Archives available at journals.mriindia.com
International Journal on Advanced Computer Theory and Engineering
ISSN: 2319 - 2526
Volume 15 Issue 01s, 2026

Enhanced Secure Digital Data Embedding and Extracting Using Advanced Crypto-Stego Mechanisms

[1]Chetan D. Chaudhari , [2]Monali Y. Khachane
[1]Assistant Professor in Computer Science, KPG ACS College, Igatpuri, Dist. Nashik, India
[2] Assistant Professor in Computer Science, Dr.Annasaheb G.D. Bendale, Mahila Mahavidhyalaya, Jalgaon, India
Email: [1]chetanmcs7@gmail.com, [2]monalikhachane@gmail.com

Peer Review Information

Submission: 08 Dec 2025

Revision: 25 Dec 2025

Acceptance: 10 Jan 2026

Keywords

NTRU, GAN, CNN, Arnold Transform, Steganography, Cryptography

Abstract

In this proposed study, a new hybrid approach is employed, which ensures the safe embedding as well as retrieval of digital data by using modern cryptography techniques along with steganographic techniques. By combining NTRU encryption, which provides quantum-resistant security, with the Arnold Transform, which improves data scrambling, the method significantly increases the stability of encrypted data. The transmission and storage of data are enhanced using Generative Adversarial Networks (GAN)-based compression without carrier file integrity being compromised. Efficient embedding and robust resistance to steganalysis attacks are promised by the Convolutional Neural Networks (CNN)-based data hiding method..

Introduction

The continuously growing rate of data transfer using modern technologies has revolutionized digital communication [1]. Text, images, audio, and video transmission over the Internet have become an integral part of daily life [2]. With the increase in the usage of the Internet, ensuring the security and privacy of digital information has become a serious issue [3,4]. Cyber-attacks such as data stealing, unauthorized information access, and content modification have grown with the simplicity of extremely advanced hacking software. Therefore, researchers have been creating extremely advanced security solutions to give secure and guarded data transfer [5].

Cryptography is among the most fundamental methods that are used to protect confidential information by transforming it into ciphertext using encryption methods [6,7]. Traditional encryption protocols, like the Prominent encryption techniques such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Elliptic Curve Cryptography (ECC), are widely used in secure communication systems. Algorithms rely on secret keys for encrypting and decrypting data, and it becomes difficult for unauthorized access [8,9]. However, these techniques are constrained by the length of the key, vulnerability to brute-force attacks, and inefficiency in handling large data sets. Moreover, encrypted data, though secure, can attract the interest of eavesdroppers and thereby become a cryptanalysis target [10]. This is why data hiding has been extensively employed by researchers to conceal the presence of sensitive information, making it imperceptible to potential intruders [11-13].

Data hiding methods, including watermarking, steganography, etc., are a booming security

solution in secure communication [14]. As opposed to the encryption process, steganography protects the confidentiality of secret data in such a way that its very existence remains unexposed, thereby slowing down the risks of data exposure [19]. As soon as the eavesdropper is aware of the steganographic algorithm, the embedded data can be retrieved, thereby reducing security. Hence, in order to provide better security, there is a need to preprocess data using cryptography methods in the data hiding process [24]. Many researchers have introduced the concept of crypto-stego, a combination of steganographic methods and cryptography, in order to provide a multi-level security solution in data security [26]. This crypto-stego solution involves encrypting data, followed by hiding data in a cover file, in a manner that the data remains both secure and confidential. It is a security solution that also decreases the chances of exposure of data to an intruder. Recently, advancements in Deep Learning concepts have elevated the concept of crypto-stego to provide a more efficient data embedding solution [27,28]. DL techniques such as CNNs are applied to intelligent steganography. In contrast, GANs are applied to generate stego images that are practically indistinguishable from authentic images, hence making the detection even more challenging [29,30].

