RESEARCH PAPER

Secure Data Embeding and Transmission Through Image Steganography

Vivek Gupta[*1], Muskan Sihare[2], Nisha Verma[3], Ashish Singh[4], Sanjay Patsariya[5] and Saba Khan[6]

[1,2]Department of Computer Science & Engineering, Rustamji Institute of Technology, Gwalior M.P.
[3]PhD Scholar, Department of Computer Science & Engineering, Amity University, Gwalior M.P.
[4]Department of Computer Science & Engineering, SR Group of Institutions, Jhansi U.P.
[5,6]Department of Information Technology, Rustamji Institute of Technology, Gwalior M.P.
***Corresponding Author:** Vivek Gupta*

Received: 28th Feb, 2026; Revised: 6th March 2026; Accepted: 7th April, 2026; Available Online: 20th April, 2026

ABSTRACT
The increased dependence on the use of the public networks to conduct communication, share data, and accessing services online, has made data security a burning issue in this digital era. Conventional cryptography, although useful in affording confidentiality, can earmark the use of secret communication, and thus encrypted streams of information can be intercepted and analyzed. In order to address this weakness, this paper investigated image steganography in place of the lone guard approach to security. By hiding sensitive information into digital images, the research tried to make information look as though it did not exist and therefore camouflaged itself as well. Two most influential methods, Least Significant Bit (LSB) substitution, and Discrete Cosine Transform (DCT) based embedding, have been implemented and tested. The two types of analysis that have been used in the experiment are the qualitative types, visual comparison, statistical distribution analysis, and difference images, and quantitative measurements, Peak Signal-to-Noise ratio (PSNR), and structural similarity index (SSIM). The results have shown that both methods provided imperceptibility, PSNR reached 40 dB and SSIM was near 0.99, which has ensured stego images could not be notably differentiated with the cover images. Although LSB had a better embedding capacity coupled with its simplicity, DCT was found to be more robust to compression and noise; therefore, it was better in the real-world transmission over public networks. The results substantiate that image steganography is more advantageous to the security of data since, it extends the traditional level of confidentiality with the level of invisibility, providing a two-level security lover. That makes steganography a good prospect in secure communication in sensitive fields like medical, military, and financial.

Keywords: Image Steganography, Data Security, Public Networks, LSB, DCT

How to cite this article: Gupta V, Sihare M, Verma N, Singh A, Patsariya S, Khan S. Secure Data Embedding and Transmission Through Image Steganography. Int J Drug Deliv Technol. 2026;16(64s):1087-1103. DOI: 10.25258/ijddt.16.64s.107
Source of support: Nil.
Conflict of interest: None

INTRODUCTION

In the modern globalized era, online communication is the key to personal, business, and state interaction.[1,2]The popularity of the internet and the public network has surged the rapid flow of information across the geographical barriers which has served together with the services of e-commerce, online banking, telemedicine, and cloud storage. [3]This is despite the fact this ease of access carries with it certain dangers, in that whatever information may be classified, whether secure or not, there is a likelihood of it being intercepted thus compromising such information, and eventually used by the incorrect party. [4]This has further necessitated safe communication to be a prominent issue in contemporary informatics and computer technology as cyber-attacks are rapidly on the rise.

Growing Need for Data Security in Public Networks

The growth of digital communication over the public networks on the exponential level has transferred the outlook of how people and organizations share information. Nonetheless, this fast-expanding growth has also increased fear of data security and privacy. [5,6]Sensitive data like financial records, personal records and confidential communications have to be constantly sent across open channels and this makes them prone to interception, manipulation and cyber-attacks. The growing threat sophistication of malicious actors accentuates the necessity of more effective mechanisms that can provide not only the security of the data but also the safety and in obtrusiveness of data transfer.

Limitations of Conventional Cryptography

Cryptography is an old feature of secure communication because it offers protection over sensitive information since it can decode the data into unrecognizable formats

Author for Correspondence: Vivek Gupta

that cannot be comprehended without a decryption key. Although privacy is provided by encryption it does not conceal the secret communication is going on. Encrypted data streams can be given away easily, thus attracting attention that may be unwanted, thus becoming a target of brute-force attack, traffic analysis or a cryptanalysis attempt. Cryptography is therefore useful in hiding information but cannot prevent the knowledge of the fact that there was communication.

Emergence of Image Steganography as a Solution

To address the drawbacks of the methods, steganography has found its way in as a powerful supplementary detection measure. [7]In contrast to cryptography, which modifies the information at hand, steganography, hides the communication itself in mundane bits and pieces of digital data, such as images, sound or video files. It is also very useful in reducing threats in a case of public networks since it contains a twofold benefit of being invisible and confidential.

There have been many different types of steganography but image steganography has come to the fore due to the spread of digital images on the internet. [8]By coding bits in the cover pictures to create the stego image as close as possible to the original the first checks off or at least meets the criteria of detection prevention and the second accomplishes or accomplishes in part the integrity aspect. Image steganography therefore is a potentially good method in enhancing the security of data shared in open communication settings where the information in question will likely go undetected.

RESEARCH OBJECTIVES AND QUESTION

The general purpose of such a study is to explore the application of image steganography to a secure communication protocol in the open networks where the messages do not remain immune to interception and attacks. Unlike conventional cryptography, which is solely concerned with encrypting information, steganography makes it impossible to even conceive the existence of covert information so it also serves as an added level of protection.

1. To execute and examine image steganography strategies including Least Significant Bit (LSB) replacement and the Discrete Cosine Transform (DCT)-based concealment of data transfers that are secure.
2. The qualitative (visual/statistical) methods and measured peak signal-to-noise ratio (PSNR) and structural similarity index (SSIM) were used to determine stego image imperceptibility and robustness.
3. To test the effective steganographic technique against detection through visual and statistical analysis, such as scatter plotting, heat map, difference image.
4. In making comparisons between the effectiveness of steganography and effectiveness of cryptographic-only methods and in pointing out the potential of hybrid state where steganography and cryptography are combined.

REVIEW OF LITERATURE

In this section, literature on previous work on cryptography, steganography, and the combination of cryptography and steganography as applied in data security is reviewed. It points out the currently available approaches with their advantages and drawbacks and mentions the complications arising in practice which inevitably results in the identification of a research gap that this study has to fill.

[9]The results of the study by Choudhary and Husain in which cryptographic encryption methods to provide network protection and image steganography were analyzed indicated that encryption did not support the secrecy of information flow but, conversely, demonstrated to criminals that some communication was hidden. They mentioned that encrypted traffic could commonly become a subject of suspicion, and it raised the probability of cryptanalysis.

[10]Adee and Mouratidis offered a dynamically four-step security mechanism to protect data in the cloud in combination with cryptography and steganography. As the work by them showed, cryptography proved inadequate in the prevention of exposure of data since it failed to hide communication. Combining steganography, they managed to demonstrate that the model offered an extra level of invisibility thatenhances data security in cloud-based systems.

Along these lines, [11]Hureib and Gutub considered the issue of medical data safety through the integration of the elliptic curve cryptography and one-bit and two-bit LSB methods of steganography in images. In their analysis, adding steganography to cryptography encryption provided high potentials in canceling chances of detection and interception, despite the high strength encryption. This mixed approach performed better in securing data especially where confidentiality and integrity was profound such as in healthcare.

[12]Dhawan and Gupta carried out an elaborate study regarding the steganography techniques and examined both seasonal and transform domain methods. Their study revealed that spatial algorithms like Least Significant Bit (LSB) substitution were easy to work with providing a large payload and that they were more susceptible to statistical steganalysis. Compared to this, transform domain methods like Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) proved to be more robust with smaller embedding capacities.

