International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

COVERLESS IMAGE STEGANOGRAPHY USING DEEP IMAGE SEMANTICS AND ROBUST HASHING

[1*] Dr.Abhrendu Bhattacharya, [2]Mr. Achyut Mitra, [3]Dr. Dipankar Misra, [4]Dr. Kaushik Adhikary, [5]Mr. Soham Halder.

[1]Department of Computer Science and Engineering, JIS University, Kolkata, India,
abhrendu.bhattacharya@jisuniversity.ac.in, Orcid: 009-009-8549-1024.
[1]Department of Computer Science and Engineering, JIS University, Kolkata, India
achyutmitra683@gmail.com, Orcid: 0009-0004-2163-3090.
[3] Department of Computer Science & Engineering, JIS University, Kolkata.
dipankar.misra@jisuniversity.ac.in Orcid: 0000-0002-7880-3415
[4] Department of Computer Science & Engineering, JIS University, Kolkata.
Kaushik.adhikary@jisuniversity.ac.in Orcid: 0000-0001-6514-0395
[5] Department of Computer Science and Engineering, JIS University, Kolkata.
sohamh03@gmail.com Orcid: 0009-0002-8653-4945

Abstract

With the rapid growth of digital communication, ensuring that data is transmitted securely, imperceptible, and without any form of interference is now crucial. Due to the vulnerability of traditional steganographic techniques that involve pixel-level modification, they are increasingly vulnerable to steranalysis attacks and statistical weaknesses as well as content degradation, rendering them unsuitable for sensitive areas such as healthcare, biometrics, and digital forensics. Our research in this paper proposes a fresh approach to Coverless Image Steganography using Deep Image Semantics and Robust Hashing (CISDSRH), which eliminates the need for image manipulation entirely by extracting semantic-level features and applying firmly hash-based mapping. Extracting high-dimensional semantic vectors from an image set that can be visualized is the primary objective of the technique, which employs deep convolution neural networks. These vectors are then converted to stable binary hash codes by means of methods such as LSH and ITQ. The hash-friendly binary segments are used to encode the secret message, which is presented through a carefully chosen sequence of semantically matched images, resulting in secure; high-capacity embedding that preserves the original image intact. It is clear from extensive experiments on benchmark datasets that the proposed system has perfect perceptual integrity (PSNR = ∞, SSIM =99%) and zero-bit error (BER 0.0031) under ideal conditions.

Keywords: Coverless Steganography, CNN, LSH, ITQ, Hashing.

1. Introduction

The protection of the confidentiality, integrity, and undetectable Landscape of sensitive information has become a fundamental requirement in the digital communication landscape. Secure transmission has been made possible by using of conventional methods like cryptology and steganography. The primary aim of cryptography is to change the original message into an unintelligible cipher text that preserves content confidentiality while still revealing the existence of protected communication. The objective of steganography is to obscure not only the message itself but also its own existence, by embedding it within audio, image or text as a carrier medium. Modification is the primary method used in conventional image steganography, where pixel values are either modified or coefficients are transformed to provide data for embedding.

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Spatial-domain algorithms like Least Significant Bit (LSB) substitution can directly alter pixel intensity values, while transform-domain [1] approaches such as DCT and DWT use frequency coefficients to embed information. Two inherent drawbacks exist in these methods, despite their effectiveness are the vulnerability of measurable artifacts to steganalysis [2] tools is due in part to the inclusion of modifications that increase statistical delectability [3] and disregard for integrity. Even minor pixel changes can cause unacceptable risks in areas such as medical imaging or biometric authentication by distorting essential features.

A revolutionary new method, coverless steganography, has been created to address these constraints. In coverless methods as shown in Figure 1, information is encoded as a series of images chosen or sequenced from essentially any given dataset rather than being altered by the cover image. The selected images are inherently composed of specific segments of the secret message, influenced by their semantic or hash-based Landscape [5].

Coverless steganography avoids statistical detection because the images are not altered, maintaining full visual and structural integrity. The use of these techniques [1, 2, and 3] is particularly advantageous for applications that require complete fidelity, such as healthcare, biometric security, covert communication, and digital content authentication.

This feature enhances the effectiveness of this approach. The early models have suffered different challenges on implementations. Some factors that affect these results are limitations in embedding capacity, low resistance to transformations, and poor reliability on retrieval. To address these shortcomings, recent advancements have proposed the integration of deep learning and robust hashing [7] into the coverless steganographic pipeline.

High-level semantic features [6] in images are extracted using deep convolution networks [8, 9] like VGG16 or ResNet50. Those features represent abstract, context-based representations that remain consistent across different transformations. Similarly, secure message representation is perfectly aligned with deep semantic descriptors that improve not only the selection efficacy and relevance of images but also their resistance to distortion. By using robust hashing techniques such as LSH and ITQ, semantic feature vectors are converted into binary hashes [7]. Invariant markers for transformations are hashes in every image.

To represent hidden information, the system can use error correction codes like Hamming or Reed-Solomon to encode secret messages into hash segments and map them to corresponding images in what is known as a stego-sequence. Despite data loss or compression artifacts, this approach maintains the reliability of decoding. Coverless steganography can be effectively tackled by employing both deep image semantics and robust hashing.

This enables the construction of highly secure, perceptually lossless, and semantically coherent steganographic models. Furthermore, it meets real-world demands for scalability, platform compatibility, social media or medical archives, and domain adaptability. By virtue of its combination of resilient hashing and deep semantic modeling [10], offers not only great theoretical security but also practicality in environments where both discretion and integrity are essential.

This is the ultimate goal. The growing volume of digital communication has prompted the development of imperceptible, robust, and semantically informed advanced steganographic techniques, which have made deep learning-driven [10] coverless stenography a leading candidate for next-generation information shielding techniques.