The rise of cyberattacks presents substantial challenges for safe data transmission. Despite being able to encrypt effectively, traditional cryptography does not conceal the existence of data being encrypted and, therefore, is an open target for malicious attackers. Steganography cannot originally embed, damage carriers, or be sensitive to advanced steganalysis. The Current hybrid crypto-stego techniques are limited by high computational complexity and a lack of standardization. Such limits demand an integrated solution that leverages the power of both steganography and cryptography to eliminate their weaknesses and produce total security for sensitive digital information.

Therefore, in overcoming these challenges, the hybrid proposed model in this research is an efficient crypto-stego hybrid model that will address the issues being faced in secure data transmission. The proposed model is a combination of NTRU encryption, the Arnold Transform scramble and GAN compression with CNN steganographic techniques. The proposed model combines the abilities and benefits of both steganography and cryptography that play vital roles in the concealment and security of sensitive data in the current digital world, which is being exposed to various risks and attacks.

The primary goals and objectives of the proposed model are:

- To devise and develop an effective hybrid crypto-stego system that combines sophisticated crypto and steganographic processes and data-hiding networks for improving the security and confidentiality aspects involved in digital data transfer.
- To determine whether NTRU encryption methods provide quantum resistance to ensure the security and protection of digital data integrity and confidentiality while in transit.
- The goal of employing an effective data scrambling technique based on the Arnold Transform is to enhance the data embedded in the medical images.
- The estimation and comparison of the effectiveness of the developed hybrid crypto-steganographic method with other cryptographic, stenographic, and traditional approaches.

The rest of the paper is outlined below: Section 2 gives a literature study, while Section 3 mentions the methodology used in this study. Section 4 discussed the implemented results, and finally, in Section 5, the findings are summarized.

Literature of review

The security of data when embedding and extracting through cyberspace has emerged as a necessity because of the steady increase in cyber-attacks. **Sanjalawe et al. (2025) [31]** proposed a multi-level steganographic scheme combining Huffman coding, LSB embedding, and a deep learning encoder and decoder to enhance security and perceptual concealment. The scheme registered a Peak Signal to Noise Ratio (PSNR) value of 57.5 dB when tested under Gaussian noise. In the same year, **Ramadhan et al. (2025) [32]** proposed a steganographic scheme based on image segmentation to optimize data embedding via Huffman coding, maintaining high values of PSNR from 51.159 dB to 44.316 dB along with a constant Structural Similarity Index Measure of more than 0.98. Subsequently, **Priya et al. (2024) [33]** proposed a scheme that integrated deep learning networks and ECC, restoring images up to 93% and decreasing the security processing time complexity by 78%. Additionally, **Huo et al. (2024) [34]** proposed a Chaotic mapping-enhanced image Steganography network (CHASE), which combined chaotic mapping and GANs with high-capacity steganographic techniques. The proposed technique resisted detection by a higher margin of 8% compared to DeepMIH, as well as 7.9% compared to Zhu-Net.

In a similar approach, **Mawla & Khafaji (2023) [35]** employed protein bases in both encryption and steganographic techniques, measuring an entropic rate of 7.99941 with a capacity of 2.666 bits. Taking this approach further, **Kosuru et al. (2023) [36]** proposed a Multiple Histogram Coding (MHC) scheme, resulting in an appropriate PSNR of 36.76 with a Quality Index (QI) of 0.9977.

Improving the security mechanism, **Rathore et al. (2022) [37]** developed the Efficient Algorithm for Secure Transmission (EAST) technique for IoV, providing an avalanche strength measure of 58.81% and a PSNR value of 78.58 dB. Later, **Awadh et al. (2022) [38]** used image steganography with DWT and AES encryption and got the PSNR value as 47.8 dB with an SSIM value of 0.92. Further, moving on the same line, **Mahmoud et al. (2022) [39]** presented LSB-BMSE audio steganography and provided an average SNR value of 99.98 dB. Earlier, the need for image compression and security was fulfilled by combining RSA encryption, Huffman encoding, and steganography using DWT by **Wahab et al. (2021) [40]**. In the same context, **Rakshit et al. (2021) [41]** presented an intensity-based image steganography technique along with audio steganography. They provided an efficient way to hide image data in stereo audio files effectively. This gave an effective PSNR value of 48.08 dB, which made possible the secure and lossless recovery of hidden images with no distortion to the cover audio files. It was observed that all the above studies emphasized the development of secure data embedding and made way for improved robustness, imperceptibility, and efficiency in cryptographic and steganographic solutions.