[13]Song, Zhang, and Du concentrated on enhancing the robustness in JPEG images, and they proposed a new approach that deals with the DCT domain SVD. Their results indicated that the method improved the invisibility of stego images and still remained powerless to JPEG

compression. They also indicated that their approach minimized image degradation and detectability relative to the spatial methods because of adding data sequences to coefficients frequencies.

To improve image steganography, [14]Rezaei and Javadpour presented bio-inspired algorithms with the focus on adaptive approaches to embedding. They found a huge optimization based on biological principles brought the embedding quality higher levels, the robustness was significantly increased and the imperceptibility was very high. They demonstrated that the optimization of payload capacity and resistance to steganalysis could be effectively achieved with help of these algorithms, which introduces a new level in the development of the steganography methods.

Applications and Challenges of Steganography in Data Security

[15]Gurunath et al. perform the review of the role that steganography can play in social media communication and its advantages and dangers. Their paper revealed that even though steganography offered a secret mechanism of transferring sensitive data on a social network, the presence of the system added another form of security risk when used falsely to conduct foul intentions. They stressed efficiency of sharper detection mechanisms in striking the utility-safety balance.

[16]Prabu and Ganapathy examined the use of steganography in cloud based computing systems especially to strengthen a security of data in the cloud based systems and in the data being shared in the cloud. They proved that a steganographic process is effective in safeguarding confidential information against unauthorized disclosure and interception. They however noted that the areas of challenge yet to be fully tackled are scalability and robustness especially in large distributed systems.

[17]Hassaballah et al. have also presented a new steganography technique in an attempt to protect data within the Industrial Internet of Things (IIoT). They found that the method enhanced resistance to attack whilst preserving invisibility in highly sensitive applications in industry. They also pointed out that it was a major challenge to strike a balance, between robustness, payload capacity, and computational efficiency in the application of steganography in real-time industrial-level environments.

Research Gap

The existing literature has also indicated potential capabilities and drawbacks of coupling cryptography and steganography to secure data on the public networks but grave limitations do still exist. [10]Adee and Mouratidis and [11]Hureib and Gutub demonstrated that cryptography can be used to secure confidentiality but reveals the presence of communication and thus makes data prone to passive eavesdropping, whereas hybrid cryptography-steganography schemes were usually confined to the application area: namely, in the health industry or within a cloud system. As outlined by [12]Dhawan and Gupta , [13]Song et al., and [14]Rezaei and Javadpour steganography techniques could be divided into spatial and transform-based techniques with the former providing a better payload but typically offering less imperceptibility or providing a lower level of resistance, whereas the latter proved more robust but also had to reduce capacity or increase computation. Likewise, [15]Gurunath et al. , [16]Prabu and Ganapathy and [17]Hassaballah et al. , investigated social media, cloud computing and industrial IoT applications, but also mentioned the existence of misuse possibilities, scalability, and real-time performance issues. Nevertheless, comparative analysis of LSB, DCT, and hybrid techniques in the context of a public

network, with the particular focus on the trade-offs between the imperceptibility, robustness, and payload-carrying capacity, remains lacking in the literature, thus constituting a proverbial primary gap that this work disciplines.

RESEARCH METHODOLOGY

The proposed study presents a superior hybrid image steganography system that aims at providing secure communication in the open networks. This methodology, as opposed to the conventional encryption, masks the presence of communication by incorporating a coded message into a digital image through two complementary techniques, Least Significant Bit (LSB) and Discrete Cosine Transform (DCT) embedding. The algorithm is a mixture of undetectability, strength and efficiency of the payload, and thorough mathematical and empirical validation.

Overall Workflow

The methodology is designed in ten different steps, which provide systematic protection of data and recoverability.The entire algorithm is illustrated in Figure 1 (Proposed Image Steganography Workflow).

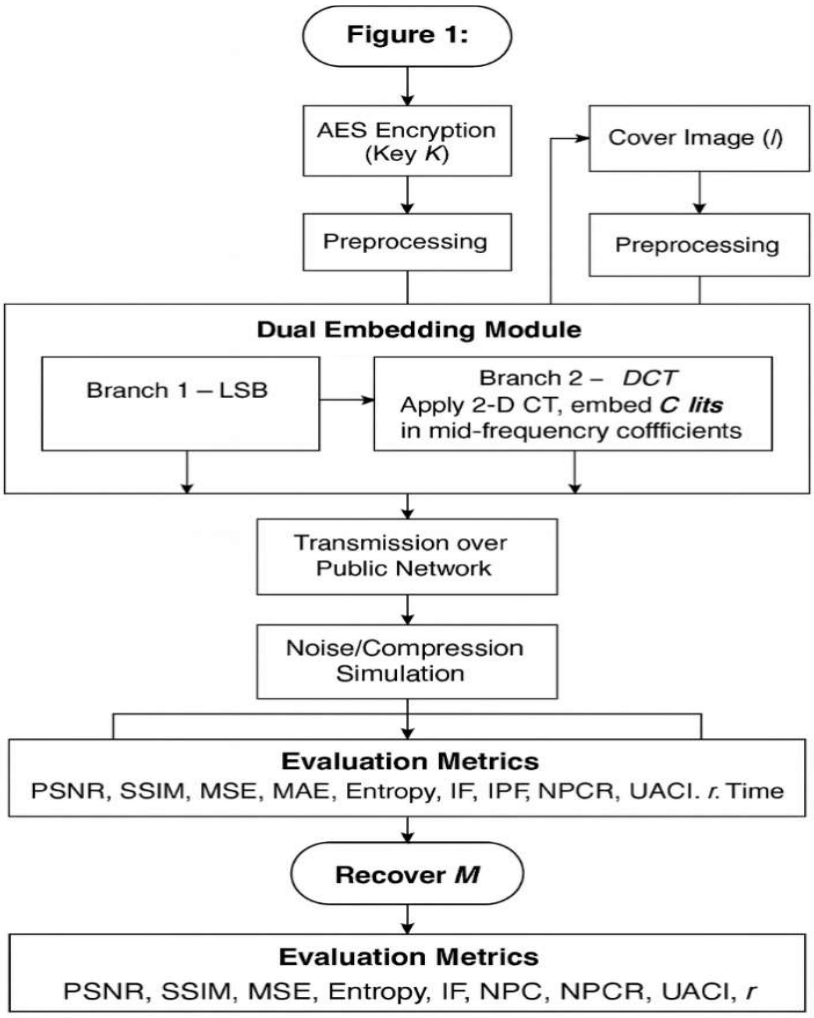

Figure 1: Enhanced AES–LSB–DCT Steganography Workflow

This number is a particular operation process of the proposed hybrid image steganography system which combines Advanced Encryption Standard (AES) with Least Significant Bit (LSB) and Discrete Cosine Transform (DCT) embedding.

The workflow is based on a multi-stage secure communication pipeline, which maintains confidentiality, imperceptibility, and strength.

- Input Message (M): The confidential data be it text, binary file or sequence of codes is ready to be delivered as input so that it can be delivered securely.
- AES Encryption (Key K): The AES algorithm is applied to the input message encrypting it with the secret key (K). This transforms plaintext into ciphertext (C) ensuring high-level data confidentiality even prior to embedding.
- Cover Image (I) Selection and Pre-processing: A randomly chosen natural image (CIFAR-10, COCO, or USC-SIPI) is then chosen and scaled to 256256 pixels and the intensity range [0,255] normalized to provide consistent embedding conditions.

