAU. In addition, he has been involved as an external examiner for several academic programs, and faculty members' promotion around the world. He has published many papers in high-impact journals, books, and patents. His main research areas are software engineering and systems, artificial intelligence, data analytics, business intelligence, and decision support systems.



Rana Al-Rawashdeh received the bachelor's degree in computer science from Albalqa applied University, Jordan, in 2009, and the master's degree in computer science from the Jordan University of Science and Technology, Jordan, in 2019 and PhD from KFUPM university in 2025. Her research interests are in machine learning, deep learning, Cybersecurity, and data mining.