Research Gaps

- Most existing approaches rely on conventional cryptographic techniques, which are vulnerable to quantum attacks [33].
- Many existing steganographic techniques focus only on embedding methods without employing strong scrambling mechanisms to further obfuscate data [40].
- Prior works either focus on majorly on cryptography or steganography separately, leading to potential weaknesses in security [32,33].

Research Methodology

The methodology section presents an in-depth description of the datasets and techniques employed in the proposed study, along with the proposed work for secured digital data embedding and extraction.

1. Dataset Description

This section has provided a detailed discussion of the dataset employed in the study.

a) DIV2K

High-quality images with a resolution of 2K are included in the DIV2K dataset, as shown in Fig. 1. These images were created to perform activities such as restoration of images, enhancement, and increased resolution. It includes a total of a thousand images, with 300 being reserved for testing purposes and 700 for training purposes. During research, GAN is trained in image compression by using the DIV2K dataset [42]. During the procedure of steganography, there is an important need to maintain picture qualitybecause high-resolution images lead the network to obtain precise details about numerous textures and colors.

Fig 1: Sample pictures from the DIV2K dataset

b) Common Objects in Context (COCO)

The COCO dataset is a large database for tasks including segmentation, object detection, and captioning. The dataset encompasses in excess of 330,000 images, as seen in Fig. 2, of which 2 lakh are object-labeled with a total of 1.5 million object instances [43]. The instances cover 80 object categories.

Fig 2: Sample images from the COCO dataset

It is used for training the CNN hidden network. The different array of scenes and objects included in COCO enhances the network's resilience, allowing it to efficiently integrate hidden pictures into a wide range of cover images.

2. Technique used

The following section presents the techniques used in the proposed study:

a) GAN

GANs have significantly transformed several domains, such as steganography, by using a competitive architecture consisting of two neural networks: the generator and the discriminator, as seen in Fig. 3. GANs have the potential to greatly improve security and efficiency in image steganography by using image compression techniques [44]. The generator employs compression techniques to transform the secret data into a representation with fewer dimensions while preserving crucial characteristics and minimizing its size.

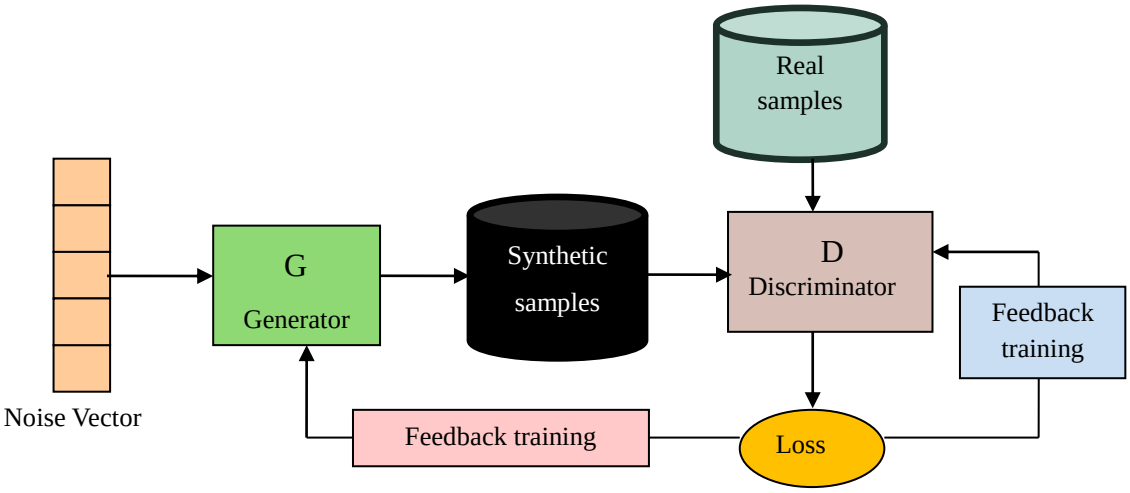

Fig 3: Generative Adversarial Networks [45]