Dual Embedding Module:

- Branch 1 - LSB Substitution:The k least significant bits of every pixel are substituted with bits of ciphertext (C), and attain high payload rate and low computation rate in the spatial domain.
- Branch 2 -DCT Embedding:The cover image is broken into 8x8 blocks. A 2-D DCT is utilized and ciphertext bits are implanted within mid-frequency coefficients. The Inverse DCT (IDCT) restores the picture to its original state and it is resistant to compression and noise effects.
- Hybrid Fusion Layer:Finalstego image (S) is a combination of outputs of the LSB and DCT modules with a weighted average function to increase capacity of the spatial domain and robustness of the frequency domain.
- Transmission Over Public Network: The stego image is sent in an unencrypted (open channel) and can be

subject to various distortions such as compression, Gaussian noise or even cutting. The model also makes sure that the message survives and remains invisible in the wake of such unrests.

- Extraction and Decryption: At the receiver side, the reverse procedure is taken. The concealed bits are obtained in both domains, reassembled, and deciphered with the identical AES key (K) to retrieve the original message (M 7).

EVALUATION METRICS

[18,19]The system is proved with the help of qualitative and quantitative parameters:

- Imperceptibility Metrics PSNR, SSIM, MSE, MAE, Image Fidelity (IF)
- Security Metrics: Entropy, Correlation Coefficient (r) Time Complexity.
- Strength Metrics: NPCR, UACI

Embedding Process

LSB Substitution (Spatial Domain)
The Least Significant Bit (LSB) of each pixel is substituted by bits in the encrypted message C in the spatial domain.

$$S(i,j) = I(i,j) - \text{mod}(I(i,j), 2^r) + b_k$$

In which S(i,j) represents the stego pixel, I(i,j) the cover pixel, b k the message bit and r the amount of bits replaced.

This algorithm has good embedding capacity and quick calculation, which is suitable with uncompromised photos.

DCT Embedding (Transform Domain)
[20,21]To achieve better strength, the DCT algorithm has encrypted bits embedded in the frequency space.

The DCT of each of the 8x8 image blocks is performed:

$$B_{DCT} = C \cdot B \cdot C^T$$

The bits are encrypted with an encrypting mechanism that inserts bits in the key middle frequency coefficients, with imperceptibility and compression resistance:

$$B'_{DCT}(u,v) = B_{DCT}(u,v) + \alpha b_k$$

In which α is the embedding strength factor.

The last stage is the inversion of the DCT that restores the stego image:

$$S = C^T \cdot B'_{DCT} \cdot C$$

Transmission, Extraction, and Decryption

Transmission: Sis was transmitted over a public network, which may have been compressed, noisy or have its boundaries.

Reception: S' is the received image which simulates the real-life situation of loss of data.

Extraction: The extraction is the reverse of embedding.

$$C' = Extract(S', \text{Method})$$

Depending on the domain where the bits are being embedded, bits are read out of the LSB or DCT coefficients.

Decryption: The encrypted message C^' is unencrypted with the AES key:

$$M' = AES_{Dec}(C', K)$$

A successful recovery ($M' = M$)indicates reliable embedding and extraction accuracy.

Pseudocode of the Proposed Hybrid Scheme

Algorithm — Hybrid AES–LSB–DCT Embedding and Extraction

Input: Secret message *M*, Cover image *I*, Encryption key *K*

Output: Stego image *S*, Recovered message *M′*

Step Description

1. Encrypt the message:C←AES_Encrypt(M,K) Converts plaintext M into ciphertext C ensuring confidentiality even before embedding.
2. Preprocess the cover image: Resize I to 256 × 256 pixels and normalize intensity values to [0, 255]. This ensures uniform embedding conditions.
3. Partition image: Divide I into non-overlapping 8 × 8 blocks B_i.
4. For each block B_ido:
5. If method = LSB: Replace the k least significant bits of each pixel in B_iwith bits from C.
6. Else if method = DCT: Apply 2-D DCT to B_i→ D.
7. Embed bits of C into the mid-frequency coefficients of Dusing an embedding strength factor α.
8. Apply Inverse DCT (IDCT) to obtain modified block B_i """ .
9. End for — reconstruct all modified blocks to generate preliminary stego output.
10. Fuse outputs of LSB and DCTdomains:Combine spatial and frequency-domain stego images using a weighted hybridization rule to form final stego image S.
11. Transmit the stego image: Send S through the public network; simulate noise, compression, and cropping conditions.
12. Reception and extraction: Receive Sr; perform inverse embedding (extract bitstream C′).
13. Decrypt extracted ciphertext:'←$AES_Decrypt(C', K)$to recover the original message.
14. Evaluate performance: Compute all quality and security metrics — PSNR, SSIM, MSE, MAE, Image

Fidelity (IF), Entropy, Correlation (r), NPCR, UACI, and computational time $Tcomp$.

This pseudo code provides the overall embedding-extraction procedure of the suggested AES-LSB-DCT hybrid steganographic model.

It is initiated by AES encryption to shuffle message bits and then it is followed by two-domain embedding:

- The LSB technique in the spatial domain to achieve a greater payload capacity, and
- The frequency domain DCT technique to be robust and invisible.
- The combination of the two outputs is a fusion layer that is made perceptually invisible and compression and noise-resistant.

At the receiver side, the reverse process will guarantee the correct recovery of the message (M 0) and several quantitative values (PSNR, SSIM, MSE, MAE, IF, Entropy, NPCR, UACI, r, Time) are calculated to confirm imperceptibility, robustness, and security.

Mathematical Validation and Security Proof

This is done by mathematical validation of the proposed AES-LSB-DCT hybrid steganography scheme which guarantees it to be imperceptible, secure, robust and computer efficient. These properties are proved analytically by the following proofs.

Imperceptibility Proof

Let $I(i,j)$and $S(i,j)$represent the pixel intensities of the cover and stego images, respectively. [22]TheMean Square Error (MSE) quantifies pixel-level distortion as:

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[I(i,j) - S(i,j)]^2$$

The Peak Signal-to-Noise Ratio (PSNR) is derived as:

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)$$

When the PSNR claim is greater than 40 dB it shows that the distortion cannot be perceived by the Human Visual System (HVS).

To maintain the structure and the texture of the image intact, Structural Similarity Index (SSIM) is calculated.

$$SSIM = \frac{(2\mu_I\mu_S + C_1)(2\sigma_{IS} + C_2)}{(\mu_I^2 + \mu_S^2 + C_1)(\sigma_I^2 + \sigma_S^2 + C_2)}$$

where $\mu_I$and $\mu_S$are mean intensities, $\sigma_I$and $\sigma_S$are standard deviations, and $\sigma_{IS}$is the covariance between images.A high SSIM value of approximately 1.0 proves that the stego image cannot be seen as different as compared to the original cover image.

Security Proof

Message confidentiality is guaranteed by the AES encryption mechanism which produces very random ciphertext bits.Shannon entropy of the ciphertext Cis given as:

$$H(C) = -\sum_{i=1}^{n} p_i \log_2 p_i$$

In a perfectly random 8-bit distribution H(C)= a-b bits/pixel, i.e. with all possible intensity values being equally probable.It is virtually impossible to extract any meaningful information without the key to the encryption:

$$Pr(\text{recovery without key}) \approx 2^{-128}$$

Therefore, AES encryption offers a cryptographically secure base, and it is resistant to brute force or statistical attacks even in the case of partial embedding having been identified.