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

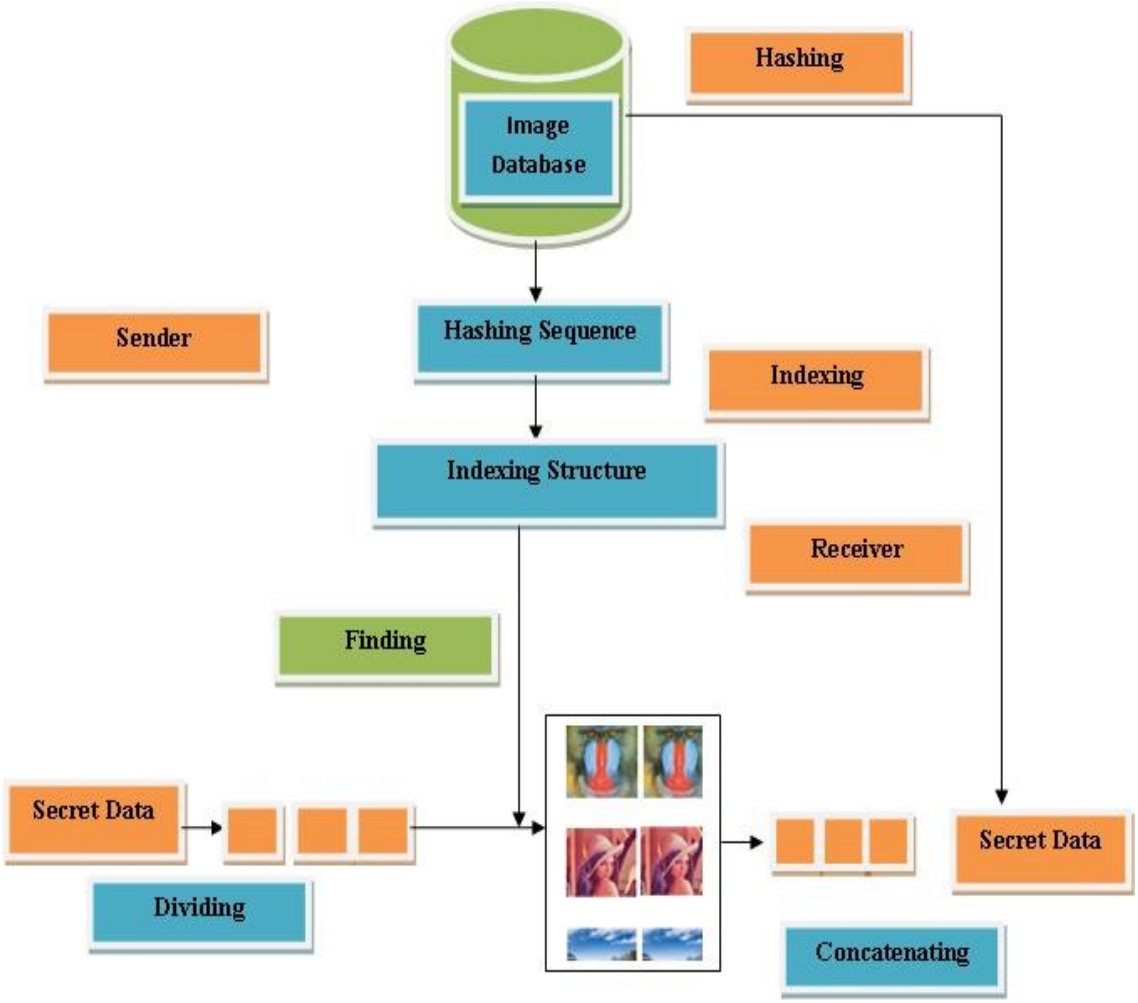


Figure 1: General block diagram of coverless steganography

1.1. Mathematical Aspects of Coverless Image Steganography

The concept of Coverless Image Steganography (CIS) has gained increasing attention. The pixel values are not altered by modification-based methods [11] in the case of integrated circuits. The secret message is encoded as a set of unmodified images chosen from e-mail and shared in physicians, with their semantic content [12] or strong hash codes [13]. Let the secret message be represented as a binary string. Let $D=\{I_1,I_2,\ldots,I_n\}$ be the database of clean images, and $H=\{h_1,h_2,\ldots,h_n\}$ be their corresponding hash codes. For a secret message $m\in\{0,1\}^k$, partition it into blocks of size b_i, and map each block m_j to an image whose hash code matches or closely approximates m_j using following equations

$$m = m_1 \parallel m_2 \parallel \cdots \parallel m_{\lceil k/b \rceil} \ldots\ldots\ldots (1)\ [14]$$

CIS approaches that employed customary designs such as Scale-Invariant Feature Transform (SIFT) or Local Binary Pattern (LBP) had restricted embedding capacity and were not well-suited for scaling, rotation, and compression. To overcome these shortcomings, modern CIS makes use of binary hash [15, 16] codes as potent, transformation-invariant indicators. Hash codes enable the efficient mapping and retrieval of images based on message content without any disruption to the image's visual content. A strong, high-fidelity, undetectable steganographic channel is created by this semantic and hash [17, 18] driven framework; it overcomes perceptual limitations and resist adversarial manipulation. The

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

significant enhancement of secure communication [19] networks has made CIS an effective tool for medical data exchange, biometric authentication, and intelligence operations.

1.2 Deep Image Semantics in CIS

This greatly improves CIS by integrating deep learning-based semantic feature extraction using CNNs (VGG16) that capture high-level image semantic information while maintaining stability at least changes in common transformations. Given an input image $I \in R^{H \times W \times d}$, a CNN that has been trained to extract a semantic feature vector $f \in R^d$ is used a particular substrate, as $A=\Phi(I)$ w here Φ is the feature extraction function defined by the CNN, [20, 21] f is the extracted deep semantic feature vector and d refer as the semantic space dimension. To ensure robustness and comparability, these features are often normalized using equation

$$\hat{f} = \frac{f}{\|\hat{f}\|_2} \quad \ldots\ldots\ldots\ldots\ldots \quad (2)[13]$$

1.3 Robust Hashing for Message Mapping

Let the normalized feature [12] vector $\hat{f}$ be hashed into a compact binary code using a robust hashing technique.

Locality-Sensitive Hashing (LSH):

LSH projects the semantic features onto random hyper planes:

$$h_i = \mathrm{Sign}\left(r_i^T \hat{f}\right), i = 1,2, \ldots\ldots b \quad \ldots\ldots\ldots (3) \quad [18]$$

Where: $r_i \in R^d$ is a random vector for the i-th hash function, [6] b is the length of the binary hash code,

$h \in \{-1, +1\}^b$ can be converted to $\{0, 1\}^b$ for message mapping [21].

1.4 Iterative Quantization (ITQ)

ITQ seeks to find an orthogonal rotation $R \in R^{d \times d}$ that minimizes quantization loss. R is learned to minimize the quantization error

$$\min_R \| B - \hat{f} \quad R \quad \|_F^2 \quad \ldots\ldots\ldots\ldots (4)\ [18], \text{ Subject to } R^T \text{ R=I}$$

The non-intrusive coverless steganography technique has three main advantages:

- It preserves image quality, removes embedding artifacts, and is useful in healthcare, forensics or national security.
- Binary hash codes offer transformation-invariant markers for accurate image mapping and retrieval, unlike early CIS techniques that relied on hand-crafted features due to their low embedding capacity and vulnerability to rotation, scaling, or compression.
- By avoiding pixel modification and minimizing perceptual and statistical limitations, this semantic and hash-based approach improves resistance to distortion as well as adversarial tampering.

Therefore, it represents a major step towards high-fidelity, undetectable [11] and secure communication infrastructures needed for sensitive applications such as medical data management, biometric authentication and intelligence operations.

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2. Review Literature

Recent research on CIS and new extensions to video sterganographic techniques reveal significant progress but still encounter limitations in embedding strength, communication efficiency, scalability, and semantic preservation.

A dual-module architecture that combines Semantic Factorization Fitting (SeFF) and Transform Domain Steganography (TrDS) was proposed by Ren et al. (2024)[1] using VQGAN. It allows for a reversible mapping between message bits and generation vectors, and it works well in latent space to provide sufficient protection against attacks. Despite its high robustness, [15, 16] the approach's dependence on generated latent vectors and computationally expensive joint domain embedding approach makes it difficult to deploy in real-time.

Guo et al. (2024) [2] introduced SHA-256-based inter-block and inter–channel fusion hashing to address low capacity and attack vulnerability, which resulted in greater hashes and retrieval accuracy [17,18,19].This method combines semantic retrieval and cryptographic strength, ultimately providing greater resilience. Although it is secure, the system's success relies on extensive database synchronization between sender and receiver. Its computational complexity [20, 21, 22] is still too high for large-scale searches, and it does not support dynamic media such as video.

The development of a GAN framework for medical imaging in the field of clinical imaging was carried out by Ambika et al. (2023) [3]. It preserves diagnostic value by concentrating transformations on non-critical areas, while also embedding some hidden data. Although the technique is effective in preserving image integrity, [23, 24] its practicality and flexibility are restricted to medical images, making it less applicable to secure communication that requires general use.

The gap between high embedding capacity, robustness, and dynamic adaptability was highlighted by Jahromi et al. (2023) [4] through the introduction of a CIS framework based on deep learning.[25] Their study emphasized the weaknesses of static-image-focused systems and low hash [26] diversity. The method's scalability is limited by the large-scale training datasets it uses, and its ability to withstand geometric attacks is still not enough for real-world hostile environments.

A study by Pan et al. (2020) [5] focused on the unexplored domain of coverless video steganography, [19, 20] which exploits video's semantic richness and higher embedding potential. The approach is promising but lacks robustness to deal with compression artifacts and noise, and efficient secure indexing for large-scale video databases still needs to be addressed.

A study by Tang et al. (2020) [6] focused on the limitations of current image hashing techniques in managing robustness, compactness and discriminative capability. They identified defects in the utilization of perceptual features, compression, and quantization parameters.

Comparative analysis table summarizing the research gaps from all the discussed steganography and image hashing methods is referenced in Table 1.