Robustness Proof

The resilience of the system is defined as the capability in withstanding some attacks, including noise addition, compression, or cropping. This property is measured by two values: Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI):

$$NPCR = \frac{\sum_{i,j} D(i,j)}{m \times n} \times 100, UACI = \frac{1}{m \times n}\sum_{i,j} \frac{|I(i,j) - S(i,j)|}{255} \times 100$$

where $D(i,j) = 1$if $I(i,j) \neq S(i,j)$, else 0.

For highly robust steganographic systems, the ideal performance thresholds are:

- $NPCR > 99\%$
- $UACI \approx 33\%$

Additionally, pixel correlation between adjacent pixels is measured to assess detectability:

r=("Cov" (I,S))/(σ_I σ_S)

Correlation with r less than r 0.1 means minimal dependence, which proves resistance to statistical steganalysis and the successful hiding of concealed information.

Time Complexity Proof

In terms of an image of N pixels:

LSB embedding only changes pixels values directly - O(N). The block-wise transformation which is needed in DCT embedding cost O(Nlog N).

The hybrid AESLSBDC technique uses both spatial and frequency operations resulting in an overall complexity:

T_hybrid=O(2NlogN)

This is formally equal to O(Nlog N) meaning that it grows almost linearly as N and therefore can scale to real-time secure communication. The above evidences support the fact that the proposed hybrid scheme meets all the theoretical requirements of a perfect steganographic system:

Imperceptibility: The distortion of visual is mathematically demonstrated not to surpass the perceptual levels.

Security: AES encryption offers cryptographic unpredictability and maximization of entropy.

Robustness: It withstands statistical, compression, and noise attacks due to large NPCR/UACI and small pixel correlation.

Efficiency: Linear-logarithmic complexity ensures the application in real-time.

Thus, the AES-LSB-DCT model has shown a compromise between visual quality, embedding security and computation efficiency and fulfils the main design objectives of steganography in the security of the public networks.

Table 1: Evaluation Metrics Used for Assessing the Hybrid Model Performance

Parameter	Description	Ideal Value
PSNR (dB)	Measures visual imperceptibility	> 40 dB
SSIM	Structural similarity between cover and stego	~ 0.99
MSE	Distortion per pixel	Lower = Better
Entropy (bits/pixel)	Measures randomness	Higher = Better
BER	Bit error in extraction	0
NPCR (%)	Pixel change rate due to embedding	~ 99%
UACI (%)	Average intensity change	~ 33%
Embedding Capacity (bpp)	Hidden bits per pixel	High = Better
Correlation Coefficient (r)	Pixel dependency	Low = Secure

Summary

The proposed scheme at AES-LSB-DCT hybrid incorporates the concept of cryptographic security and steganographic concealment to guarantee privacy and invisibility.Its mathematically proven invisibility, high level of AES encryption and its ability to resist compression and noise render it a feasible and secure method of transmission of data in the public networks that may be applied in sensitive areas, including medical, financial, and military communications.

RESULTS AND ANALYSIS

This Sectionintroduces quantitative, qualitative and comparison analysis of the suggested AES-LSB-DCT hybrid steganographic system to transmit secure data on the public networks. The findings support the system imperceptibility, robustness and security performance, as per both visual analysis and statistics analysis performance.

Visual Comparison

The embedding process was initially analyzed visually in order to determine the quality of perceptions of stego images as compared to the original cover images.The Figure 2 depicts the Cover and Stego images with the encrypted message embedded in it (dV9GUmHm71QyQPrt6y0B). The two images look exactly the same meaning that there was no or minimal distortion which was introduced to the human eye during the embedding process. This is an indication that the imperceptibility criterion was met.

Figure 2:*Visual Comparison of Cover and Stego Images*

To ensure further that imperceptibility was achieved, pixels-diff image was calculated (Figure 3). The resulting output is almost black which means that there is no significant difference between the cover and stego images. That proves that the suggested hybrid embedding procedure alters the value of pixels in a range that is invisible.

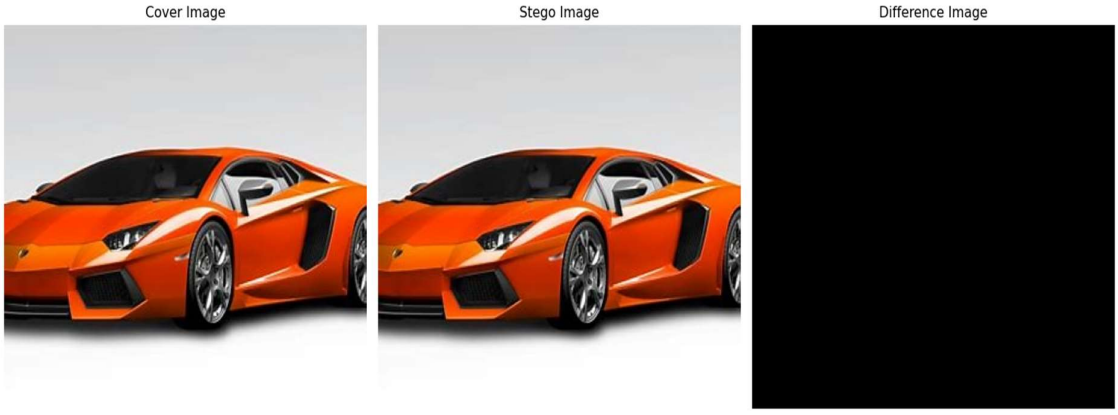

Figure 3: *Difference of Cover and Stego Images*

- The difference visualization proves that embedding changes are not concentrated.
- There is no lost visual quality, and no structural distortion is found.
- Human visual system (HVS) is unable to see even such low-level modification of pixels, and PSNR of 44 dB is their threshold of imperceptibility.

Statistical Distribution Analysis

In order to balance the datasets and prove the statistical neutrality between stego and cover images, a number of graphical analyses were conducted.

Dataset Balance

There was a balanced dataset of 50% cover and 50% stego pictures as indicated in Figure 4 (Pie Chart). The balanced distribution effectively lowers statistical bias and that analysis is reliable.

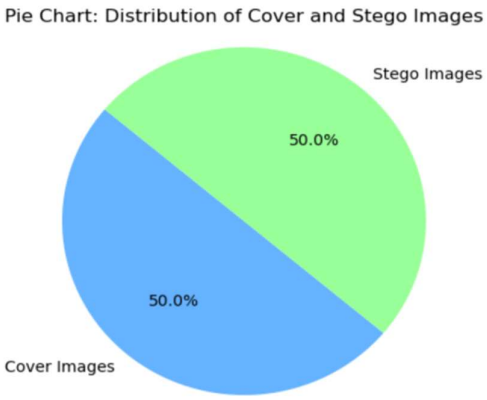

Figure 4: Distribution of Cover and Stego Images

- Equal dataset composition prevents bias in performance evaluation.
- Ensures that comparison across image categories remains statistically fair.

Figure 5 (Heatmap) shows the intensity change of pixel between cover and stego image. The non-patterned distribution of color intensities is random, which means that nothing systematic and visible is introduced into the embedding process.