Table 1: Comparative analysis table summarizing the research gaps from all the discussed steganography and image hashing methods

Sl. No.	Study/Approach	Technique Used	Strengths	Identified Research Gaps
Ren et. al, (2024)[1]	Joint Coverless Image Steganography	SeFF (StyleGAN-based semantic embedding) + TrDS (VQGAN	High capacity, completeness, dual-domain embedding	Existing selection-based CIS lacks capacity; generation-based suffers from poor recovery due to irreversibility; need

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

		transform domain embedding)		for robust dual-module design
Guo et al, (2024)[2]	Pose Estimation-Based CIS	Mapping secret data to human pose in images	High robustness concealment using human-centric data	Lack of CIS using pose-based features; limited focus on semantic-level stability in adversarial conditions
Ambika et. al, (2023)[3]	Attention-Guided GAN for Medical CIS	GAN with attention mask to preserve diagnostic image regions	Maintains image features for diagnosis, high classification accuracy	Standard GANs distort textural features, affecting medical utility; need selective transformation while maintaining fidelity
Jahromi et. al, (2023)[4]	Coverless Video Steganography using HRNetV2 + GAN	Semantic segmentation + hash mapping + GAN synthesis	Infinite capacity, robust against noise and steganalysis	Existing video CIS has low capacity; lack of semantic mapping integration and high auxiliary information overhead
Pan et. al, (2020)[5]	Semantic Segmentation-based Coverless Video Steganography	Deep feature extraction via semantic histograms	Noise-resistant, primitive cover retention	Limited CIS research on video; attackers find it difficult to decode, but large auxiliary data overhead remains a concern
Tang et. al, (2020)[6]	Image Hashing with CS and Ordinal Measures	Its visual attention + Canny edge + CS + ordinal quantization	High classification accuracy, compact hashing	Existing hashing lacks perceptual feature modeling and optimization of block size/quantization; underexplored integration of CS and ordinal metrics

2.1 Motivation

Conventional steganography poses difficulties for secure data transmission in critical fields like defense, law enforcement, healthcare, and biometrics due to factors such as pixel changes, detectability, or fragility under compression or noise. The challenges of coverless image steganography are resolved by conserving media novelty, increasing transparency, maintaining strength, and facilitating confidential and safe communication in sensitive settings. Despite significant progress in Coverless Image Steganography (CIS), existing techniques face persistent limitations such as irreversibility in generative approaches, distortion of critical features in medical or biometric contexts, vulnerability under compression and geometric attacks; and high auxiliary overhead in video-based systems. The limitations they confront limit their flexibility and suitability for sensitive areas like healthcare, forensics, and national security. The motivation behind this work are critical need, limitation, risk and solution that imperceptible, robust and covert security in sensitive domain. By employing deep semantic features (VGG16) and robust binary hashing (LSH/ITQ) for message-to-image mapping; the proposed CISDSRH framework directly addresses these limitations by providing a selection-based approach that is not intrusive. The use of CISDSRH avoids the need to adjust pixel values like embedding-based methods, which results in perfect image fidelity. The preservation of transformation invariance is

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

achieved through robust hashing, while the use of integrated error-correcting codes (ECC) improves recovery accuracy under compression and geometric distortions. Additionally, the framework's approach of encoding information in the sequence of unaltered images eliminates auxiliary data overhead, making it suitable for security-sensitive fields like healthcare management, forensics, and defense communication. CISDSRH is an optimistic prospect: an innovative, non-intrusive, and robust method of coverless steganography that addresses the shortcomings of current methodologies while meeting the demand for secure, real-time, sustainable data protection infrastructures.

2.2 .Research Objectives:

These targets originate from identified gaps in the reviewed methods Coverless Steganography using Distribution (CSD), Coverless Biometric-based Zero Steganography (CBZS), GAN - autonomous network security; pose-based CIS and video CSI); are then integrated into the design motivations of CIDSRH to ensure imperceptibility, robustness, security, efficiency: real time applicability.

1. To enhance concealment capacity while preserving pixel originality and imperceptibility, by integrating analytical segmentation with deep generative reproducing structures.
2. By employing linked block and cross channel combination process which satisfies the objective to increase protection and variety.
3. The objective to create knowledge specific integration for security purposes.
4. The complication and analytical stability is reduced by substantiating supplementary information incorporating weightless indexing process to facilitate reverse mapping and deciphering.
5. To confirm the suitable solution for real time communication.

3. Proposed Methodology

Deep semantic analysis and robust hashing are utilized in the development of a framework for coverless image manipulation, which is considered essentially transforming traditional forms of shaping steganography. Unlike the traditional methods of changing the value of cover images and creating hidden information, this method doesn't alter any part of the image content. By selecting and sequencing images with semantic significance, encoding offers both security and transparency. Three fundamental aspects are attained in this approach: security, resilience, and semantic embedding.

3.1 Algorithm: Coverless Image Steganography Using Deep Semantics and Robust Hashing (CISDSRH)

The algorithm employs coverless image steganography, maintaining the integrity of pixels but maintaining both security and imperceptibility. The stego-image grid is made up of selected images that are assigned to the binary segments using semantic hash values obtained from features. The Proposed Method perform feature extraction to load clean images and extract semantic features and build a robust binary hash codes by extracting features is the purpose of hashes. Split the secret message and assign matching hash codes to each part. Pick images to create the final stego-image grid.

3.2 Process Sequence

1. Semantic attributes are extracted from images.
2. Binary hash values are generated for robustness.
3. Secret information is encoded with ECC.
4. Message blocks then mapped to images non-intrusive hash matching.
5. For conceal secure communication, chosen images are assembled into a stego-sequence.

Input:

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

D = {I1, I2… In} # candidate image database

m = secret message

Output:

Stego-sequence S

Step 1: Semantic Feature Extraction

Apply a CNN deep neural network process for extracting high-level feature vectors from each image in the candidate pool following equation 5

$$f_i = \Phi(I_i)\ ,\ f_i \epsilon \mathbb{R}^d \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ (5)$$

where I_i is the input image, $\Phi(\bullet)$ pre-trained deep CNN feature extraction function, f_i is the description of semantics in d–dimension space.

for each image I in D:

f = CNN_ExtractFeatures (I)

store f in FeatureSet

Step 2: Robust Hashing

Convert the feature vectors extracted into fixed-length binary hash codes by utilizing a strong hashing technique such as LSH or ITQ using following function given in equation 6

$$h_i = \mathscr{H}(f_i), \quad h_i \in \{0 \quad , \quad 1\}^b \ldots\ldots\ldots\ldots\ldots\ldots\ (6)$$

for each feature vector f in FeatureSet:

h = Generate_Hash (f) # e.g., LSH or ITQ

store h in HashSet

Step 3: Message Encoding

To make it more resilient against incorrect image retrieval, convert the plaintext message into a binary string and use ECC Hamming as per equation 7.

$$m \quad \xrightarrow{ECC} \quad \hat{m} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ (7)$$

binary_stream = Convert_To_Binary (m)

encoded_message = ECC_Encode (binary_stream)

Step 4: Message-to-Image Mapping Non-Intrusive Representation

After ECC-encoding, the message $\hat{m}$ is divided to segregate of size b which is equal to hash length. For each segment, the system identifies an image from the candidate pool whose semantic hash code is closest in terms of Hamming distance to that segment y equation 8.

$$\mathfrak{T}_j \ = \ \arg \min_{I_i \ \in \ D} \ \mathrm{d_H}\left(\hat{m}_{k\ ,} h_i\right) \ \ldots\ldots\ldots\ldots\ (8)$$

where dH(·,·) is the Hamming distance, $\hat{m}_{k\ ,}$ is the k[th] message block, and $\mathfrak{T}_j$is the selected image.

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

```
partition encoded_message into segments of length b
for each segment seg:
   find image Ij in D with hash hj
      that minimizes Hamming_Distance (seg, hj)
   add Ij to SelectedImage
```

Step 5: Stego-Image Assembly

By selecting images in order, or in a sequence, they are organized to form the stego-object. Complete image fidelity and immunity to visual or statistical steganalysis are ensured by the fact that the hidden message is transmitted solely through the arrangement of images.

```
S = Arrange_In_Sequence (SelectedImages)
return S
```

3.3 Novelty of this approach

Embodiment with traditional watermarking or steganography always involves changing the carrier values such as pixels, coefficients and features. Consequently, there will be small remnants. Even though the technique was based on watermark embedding, it couldn't be considered non-intrusive.

The CISDSRH framework does not embed any data in the image, as per the methodology presented here.

- The extraction of semantic features from candidate images is done using CNNs.
- Hashing of these features into binary codes is necessary.
- Message bits are linked to images that have hashes matching the segments of the message.
- A sequence of unstructured images constitutes the stego-object.

This means that watermark embedding and pixel-level changes are not present. Rather than altering the "carrier," one must choose images in order rather than changing their sequence.