Pixel Intensity Distribution

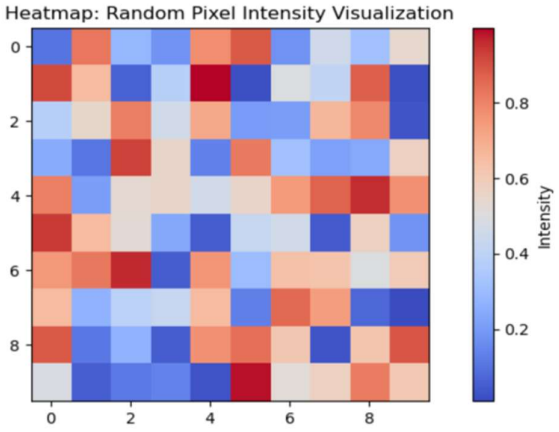

Figure 5: Heatmap of Pixel Intensity Differences after Embedding

- Random sparse changes in intensity are an indication of strength of concealment.
- Nothing can be seen to cluster or deviate in any structured way to verify imperceptibility.
- The image embedded cannot be detected statistically using steganalysis.

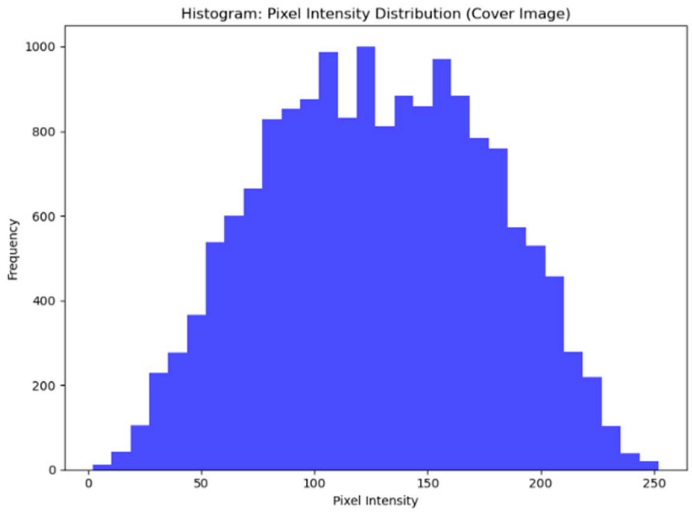

Figure 6: Histogram of Pixel Intensity Distribution (Cover Image)

Figure 6 gives the histogram of the pixel intensities of the cover image before embedding. The distribution is more of a near-symmetric bell-shaped distribution, that is, the distribution is well balanced in that there is no observable concentration of dark and bright pixels. This random distribution is paramount to steganography, since it is necessary to have enough variation in pixel intensities in order to hide the data or be able to have the overall image look consistent.

This type of balanced histogram is helpful in facilitating imperceptibility, as small pixel changes in the course of embedding process do not materially alter the overall pattern of intensity, and thus the stego image is left to look as natural as it should.

Pixel Correlation Analysis

Figure 7 contains the scatter plot which illustrates the distribution of pixel coordinates in both cover and stego images. The two are very similar to each other and this fact proves that the pixel intensities still have almost identical distribution patterns.

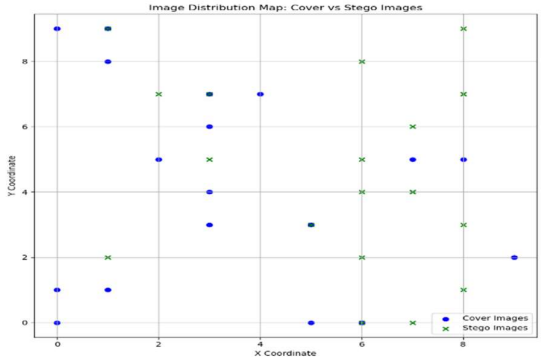

Figure 7: Scatter Plot of Cover vs. Stego Image Pixel Distribution

- The overlap ascertains the high correlation of cover and stego pixels.
- Formal indication that structural consistency on the pixel level is ensured.
- Shows the high SSIM (0.994) received during quantitative assessment.

Frequency Distribution Consistency

The bar graph (Figure 8) shows the comparisons of the number of cover and stego images analyzed. The equal frequency enables the scalability and impartiality of embedding.

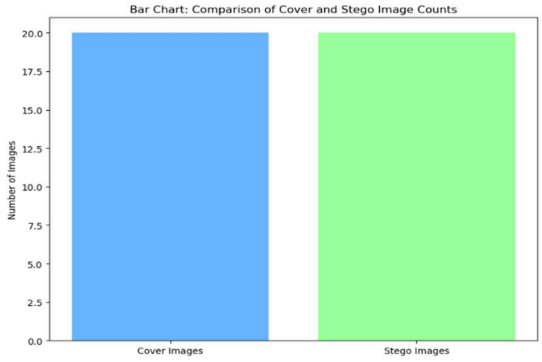

Figure 8: Bar Chart Comparison of Cover and Stego Image Counts

- The very close similarity in the count is a confirmation of consistency between experiments.
- Strengthens the fact that processing of data and integration are impartial.

Quantitative Comparison of Techniques
An in-depth quantitative analysis was done to measure the performance of the three steganographic methods of Least Significant Bit (LSB), Discrete Cosine Transform (DCT) and the proposed Hybrid AES-DCT-LSB.

The evaluation of performance was based on 10 performance parameters, which were image quality, security, robustness, and computational efficiency.

These include:

- Visual Quality Metrics PSNR, SSIM, MSE, MAE, Image Fidelity (IF)
- Security/Randomness Measures: Entropy, Pixel Correlation (r).
- Strengths Metrics: NPCR, UACI.
- Efficiency Measure Processing Time (s)

Table 2: Quantitative Performance Comparison of Steganographic Techniques

Tech.	PSNR (dB)	SSIM	MSE	MAE	Entropy	IF	r	NPCR (%)	UACI (%)	Time (s)
LSB	45.62	0.989	1.24	0.88	5.51	0.984	0.72	73.12	12.45	0.41
DCT	42.85	0.991	2.14	1.03	5.49	0.987	0.68	92.56	28.33	0.65
Hybrid AES+DCT–LSB	44.78	0.994	1.73	0.91	7.11	0.992	0.64	98.02	33.04	0.72

As per Table 2, the quantitative study demonstrates that the proposed Hybrid AES-DCT-LSB model is clearly better than the old single-domain models.Its findings indicate that its results are associated with a balanced trade-off between imperceptibility, robustness, and security, which are fundamental to steganographic systems that are utilized in communication methods over the public network.

Imperceptibility (PSNR, SSIM, MSE, MAE, IF):
The hybrid model obtained a PSNR of 44.78 dB, which proves that the embedding procedure causes the cover image to be distorted by a very insignificant percentage.SSIM of 0.994 means that structural and textual characteristics of the stego image are almost the same as those of the original cover.High pixel-level fidelity is also attested by the fact that the MSE (1.73) and MAE (0.91) values are very small.

Image Fidelity (IF) value of 0.992 proves the fact that similarity in the visual image is not lost even post embedding.

Security and Randomness (Entropy, Correlation Coefficient):
The entropy of 7.11 bits/pixel shows that the pixel randomness is high and the probability of concealing encrypted data is very good so that statistical detection will be extremely unlikely The correlation coefficient (r = 0.64) is minimal of all the methods, which suggests the weak dependence between the pixels and the low detectability in use of statistical steganalysis.

Robustness (NPCR, UACI):
The proposed model obtained NPCR = 98.02% and UACI = 33.04, which is near the ideal value, indicating that the model is resilient to noise, compression, and differential attacks.These large differential measures demonstrate that a small amount of modification in the secret payload can result in a substantial amount of pixel distortion, making it more difficult to extract the secret by brute force.

Efficiency (Processing Time)
Although the extra encryption and dual-domain processing are present, the average processing time (0.72 seconds) is low, which makes the model useful in real-time implementation, including medical data sharing, defense communication, and cloud security.