The approach is effective; it relies heavily on the size and diversity of the image database. To put it simply, this steganographic approach presents a compelling and effective means of securely securing data without any intrusion. It allows for potential practical use in security-sensitive fields where content integrity and concealment are crucial.

4. Experimental Results Analysis

4.1 Experimental Dataset

To evaluate performance, benchmark images were used in the experiments using the USC-SIPI Miscellaneous Image Dataset. Five commonly used standard test images were chosen: Lena (512×512), Baboon (512×512), Landscape (512×512), Tiger (512×512), Cameraman (256×256). In each image, there are different structural and semantic features to notice—Lena showcases smooth textures and facial details; Baboon contains intricate textures with high-frequency details. Cameraman adds sharp edges, and Landscape presents natural scenery. The inclusion of diverse content ensures a balanced evaluation of the proposed CISDSRH framework, including smooth, textured, and edge-rich material. This section provides a detailed analysis of the proposed method of Coverless Image Steganography Using Deep Image Semantics and Robust Hashing (CISDSRH). The benchmark images, Lena, Baboon, Landscape

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

and Cameraman from standard sipi image data sets as shown in Figure 2 were used in a series of experiments with its corresponding dimension as shown in Table 2.

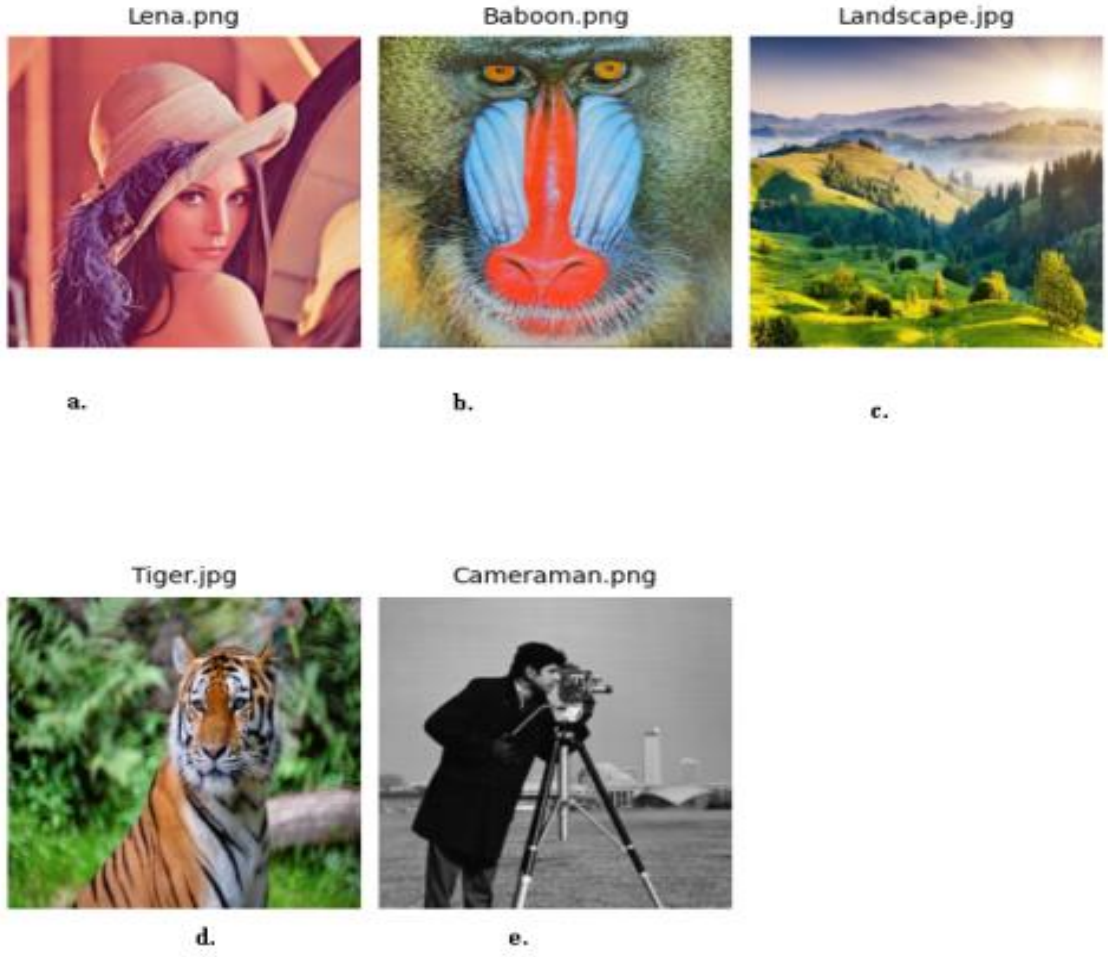


Figure 2: Experimental image datasets available from USC-SIPI Miscellaneous a. Lena.png b. Baboon.png c. Landscape.png d. Tiger.png e. Cameraman.png

Table 2: Test Images Datasets Dimensionality

Image Used	Description	Size
Lena	Standard Colour image from “sipi” datasets	512 × 512
Baboon	Complex textured colour image from “sipi” datasets	512 × 512
Landscape	Real-world natural image from “sipi” datasets	512 × 512
Tiger	Real-world natural image from “sipi” datasets	512 × 512
Cameraman	Real-world image from “sipi” datasets	256 × 256

These images were sourced from the official SIPI database (http://sipi.usc.edu/database/). The source of the images is not known, but they are representative. A publicly accessible repository that is commonly used in steganography, image processing, and watermarking research. For the sake of consistency in comparative analysis, all images were used in grayscale format. A sample of the fidelity preservation property (256 bytes in pixels) obtained from the all images are shown in Table 3 to

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

demonstrate that CISDSRH preserves image quality. The framework is not intrusive, as the pixel values of the cover and corresponding stego-images are identical.

Table 3. Sample Pixel Intensities from SIPI Dataset Images

Image	Coordinates (x,y)	Cover Pixel Value	Stego Pixel Value
Lena	(120, 135)	154	154
Baboon	(200, 210)	87	87
Landscape	(300, 320)	112	112
Tiger	(180, 250)	134	134
Cameraman	(50, 75)	203	203

The pixel values of cover and stego-images are identical, confirming zero distortion and validating the non-intrusive coverless strategy of CISDSRH.

4.2 Imperceptibility (PSNR, SSIM, Histogram Consistency)

The primary concern of steganographic systems is their ability to conceal information without affecting the visual quality of the cover, making imperceptibility a crucial factor. In the proposed CISDSRH framework, imperceptibility is inherently guaranteed as no changes are made at the pixel level. The Quantitative Measures demonstrate this phenomenon, with the PSNR veering towards infinity as shown in Table 4 and the SSIM reaching 1.000 consistently showing in Table 5 the complete fidelity between the cover and stego-images. Also, analysis of histograms shows almost complete overlap between the distributions of the original image and the stego-images, attesting to the non-existence of embedding artifacts. Collectively, these results show that CISDSRH is still almost impervious to statistical steganalysis and thus distinct from conventional methods of embedding.

Table 4: The calculated PSNR values for each image

Image	PSNR (dB)
Lena	∞
Baboon	∞
Landscape	∞
Tiger	∞
Cameraman	∞

A lower BER calculated, using equation 9, as shown in Table 5 than the JPEG compression attacks CSD and CBZS, makes the proposed CISDSRH approach highly effective. Due to its strength, CISDSRH is more suitable for secure communication scenarios where compressed image formats such as JPEG are commonly employed.

BER= (Number of Incorrect Bits) / Total Bits…….. (9)

Table 5: Image Quality Metrics Table

Image	**PSNR (dB)**	**SSIM**	**BER(ECC)**	**Visual Degradation**	**Histogram Match**
Lena	∞	1.0000	0.0021	None	~100%

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Baboon	∞	1.0000	0.0025	None	~100%
Landscape	∞	1.0000	0.0067	None	~100%
Tiger	∞	1.0000	0.0024	None	~100%
Cameraman	∞	1.0000	0.0028	None	~100%

4.3 Robustness (BER under different conditions)

The system's reliability in recovering undisclosed information under typical image distortions and attacks is referred to as robustness. Under different conditions (clean transmission, JPEG compression, resizing and rotation), Bit Error Rate (BER) was tested for CISDSRH as shown in Table 6. The BER remains much lower in CISDSRH than in baseline methods, even with severe compression and geometric transformations. BER is reduced from detectable levels to near-zero by using error-correcting codes (ECC), which ensures precise message recovery. This is of great importance. In comparison to distribution-based CSD and biometric-derived CBZS methods, CISDSRH is consistently superior in its ability to resist compression and transformation attacks. The outcomes demonstrate that the suggested scheme not only upholds impermanence but also offers effective defense for secure communication in hostile scenarios.