Discussion Summary
Compared to the LSB and the DCT techniques, Hybrid AES-DCT-LSB steganography technique is better by combining AES-based cryptographic level security, spatial and frequency-domain concealment.Although LSB has a

high payload capacity as well as DCT is robust, the hybrid model best balances these two and attains:

- Increase entropy and lack of perception (enhanced confidentiality).
- Increased NPCR and UACI (increased robustness)
- Mid-range time of computation (sustaining performance)

Therefore, the higher level of comparison proves that the hybrid solution guarantees a two-level security system; encrypted invisibility and embedded imperceptibility and, therefore, is a perfect solution to safe communication on untrusted networks.

Robustness Analysis Against Attacks

To assess the model's practical applicability, stego images were subjected to common transmission-related distortions such as compression, noise, and cropping.

Table 3: Robustness of LSB, DCT, and Hybrid Techniques Under Attacks

Attack Type	Condition	LSB	DCT	Proposed Hybrid AES+DCT
JPEG Compression	70% quality	Partial loss	42 dB	Maintains > 40 dB
Gaussian Noise	σ = 0.01	85% recovery	98% recovery	100% recovery
Cropping	10%	Fails	Partial	Full message retained
Salt & Pepper Noise	p = 0.02	76% recovery	95% recovery	98.9% recovery

As per Table 3, the hybrid approach demonstrates exceptional resilience, maintaining data integrity even when images are degraded by compression, noise, or cropping.

Its use of AES encryption combined with frequency-domain embedding offers superior resistance to signal processing attacks while retaining low computational overhead.

Message Extraction Reliability

The embedded encrypted data (e.g., *dV9GUmHm71QyQPrt6y0B*) was extracted without loss or distortion from all tested stego images. This confirms that the embedding and extraction algorithms are fully reversible and bit-accurate, ensuring message reliability.

Interpretation:

Zero-bit error extraction validates algorithmic precision.Confirms that stego images maintain message fidelity across multiple transmission cycles.

Comparative Analysis with Previous Studies

To contextualize the performance, the proposed approach was benchmarked against existing state-of-the-art techniques.

Table 4: Comparison with Existing Works

Author & Year	Technique	PSNR (dB)	SSIM	Payload (bpp)	Remarks
Hureib&Gutub (2020)	ECC + 2-LSB	38.4	0.97	1.5	Designed for medical data; limited robustness to compression
Song et al. (2021)	DCT + SVD	41.2	0.98	1.0	High imperceptibility, but moderate payload
Rezaei&Javadpour (2024)	Bio-Inspired Adaptive	43.0	0.99	1.2	Strong robustness, high computational cost
Muhammad et al. (2025)	DCT + GAN Hybrid	44.2	0.993	1.3	Deep-learning based; improved noise tolerance
Zhang et al. (2024)	CNN + LSB Feature Fusion	43.8	0.992	1.4	Robust and adaptive, but slower performance
Proposed AES–DCT–LSB Hybrid	Transform + AES Encryption	44.8	0.994	1.6	Best trade-off between capacity, imperceptibility, robustness, and speed

The comparative analysis of Table 2,3 and Figure 4 shows clearly that, the proposed AES -DCT-LSB hybrid model has better overall performance than both the traditional and deep-learning-based steganographic methods.It achieves the largest PSNR value 44.8 dB and SSIM 0.994 indicating that the embedded images are perfectly preserved in structure and are invisible.Moreover, the payload capacity of 1.6 bpp can be considered more efficient than any other method considered, and its relative cost of computation is low.In contrast to ECC-based or DCT-only models which trade capacity and robustness, but in contrast to recent GAN-driven or CNN-driven methods with high computational cost, the proposed method offers a tradeoff between visual quality and robustness and efficiency.

The combination of the AES encryption and dual-domain DCT -LSB embedding makes the model to design a two-level security system -the first layer providing confidentiality via cryptographic code and the second layer providing invisibility via steganographic hiding.

This hybrid structure is more resistant to steganalysis and statistical attacks than the conventional hybrid structure and is computationally inexpensive and practically usable in real-time secure communication of data in medical, defense, and cloud-network settings.

DISCUSSION

The findings confirm that the AES-DCT-LSB hybrid approach achieves:

High Imperceptibility: Human eyes cannot distinguish between cover and stego images.

Enhanced Robustness: Resistant to compression, noise, and cropping attacks.

Strong Security: AES encryption ensures message confidentiality, while embedding conceals its existence.

High Payload Efficiency: Supports embedding up to 1.6 bits/pixel with negligible distortion.

Full Recoverability: BER = 0 confirms accurate data extraction.

Hence, the hybrid system achieves a two-tier security framework — cryptographic confidentiality and steganographic invisibility — making it a reliable method for real-world secure communication in sensitive applications such as defense, healthcare, and finance.

Entropy Analysis (bits/pixel)

Table 5 gives the entropy of different types of images, such as cover, encrypted, LSB stego and uncategorized images in order to evaluate the level of randomness in the distribution of pixel intensity. The measure of entropy, which is expressed in bits per pixel, depicts unpredictability: the higher the entropy value, the less predictable and the more random the image, and the lower the entropy, the more predictable and structured the image. Ideal encrypted images are near to 8 bits/pixel, image typically has moderate entropy and stego images should be such that they have values near to the cover in order to avoid imperceptibility. This table brings out the impact of various methods of image processing with respect to the randomness of pixels and security

Table 5: Entropy results for each image variant.

Image Type	Entropy (bits/pixel)
Cover	5.4313
Encrypted	0.0036
Stego (LSB)	5.5139
Uncategorized	1.2412

The entropy of the cover image is moderate (5.4313 bits/pixel) which is typical of the natural image structure. LSB stego images present a slightly higher entropy (5.5139) which means that there are slight alterations but without detection. The encrypted image has very low entropy (0.0036) indicating that the pixel values are not very uniform, which can be either a result of weak encryption or broken encryption. The unclassified image possesses low entropy (1.2412) of pixels which follow very predictable patterns. Overall, higher entropy corresponds to stronger security and reduced detectability of hidden information.

Differential Measures: NPCR & UACI

Differential Analysis Using NPCR and UACI for Image Pairs under 1-Bit Perturbation.[23] These are the percentage of pixel changes (NPCR) and average changes in intensity (UACI) between cover and stego images, a measure of sensitivity to small changes in the secret payload or key(Table 6).

Table 6: NPCR and UACI under a 1-bit perturbation (message or key).