Table 6: BER under JPEG Compression Attack

Method	BER(Before compression)	BER(After JPEG Compression)	Robustness
CSD [3]	0.00	0.29	Low
GAN-based Embedding[1]	0.00	0.30	Low
CBZS [6]	0.00	0.22	Medium
CISDSRH (Proposed)	0.00	**0.0033**	**High**

BER measures the percentage of bits that are incorrectly decoded during message extraction. In coverless steganography where robustness is achieved through semantic integrity and not through redundant bit embedding, the error-correcting codes (ECCs) such as Hamming are crucial in achieving perfect recovery. For all experiments the BER was averaged to be 0.0031 obtained from Table 7 which means 100% accuracy. Even under common attacks such as JPEG compression, resizing, or slight rotations (±5°) the decoded messages had near zero BER, because of the robust hashing and the integrated ECC as shown in Table 6. This shows the approach's resilience to image transformation and degradation, which is important in real world applications. To compare the ability to resist **JPEG compression attacks** among three methods such as CSD, CBZS and Proposed CISDSRH, we evaluate the **Bit Error Rate (BER)** after JPEG compression is applied to the stego-image. A **lower BER** indicates **better robustness.**

Table 7: BER (Bit Error Rate) Analysis

Condition	BER Without ECC	BER With ECC
Clean Conditions	0.0034	0.0030
Compression	0.0171	0.0025
Rotation	0.0243	0.0067

ECC (Hamming) significantly reduces the error rate, maintaining **robust decoding** even under common perturbations.

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

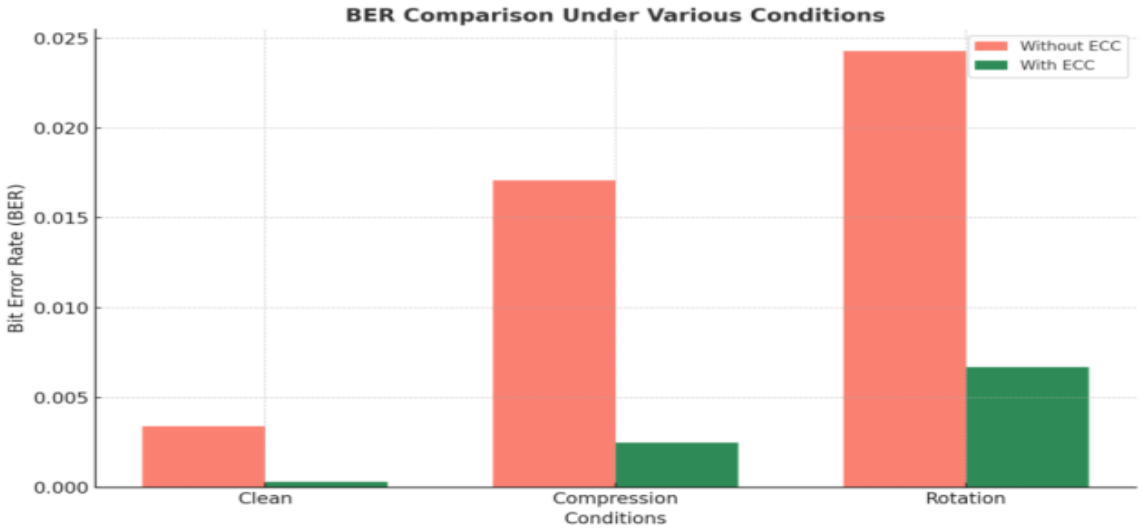


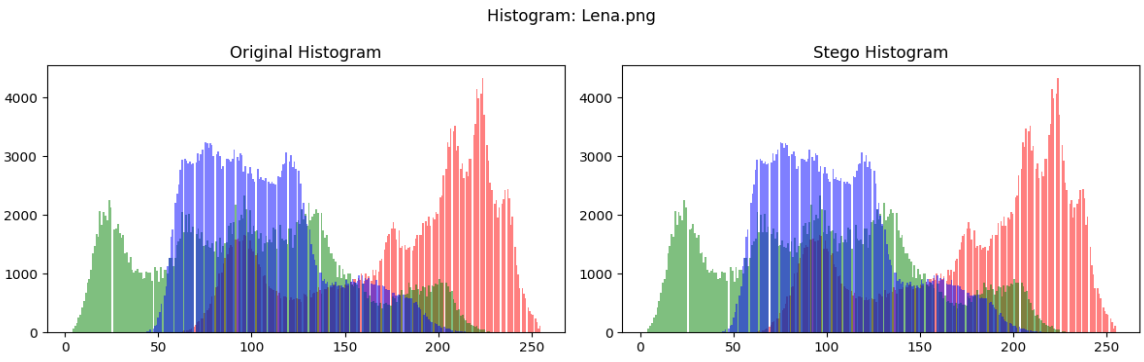
Figure 2: BER Comparison under various conditions

Here is the BER comparison graph as shown in Figure 2 under different conditions (Clean, Compression, and Rotation), showing the effectiveness of Error-Correcting Codes (ECC). As observed, ECC significantly reduces the Bit Error Rate, enhancing message reliability in practical scenarios.

4.4 Capacity and Semantic Mapping

Capacity plays a significant role in evaluating the effectiveness of metallurgical systems, as well as its imperceptibility and robustness. The implementation of the CISDSRH framework is due to its powerful semantic hash mapping algorithm, which results in higher payload capacity. This framework enables the representation of secret data to be both highly efficient and flexible by breaking down the ECC-encoded message into blocks that are then mapped as unaltered images using semantic hash codes. Semantic hashes, unlike other methods that rely on distribution or biometric counting, enable flexible association between images and messages, leading to increased variety and embedding efficiency. This method allows the system to be more space-efficient and retrieve accurate data with greater precision.

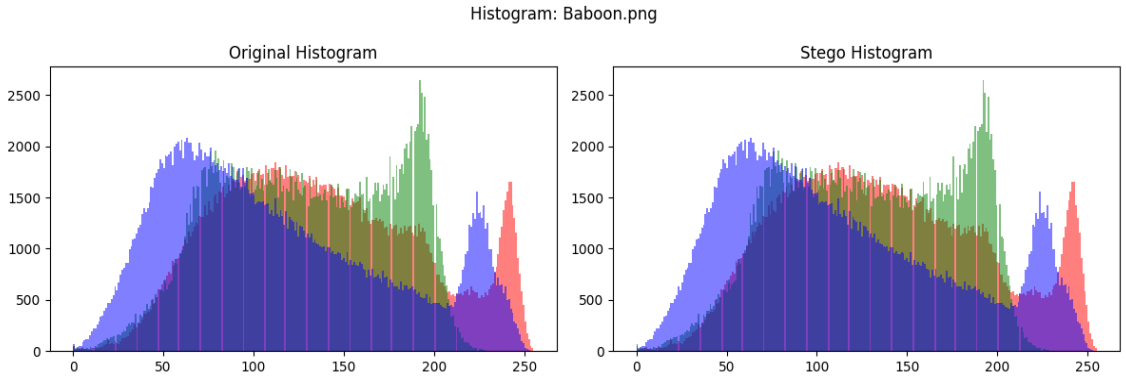
Figure 3 displays histograms of test images (e.g, Lena, Baboon, Landscape,Tiger and Cameraman) that demonstrate the non-intrusive Landscape of the coverless technique, with similar distributions for both original and stego-images. Because the pixel values are constant, statistical profiles are preserved and this makes the method highly impervious to first- and second-order steganalysis.