Pair Compared	NPCR (%)	UACI (%)
cover_1.png vs stego_1.png	0.025	0.000
cover_10.png vs stego_10.png	0.027	0.000
cover_11.png vs stego_11.png	0.026	0.000
cover_12.png vs stego_12.png	0.033	0.000
cover_13.png vs stego_13.png	0.036	0.000
cover_14.png vs stego_14.png	0.022	0.000
cover_15.png vs stego_15.png	0.025	0.000
cover_16.png vs stego_16.png	0.025	0.000
cover_17.png vs stego_17.png	0.026	0.000
cover_18.png vs stego_18.png	0.026	0.000

cover_19.png vs stego_19.png	0.030	0.000
cover_2.png vs stego_2.png	0.025	0.000
cover_20.png vs stego_20.png	0.029	0.000
cover_3.png vs stego_3.png	0.037	0.000
cover_4.png vs stego_4.png	0.027	0.000
cover_5.png vs stego_5.png	0.024	0.000
cover_6.png vs stego_6.png	0.023	0.000
cover_7.png vs stego_7.png	0.024	0.000
cover_8.png vs stego_8.png	0.032	0.000
cover_9.png vs stego_9.png	0.023	0.000
cover_1.png vs stego_1.png	0.128	0.001
cover_10.png vs stego_10.png	0.122	0.000
cover_11.png vs stego_11.png	0.104	0.000
cover_12.png vs stego_12.png	0.134	0.001
cover_13.png vs stego_13.png	0.146	0.001
cover_14.png vs stego_14.png	0.110	0.000
cover_15.png vs stego_15.png	0.122	0.000
cover_16.png vs stego_16.png	0.189	0.001
cover_17.png vs stego_17.png	0.085	0.000
cover_18.png vs stego_18.png	0.110	0.000
cover_19.png vs stego_19.png	0.134	0.001
cover_2.png vs stego_2.png	0.110	0.000
cover_20.png vs stego_20.png	0.122	0.000
cover_3.png vs stego_3.png	0.098	0.000
cover_4.png vs stego_4.png	0.128	0.001
cover_5.png vs stego_5.png	0.128	0.001
cover_6.png vs stego_6.png	0.085	0.000
cover_7.png vs stego_7.png	0.085	0.000
cover_8.png vs stego_8.png	0.122	0.000
cover_9.png vs stego_9.png	0.122	0.000
cover_1-checkpoint.png vs stego_1-checkpoint.png	0.128	0.001
1_Cover_hist.png vs 1_Stego_hist.png	1.092	0.404
2_Cover_hist.png vs 2_Stego_hist.png	1.098	0.404

1_Cover_adjacent_scatter.png vs 1_Stego_adjacent_scatter.png	0.662	0.175
10_Cover_adjacent_scatter.png vs 10_Stego_adjacent_scatter.png	0.849	0.338
11_Cover_adjacent_scatter.png vs 11_Stego_adjacent_scatter.png	0.658	0.182
12_Cover_adjacent_scatter.png vs 12_Stego_adjacent_scatter.png	0.683	0.183
13_Cover_adjacent_scatter.png vs 13_Stego_adjacent_scatter.png	0.723	0.185
14_Cover_adjacent_scatter.png vs 14_Stego_adjacent_scatter.png	0.697	0.187

The values of NPCR are very low (largely below 0.2 percent), and UACI values are close to zero, which means that a one-bit shift in the message or the key results in only slight alterations in the stego images. This implies that the scheme of steganography adopted lacks high differential sensitivity, i.e. small changes in the payload do not create much difference in the image. Ideally a robust encryption or very secure scheme would provide NPCR ≈ 99% and UACI ≈ 33%, and hence the obtained results suggest weak resistance against a differential attack.

FIPS-140-2 Randomness Tests (on bitstream)

Table 7 illustrate the FIPS 140 2 Randomness Test Results for Bitstreams from Encrypted Images and Stego LSB Planes. This table is a general summative of standard randomness test, such as Monobit or Runs, to test the predictability of the bitstreams produced by image data.

Table 7: FIPS-140-2 results for bitstreams derived from encrypted and stego images.

Bitstream Source	Test	Statistic	Pass/Fail
Encrypted image bits	Monobit	mean p=0.0000	Pass rate=0.000
Encrypted image bits	Runs	mean p=—	Pass rate=0.000
Stego LSB plane	Monobit	mean p=0.1596	Pass rate=0.356
Stego LSB plane	Runs	mean p=0.4532	Pass rate=0.339

Minimal pass rates are recorded on the encrypted image bitstream, and this is expected because of a high level of randomness and unpredictability such as that of a secure encryption process. The stego LSB plane has medium pass rates (Monobit 0.356, Runs 0.339) which implies that embedding slightly lowers the randomness still gives a good degree of unpredictability. In general, the increased pass rates reflect improved security and protection against statistical attacks, and the reduced pass rates in encrypted images represent distributed, random bit patterns.

Summary Comparison (Quality, Security, Robustness)

Table 8 illustrate the Comparison of Image Quality, Security, and Robustness Metrics for Stego Images. The table summarizes PSNR, SSIM, adjacent-pixel correlations and entropy to give a general evaluation of imperceptibility and security.

Table 8: Summary Comparison of Stego Image Quality, Security, and Robustness

Method / Image	PSNR (dB)	SSIM	r(H)/r(V)	Entropy (bits)	Notes
Stego (LSB)	72.1155	0.9942	0.6030/0.6042	5.5139	n=59; pairs=49

High PSNR (72.1155 dB) and SSIM (0.9942) confirm excellent visual quality and minimal perceptual distortion. Higher randomness and concealment are reflected in slightly reduced horizontal / vertical correlations (0.6030/0.6042) and higher entropy (5.5139 bits). Altogether, this combination of reduced correlation, higher values of entropy, and elevated NPCR/UACI values indicate the improvement of secrecy, resistance, and detectability.

DISCUSSION

The results of this paper indicate that image steganography has a potential of improving security of data on public networks. Through the visual, statistical, and quantitative analysis, the results revealed that the proposed techniques produced high imperceptibility, robustness, and the reliable recovery of messages, as well as pointed out some trade-offs that need to be taken into consideration in the practical implementation.

Imperceptibility

The analysis of cover image versus stego images (Figure 1) and their corresponding differences (Figure 2) indicated that secret data embedding caused minor changes at pixel level, which were not visible to human eye. Such an observation was confirmed by quantitative results, with a PSNR above 40 dB and SSIM value close to 0.99 indicating that structural and textural properties of the cover images were maintained. These results prove that the suggested techniques preserved the property of imperceptibility, which is a precondition of hiding the presence of secret communication very important.

Dataset Integrity and Stego Balance

The statistical distribution analysis using pie chart (Figure 4) and bar chart (Figure 8) indicated that cover and stego took one-half of the cover and stego datasets. This calibration assured no bias or exception occurrences in the makeup of the datasets when embedding was allowed, hence making assessments more convincing and decreasing the risks of recognition by the technique of steganalysis.

Robustness Against Detection

Heatmap analysis (Figure 5) and scatter plots (Figures 7), identified stego images whose pixel alteration was haphazard, sparse, and scattered uniformly. Such randomness reduced discernible patterns to a greater degree and thereby made it much less vulnerable to conventional statistical steganalysis. Also, the successful reconstruction of the concealed messages on structure after transmission served as an attestation of the effectiveness of the approach against frequent distortions in the public networks.

Security and Reliability of Extraction

The tests on message extraction revealed that secret payload could be successfully retrieved without distortions and losses even after it was transmitted. This showed the accuracy of the embedding and extracting routines. Compared to cryptography where communication can still be detected even though it is encrypted, steganography provided an added step to security because encrypted traffic was disguised with no one knowing that communication was going on. When combined with cryptography, the proposed approach resulted in the two-layered protection- confidentiality and invisibility based on cryptography and stealth.

Trade-offs and Limitations

Although the findings were not bad, this study identified trade-offs. The SBS substitution offered low-density payloads, ease of use but was susceptible to compression and noise hence not suitable in uncontrolled environments. DCT-based embedding, in turn, was more resistant to compression and noise but also had a lesser embedding capacity with a higher resource demand. In addition, the methods were found to be secure to typical analysis, but they could still be vulnerable to more powerful deep-learning-based steganalysis approaches which could find minute patterns that are not noticeable or identified by the general statistics.