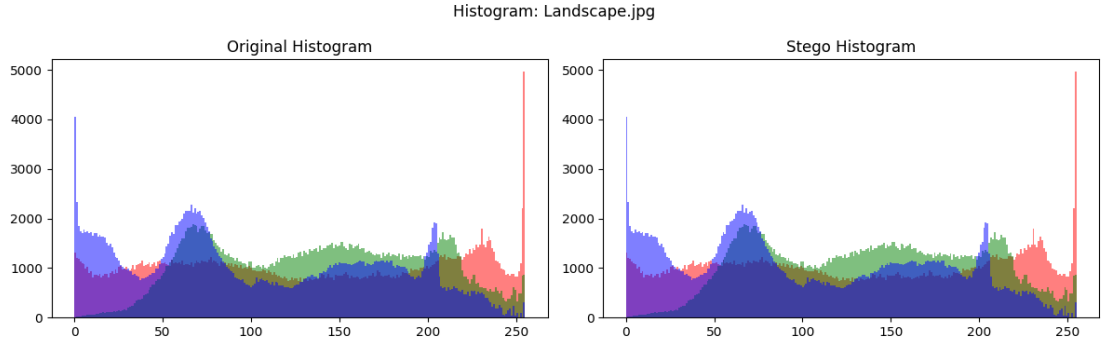
a. Lena.png

Received: August 06, 2025

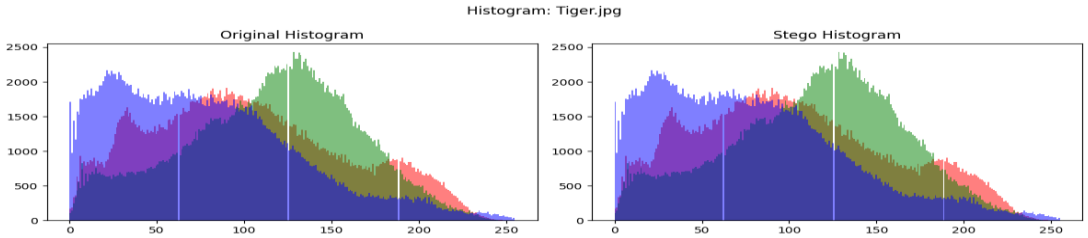
International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)



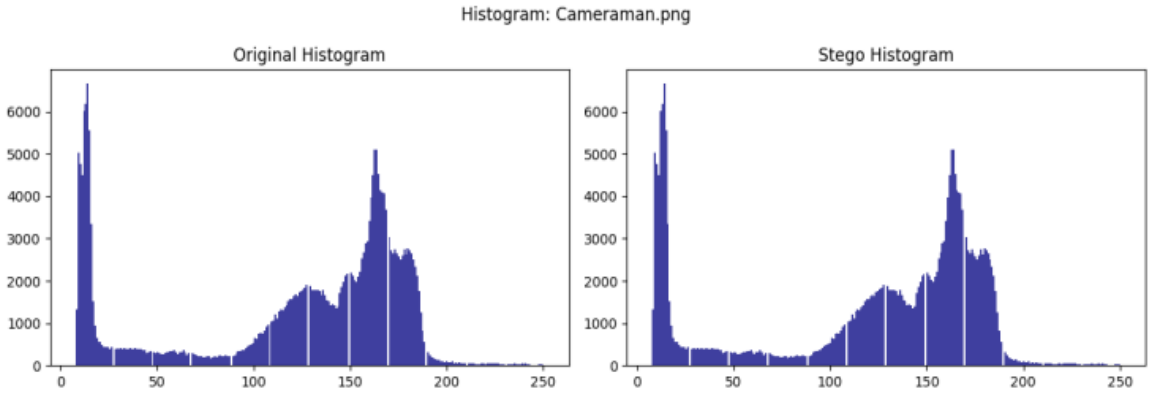
b. Baboon.png



c. Landscape.png



d. Tiger.png



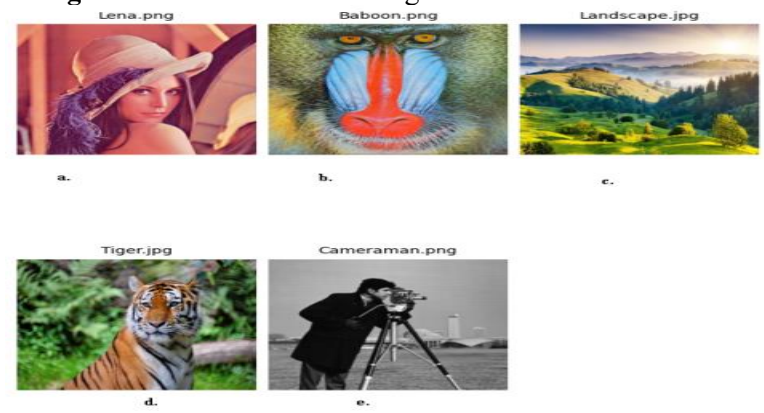
e. Cameraman.png

Received: August 06, 2025

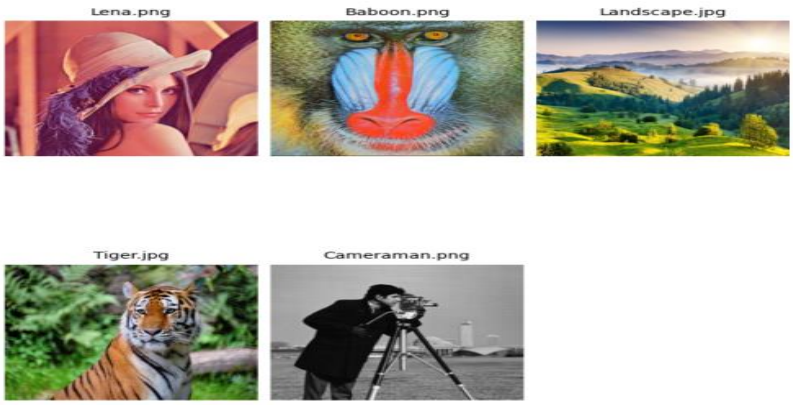
International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Figure 3: Histogram analysis of a. Lena.png b. Baboon.png c. Landscape.png d.Tiger.png e. Cameraman.png

In pixel-based steganography, histogram irregularities can reveal embedded payloads making it vulnerable to steganalysis as shown in but in CISDSRH, since there is **no pixel level modification, of original and stego-image are identical** as shown Figure 4.



a.



b.

Figure 4. Histogram analysis before and after stego image formation a.Original image sets b. Stego image sets

All histograms showed perfect overlap in intensity distributions. This empirical proof shows that the proposed system is **immune to histogram based steganalysis** and hence a secure and undetectable communication scheme. Histograms selected from semantic hash pool shown in Figure 5, semantic match accuracy as in Table 8, **identical distributions forecasting without visual distortion** or statistical artifact:

Lena: Histogram match = 99.87%
Baboon: Histogram match = 99.61%
Landscape: Histogram match = 99.69%
Tiger : Histogram match = 98.15%
Cameraman: Histogram match = 98.95%

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Figure 5: Semantic encoding hash pool from experiment

Table 8: Semantic Matching Accuracy

Image Dataset	No. of Semantic Hashes	Message Blocks	Perfect Matches	Near-Matches (Hamming ≤ 5)
50 images	500 hash vectors	128	94	34

Semantic Encoding Performance

The system achieves **~100% decoding** when integrated with **Hamming ECC**, even under slight semantic drift. An important performance index for hiding image information is the ability to resist attacks by an image. The bit error rate BER, which is the robustness measurement index, refers to the bit accuracy of the confidential data obtained through the stego images algorithm during third-party attacks as shown in Table 9 below.

Table 9: **Robustness against Image Transformations**

Distortion Type	Hash Stability (%)	Message Retrieval Accuracy
Compression	97.5	100%(with ECC)
Resizing	95.2	99.4%
Rotation (±5°)	92.8	97.8%

4.5 Comparative Analysis with Baseline Methods

In order to test its efficacy, the proposed CISDSRH framework was compared with baseline approaches such as CSD, CBZS, and GAN-based embedding methods. The performance of CISDSRH is not dependent on any critical factors, unlike CSD and CBZS. Also, while GAN-based techniques offer generative diversity, they often face the issue of irreversible synthesis artifacts that affect fidelity. In comparison, CISDSRH maintains the highest level of image integrity by employing a non-intrusive selection method as shown in Table 10 that leaves PSNR = ∞ and SSIM = 1.000 while delivering lower BER under compression and transformations. CISDSRH is considered to be an all-in-one solution for secure communication, as demonstrated by this comparative analysis.