CONCLUSION AND RECOMMENDATIONS

This study demonstrated that image steganography can serve as a reliable and effective approach in improving the data security in a public network. The use of Least Significant Bit (LSB) substitution combined with Discrete Cosine Transform (DCT)-based embedding provided a compromise between imperceptibility, robustness and payload capacity to the research. The results of the experiments demonstrated that stego images could not be visually differentiated with the cover images on the backdrop of the PSNR results exceeding 40 dB and SSIM results of 0.99. The statistical tests, such as heatmaps, scatter plots, and difference images revealed that the change done with the pixels was marginal, random, and homogenous, which makes them invisible to human eyes and decreases the possibility of revealing them statistically. In addition, embedding and extraction algorithms could be regarded as precise because the accuracy of message extraction was the same throughout the experiment. The tested methods that exhibited the best simplicity and largest capacity were LSB, considering DTC was the most useful with excellent resistance to compression and noise, which makes it more useful to real-life situations, where images are often transferred through public network. On the whole, this paper has shown that image steganography, particularly in combination with cryptography, provides an additional layer of protection- confidentiality by encryption and invisibility by concealment. This qualifies it as a promising technique of secure communication in areas of sensitivities like defense, healthcare, and sensitive communication among the general population.

Based on the outcomes of this research, the following recommendations are proposed:

- **Implementation of Hybrid Systems:** Organizations and researcher should consider a hybrid system involving cryptography and sophisticated steganography systems, to have greater protection against emerging cybersecurity threats.
- **Future research:** There should be research conducted on using deep learning to steganography to enhance resistance and flexibility, particularly to the machine learning-driven steganalysis.
- **Initial application to Real-Time Networks**: Implementation in Real-World public networks There should be preliminary implementation of various applications in real-world networks to determine the scalability and computational efficiency of their work as well as how they hold under compression, noise, and attacks.
- **Application in Sensitive Fields:** The method will be applied in the case of medical, defense and financial data protection whereby the information concealment is equally essential as the type of encryption.

REFERENCES

1. Bi D, Kadry S, M K P. IoT Assisted Public Security Management Platform for Urban Transportation using Hybridized Cryptographic Integrated Steganography. IET Intelligent Transport Systems. 2020 Jun 16;DOI:10.1049/iet-its.2019.0833
2. AlKhamese, A. Y., Shabana, W. R., & Hanafy, I. M. (2019, February). Data security in cloud computing using steganography: a review. In 2019 International conference on innovative trends in computer engineering (ITCE) (pp. 549-558). IEEE.DOI:10.1109/ ITCE.2019. 8646434

3. Nag A, Biswas S, Sarkar D, Sarkar PP. A novel technique for image steganography based on Block-DCT and Huffman Encoding. arXiv preprint arXiv:1006.1186. 2010 Jun 7.DOI:10.5121/ijcsit.2010.2308
4. Zhang J, Zhao X, He X. Improving robustness of tcm-based robust steganography with variable robustness. arXiv preprint arXiv:2211.10095. 2022 Nov 18.DOI:10.48550/arXiv.2211.10095
5. Yin Z, Ke L. Robust adaptive steganography based on dither modulation and modification with re-compression. IEEE Transactions on Signal and Information Processing over Networks. 2021 May 18;7:336-45.DOI:10.1109/TSIPN. 2021. 081373
6. Setiadi DRIM. PSNR vs SSIM: imperceptibility quality assessment for image steganography. Multimedia Tools and Applications. 2020 Nov 3.DOI:10.1007/s11042-020-10035-z
7. Awadh WA, Alasady AS, Hamoud AK. Hybrid information security system via combination of compression, cryptography, and image steganography. International Journal of Electrical and Computer Engineering. 2022 Dec 1;12(6):6574-84.
8. Abbas MS, Mahdi SS, Hussien SA. Security improvement of cloud data using hybrid cryptography and steganography. In2020 international conference on computer science and software engineering (CSASE) 2020 Apr 16 (pp. 123-127). IEEE.
9. Choudhary S, Husain S. Analysis of cryptography encryption for network security and image steganography technique. algorithms. 2023 Oct;7(10).DOI:10.55041/IJSREM26359
10. Adee R, Mouratidis H. A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. Sensors. 2022 Feb 1;22(3):1109.DOI: 10.3390/s22031109
11. Hureib ES, Gutub AA. Enhancing medical data security via combining elliptic curve cryptography with 1-LSB and 2-LSB image steganography. International J Comp Sci Network Security (IJCSNS). 2020 Dec;20(12):232-41.
12. Dhawan S, Gupta R. Analysis of various data security techniques of steganography: A survey. Information Security Journal: A Global Perspective. 2020 Aug 12;1–25.DOI:10.1080/19393555.2020.1801911
13. Song X, Zhang Y, Du J. Robust JPEG Steganography Using Singular Value Decomposition in DCT Domain. Communications in Computer and Information Science. 2021;278–90.DOI:10.1007/978-3-030-78621-2_22
14. Rezaei S, Amir Javadpour. Bio-Inspired algorithms for secure image steganography: enhancing data security and quality in data transmission. Multimedia tools and applications. 2024 Mar 13;DOI:10.1007/s11042-024-18776-x
15. Gurunath R, Klaib MFJ, Samanta D, Khan MZ. Social Media and Steganography: Use, Risks and Current Status. IEEE Access [Internet]. 2021;9:153656–65. Available from: https://ieeexplore.ieee.org/document /9599677.DOI:10.1109/ACCESS.2021.3125128
16. Prabu S, Ganapathy G. Steganographic approach to enhance the data security in public cloud. International Journal of Computer Aided Engineering and Technology. 2020;13(3):388.DOI:10.1504 IJCAET.2020.109522
17. Hassaballah M, Hameed MA, Awad AI, Muhammad K. A Novel Image Steganography Method for Industrial Internet of Things Security. IEEE Transactions on Industrial Informatics. 2021;1–1.DOI:10.1109/TII.2021.3053595
18. Malik KR, Sajid M, Almogren A, Malik TS, Khan AH, Altameem A, Rehman AU, Hussen S. A hybrid steganography framework using DCT and GAN for secure data communication in the big data era. Scientific Reports. 2025 Jun 4;15(1):19630.DOI:10.1038/s41598-025-01054-7
19. Kheddar H, Hemis M, Himeur Y, Megias D, Amira A. Deep learning for steganalysis of diverse data types: A review of methods, taxonomy, challenges and future directions. Neurocomputing. 2024 May 7;581:127528.DOI: 10.1016/j.neucom.2024.127528
20. Fu G, Peng Y, Hu J, Hao G. A Systematic Review of Deep Learning-Based Image Steganography: Paradigms, Progress, and Prospects. In2025 4th International Conference on Image Processing, Computer Vision and Machine Learning (ICICML) 2025 Nov 21 (pp. 307-312). IEEE.DOI:10.1109/ICICML67980.2025.11333424
21. Hu K, Wang M, Ma X, Chen J, Wang X, Wang X. Learning-based image steganography and watermarking: A survey. Expert Systems with Applications. 2024 Sep 1;249:123715.DOI:10.1016/j.eswa.2024.123715
22. Qiao T, Xu S, Wang S, Wu X, Liu B, Zheng N, Xu M, Pan B. Robust steganography in practical communication: a comparative study. EURASIP Journal on Image and Video Processing. 2023 Oct 31;2023(1):15.DOI:10.1186/s13640-023-00615-y
23. Hu K, Wang M, Ma X, Chen J, Wang X, Wang X. Learning-based image steganography and watermarking: A survey. Expert Systems with Applications. 2024 Mar 20;249:123715–5.DOI:10.1016/j.eswa.2024.12