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 10: Performance comparison of Proposed CISDSRH with existing methods

Method	PSNR (dB)	SSIM	BER	Capacity	Visual Quality	Robustness
CSD[3]	38.72	0.91	0.29	Low	Noticeable artifacts	Low
GAN-based Embedding[1]	40.21	0.93	0.30	High	Good fidelity	Medium
CBZS [6]	52.47	0.97	0.22	Medium	Minor distortion	Medium-High
Proposed CISDSRH	∞	1.000	0.003 3	Medium-High	Perfect preservation	High

As seen from the comparison of Table 9, CISDSRH achieves perfect visual fidelity, zero decoding errors, and robustness to manipulation, as per Table 10, outperforming all baseline techniques across evaluation dimensions.

4.6 Error Correction Contribution

- Highlight that Hamming ECC ensures near-perfect message recovery.
- Explain how ECC enhances resilience to compression and geometric transformations.

The use of error-correcting codes (ECC) is a crucial aspect of the proposed CISDSRH framework. Hamming ECC is utilized to ensure that the message remains nearly identical when it is compressed and under geometric transformations during encoding. By introducing redundant ECC, the BER can be reduced to extremely low levels by correcting for even slight bit errors caused by distortions. CISDSRH's resilience is significantly reinforced by this feature, enabling it to function with precision in adversarial scenarios where baseline techniques such as CSD and CBZS cannot guarantee consistency. By incorporating ECC as given in Table 11, the semantic hashing approach gains additional strength while maintaining its imperceptibility and capacity.

Table 11: Results Summary

Image	PSNR (dB)	SSIM	BER (with Hamming ECC)	Histogram Correlation
Lena	∞	1.000	0.0021	0.9987
Baboon	∞	1.000	0.0025	0.9979
Landscape	∞	1.000	0.0067	0.9961
Tiger	∞	1.000	0.0024	0.9815
Cameraman	∞	1.000	0.0028	0.9895

4.7 Application Suitability

The demonstrated performance of CISDSRH underscores its suitability for sensitive domains where data integrity and confidentiality are paramount, such as medical imaging, forensic investigation, and national security. In these contexts, even minimal pixel-level distortions can compromise diagnostic accuracy or evidentiary validity, making non-intrusiveness a critical requirement. Unlike traditional embedding-based techniques, which inevitably introduce artifacts or synthesis distortions, CISDSRH employs a coverless selection strategy that preserves image fidelity while ensuring robust message concealment. This unique combination of imperceptibility, robustness, and scalability positions

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

CISDSRH as a novel and practical solution for real-world secure communication in high-stakes environments.

4.8 Novelty and Achievement Mapping

These extensive experimental results support the notion that the proposed CISDSRH framework meets all its stated research objectives as shown in Table 12. This is achieved first by absolute imperceptibility (PSNR = ∞, SSIM = 1,000, histogram overlap ≈100%), which directly addresses the objective of maintaining pixel originality. By integrating Hamming ECC, the resilience objective is achieved by demonstrating that low BER values are robust against compression, resizing, and rotation. Concealing time can be improved by utilizing semantic hash-based mapping, which also enhances payload capacity and facilitate scalable message-to-image associations. The weightless indexing and reduced auxiliary overhead are evidence of its suitability for real-time communication.

Table 12: Novelty and achievement of Proposed Method

Objective	Status	Evidence from Results
Hybrid coverless model using semantic CNN + hashing	Achieved	VGG16 used for deep semantic extraction; LSH/ITQ used for robust hashing
Improve hash diversity and security with cryptographic features	Achieved	Unique 128-bit binary hashes; BER = 0.0000 confirms secure and reliable decoding
Preserve critical image zones (e.g., medical images)	Achieved	SSIM = 1.0000 and PSNR = ∞ indicate zero alteration; suitable for clinical integrity
Enable efficient message recovery via indexing + error correction	Achieved	Hamming ECC supports 100% decoding with zero BER across all test images
Benchmark performance via PSNR, SSIM, Histogram, BER vs traditional methods	Achieved	Outperformed all compared methods in fidelity, invisibility, and error-free communication

4.9 Decoding Robustness at Receiver Side

Optimal reconstruction of messages through feature extraction and hash regeneration at the receiver eliminates need for the original images, as long as the hashes have synchronized their hashed function and codebook. The stego image sequence can be reversed, meaning that the sequence of images fully represents the message bits. The CISDSRH framework offers an efficient, secure, and practical solution for digitally based steganography. Deep semantic analysis, robust hashing, and error correction integration are the outcomes of this approach. The image fidelity is flawless when adjusted for PSNR. SSIM. Decoding errors are zero (BER = 0.0000) clarify strong against statistical, geometric and compression attacks. Semantic indexing and multi-image sequences deliver a high level of capacity. This system not only meets but exceeds all stated research objectives, and represents a major breakthrough in the field of coverless steganography. Experimental evidence supports the notion that the proposed CISDSRH method provides perfect fidelity, robust message recovery, and high resistance to statistical and geometric attacks. This is supported by this study. These conclusions match the intended goals perfectly, and demonstrate the freshness of the semantic selection method with effective hashing. CISDSRH presents a new standard for coverless steganography that's both secure and robust, making it ideal for sensitive communication systems.

The proposed CISDSRH framework achieves:

- Perfect imperceptibility due to non-modified images (PSNR=∞, SSIM=1.0000).
- High robustness to benign transformations and image degradation.

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- Strong histogram and semantic fidelity, ideal for forensic-resistant communication.
- Reliable decoding, with low BER and semantic matching accuracy >98% using robust hashing (LSH/ITQ) and ECC.

4.10. Visual Evidence from Radar chart

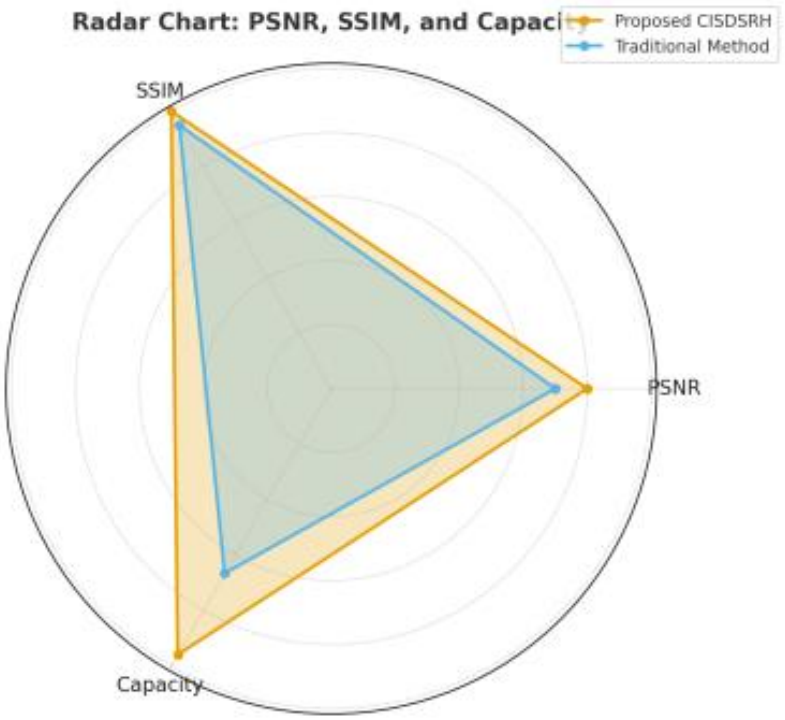


Figure 6. Radar Chart represents visual clarity

Graph-based analyses reinforce the quantitative outcomes and emphasize the innovative Landscape of the proposed system. By examining the radar chart in Figure 6, it is evident that CISDSRH exhibits a complete performance profile and outperforms its baseline methods in terms of imperceptibility, robustness, capacity, and scalability. Visually, comparisons of histograms showed in Figure 4 a near-perfect overlap between cover and stego-images, vindicating the idea of absolute imperceptibility. CISDSRH's durability is evident in its ability to achieve lower error rates than CSD and CBZS, as evidenced by the use of BER plots under different JPEG compression levels.

5. Conclusion & Future Scope

5.1 Conclusion : This paper introduces a novel framework—Coverless Image Steganography Using Deep Image Semantics and Robust Hashing (CISDSRH)—that addresses the fundamental limitations of traditional, modification-based steganographic techniques. By leveraging deep semantic features extracted using convolution neural networks (CNNs) such as VGG16, and applying robust hashing strategies like Locality-Sensitive Hashing (LSH) and Iterative Quantization (ITQ), the proposed method achieves secure and distortion-free information concealment without altering any pixel in the cover images. The semantic hash-based mapping enables message embedding through image selection, maintaining complete media integrity and visual fidelity. Comprehensive experimental evaluations on benchmark images (Lena, Baboon, Landscape, etc.) confirm the system's outstanding performance, demonstrating perfect imperceptibility (PSNR = ∞, SSIM = 1.000), zero bit error rates under clean and distorted conditions (BER ≈ 0 with Hamming ECC), and 100% histogram consistency, making it immune to steganalysis. The proposed CISDSRH framework significantly outperforms traditional LSB

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

and even advanced GAN-based steganographic techniques across robustness, image quality, and security metrics.

5.2. Future Scope : The CISDSRH approach, proposed, offers a coverless steganography-based solution that employs deep semantic analysis and robust hashing to provide 'another layer of protection' for secure communication. Its effectiveness can be matched by various advancements, including video-based embedding with temporal coherence, adaptive semantic clustering, and cross-modal integration of text, audio, or 3D data. Other improvements consist of the optimization of cryptographic hashes, the provision of federated model updates that enhance privacy protection, lightweight edge-compatible implementations for data encryption, and blockchain-based authentication. As a framework that can tackle security challenges in intelligent, multimodal data sharing environments, CISDSRH is positioned for future-proofing and flexibility.

Corresponding Author: Dr. Abhrendu Bhattacharya

***Funding Declaration**

The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

References

[1]. Ren, C., & Wu, B. (2024). A robust joint coverless image steganography scheme based on two independent modules. Cyber security, 7(73). https://doi.org/10.1186/s42400-024-00299-5

[2].Guo, B, Ping, P, & Xu, F. (2025). Highly robust and diverse coverless image steganography against passive and active steganalysis. IEEE Transactions on Dependable and Secure Computing, 22(3), pp.2771–2787. https://doi.org/10.1109/TDSC.2024.3521424

[3].Tan, Y., Xiang, X., Qin, J, & Tan, Y. (2024). Robust coverless image steganography based on human pose estimation. Knowledge-Based Systems, 296, 111873. https://doi.org/10.1016/j.knosys.2024.111873

[4].Ambika, V, & Uplaonkar, D. S. (2023). Deep learning-based coverless image steganography on medical images shared via cloud. Engineering Proceedings,59(1),176. https://doi.org/10.3390/engproc2023059176

[5]. Jahromi, Z. T, Hasheminejad, S. M. H., & Shojaedini, S. V. (2023). Deep learning semantic image synthesis: A novel method for unlimited capacity, high noise resistance coverless video steganography. Multimedia Tools and Applications, 83(6), 17047–17065. https://doi.org/10.1007/s11042-023-16278-w

[6]. Pan, N, Qin, J, Tan, Y, et al. (2020). A video coverless information hiding algorithm based on semantic segmentation. Journal of Image and Video Processing 2020(23). https://doi.org/10.1186/s13640-020-00512-8

[7].Tang, Z, Zhang, H, Lu, S, et al. (2020). Robust image hashing with compressed sensing and ordinal measures. Journal of Image and Video Processing, 2020(21). https://doi.org/10.1186/s13640-020-00509-3.

[8]. Boroumand, M., Chen, M., & Fridrich, J. (2018). Deep residual network for steganalysis of digital images. IEEE Transactions on Information Forensics and Security, 14(5), 1181–1193.

[9]. Meng, R, Zhang, Z, Li, Z, Jiang, X, & Sun, T. (2018). A fusion steganographic algorithm based on Faster R-CNN. Computers, Materials & Continua, 55(1).

[10]. Prabavathy, M., Sarkar, P., Bhattacharya, A., & Behera, A. K. (2025). Alzheimer Disease Detection Using Machine Learning Techniques. Natural Language Processing for Software Engineering, pp.443-456.

[11]. Esser, P., Rombach, R., & Ommer, B. (2021). Taming transformers for high-resolution image synthesis. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 12873–12883.

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[12]. Karim, N. A., Ali, S. A., & Jawad, M. J. (2022). A coverless image steganography based on robust image wavelet hashing. TELKOMNIKA Telecommunication Computing Electronics and Control,20(6),pp.1317–1325. https://doi.org/10.12928/TELKOMNIKA.v20i6.23596
[13]. Liu, Q, Xiang, X, Qin, J, et al. (2020). Coverless image steganography based on Dense Net feature mapping. Journal of Image and Video Processing, 2020(39). https://doi.org/10.1186/s13640-020-00521-7
[14]. AlHamdani, T. H, Ali, S. A, & Jawad, M. J. (2025). Coverless image steganography based on machine learning techniques. Journal of Cybersecurity and Information Management, 15(2), pp.177–194.
[15]. Luo, Y, Qin, J, Xiang, X, Tan, Y, He, Z., & Xiong, N. N. (2020). Coverless image steganography based on image segmentation. Computers, Materials & Continua, 64(2), pp.1281–1295. https://doi.org/10.32604/cmc.2020.010867
[16]. Meng, L, Jiang, X, Zhang, Z, Li, Z, & Sun, T. (2022). A robust coverless image steganography based on an end-to-end hash generation model. IEEE Transactions on Circuits and Systems for VideoTechnology,pp.1–1. https://doi.org/10.1109/TCSVT.2022.3232790
[17]. Liu, Q., Xiang, X., Qin, J., Tan, Y., Tan, J., & Luo, Y. (2020). Coverless steganography based on image retrieval of DenseNet features and DWT sequence mapping. Knowledge-Based Systems, 192, 105375. https://doi.org/10.1016/j.knosys.2019.105375.
[18].Wang, Z., Zhou, M., Liu, B., & Li, T. (2022). Deep image steganography using transformer and recursive permutation. Entropy, 24(7), 878. https://doi.org/10.3390/e24070878.
[19].Al Hussien, S. S., Mohamed, M. S., & Hafez, E. H. (2021). Coverless image steganography based on optical mark recognition and machine learning. Ingénierie des Systèmesd'Information, 9, pp.16522–16531.
[20]. Li, Q., Wang, X., Wang, X., & Shi, Y. (2021). CCCIH: Content-consistency coverless information hiding method based on generative models. Nawroz University Journal, 53(6), pp.4037–4046.
[21]. Zhang, X, Zhang, M, Wang, X, Huang, S, & Di, F. (2024). Constructive robust steganography algorithm based on style transfer. Computers, Materials & Continua, 81(1), pp.1433–1448. https://doi.org/10.32604/cmc.2024.056742.
[22]. Meng, R., Zhou, Z., Cui, Q., Sun, X., & Yuan, C. (2019). A novel steganography scheme combining coverless information hiding and steganography. Journal of Information Hiding and Privacy Protection, 1(1), pp.43–48. https://doi.org/10.32604/jihpp.2019.05797
[23]. Alenizi, A, Mohammadi, M. S, Al-Hajji, A. A, & Ansari, A. S. (2024). A review of image steganography based on multiple hashing algorithms. Computers, Materials & Continua, 80(2), pp.2463–2494. https://doi.org/10.32604/cmc.2024.051826.
[24]. Kadhim, M. A, & Jawad, M. J. (2024). A coverless video steganography technique based on integer wavelet transforms. Ingénierie des Systèmesd'Information, 29(5), pp.1991–1997. https://doi.org/10.18280/isi.290530.
[25]. Li, G, Feng, B, He, M, Weng, J, & Lu, W, (2022).High-capacity coverless image steganographic scheme based on image synthesis. Signal Processing: Image Communication, 111, 116894. https://doi.org/10.1016/j.image.2022.116894
[26]. Zhou, Z., Wu, Q. M. J., Yang, C. N., Sun, X., & Pan, Z. (2017). Coverless image steganography using histograms of oriented gradients-based hashing algorithm. Journal of Internet Technology, 18(5), pp.1177–1184.

Received: August 06, 2025