The discriminator guarantees that the compressed data maintains an identical appearance to the original data. The compressed confidential data is then included in the cover image. When extracted, the GAN decompresses the data, guaranteeing the minimum loss of information and a strong defense against cyberattacks. The goal function for training a GAN is defined as [46] :

$$\min_G \max_D V(D,G) = E_{x\sim Pdata}(x)[\log D(x)] + E_{z\sim Pz}(z)[\log(1 - D(G(Z)))] \quad (1)$$

Where x is the original sample, z is the arbitrary noise input to the generator, P_{data} and $P_z(z)$ are the distributions of x and z, respectively.

b) CNN

CNNs are used in image steganography to hide and retrieve secret data [47]. The CNN employs convolutional layers to extract features from both the cover photos and secret data, which can be given by :

$$y = f(W.x + b) \quad (2)$$

The feature map is denoted by y, the filter by W, the input picture by x, and the bias by b. The covert picture incorporates the hidden data attributes by employing numerous convolutional and pooling layers, as shown in Fig. 4. This process guarantees minimum distortion. Subsequently, CNN employs layers that have been provided to detect hidden information to identify embedded features.

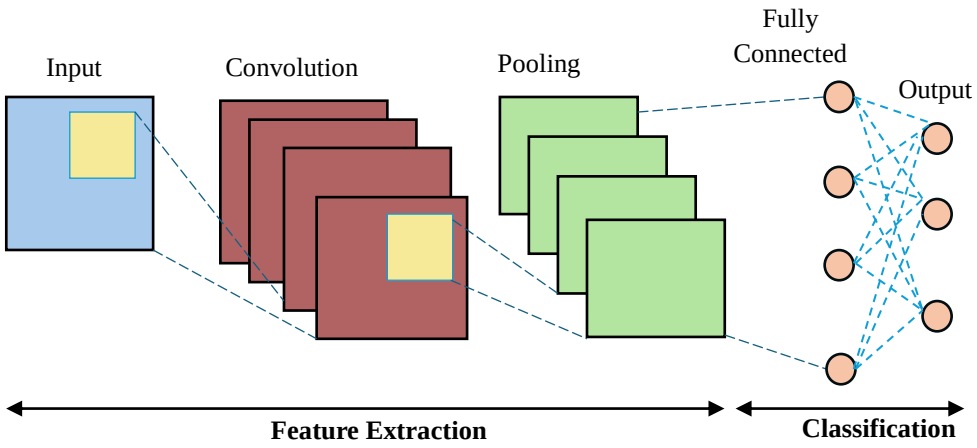

Fig 4: Convolutional Neural Network [48]

The deconvolutional layers are used to extract the hidden data from the features. This process is described by the equation:

$$x' = f(W'.y + b') \quad (3)$$

The reconstructed data is denoted as x′, whereas the weights and biases of the deconvolutional layers are represented by W′ and b′.

c) Arnold Transform

Image steganography enhances data security by embedding secret information within image files, making it difficult to detect and target by cyberattacks. One effective method to improve this technique is the Arnold transformation, which restores the pixel matrix of a digital image, effectively scrambling the image to enhance security. It is a 2-dimensional process defined as follows [49]:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \quad (4)$$

The variables x and y indicate the starting pixel positions, N defines the image dimension, and x′ y′ correspond to the new coordinates. The application of the Arnold transformation in image steganography decreases the likelihood of cyber attacks and reduces information loss while maintaining the secret concealed message as secure and unaltered.

d) NTRU encryption

NTRU is an efficient public cryptosystem offering maximum security. The process of embedding within steganography secures data in a way that hidden information is not vulnerable to attacks of cryptography [51]. An encrypted message that is required to be concealed is encoded using NTRU, which gives a secure format. The encryption process is defined by the equation:

$$e = f * h + m(modq) \quad (5)$$

Where e is the ciphertext, h and f are private and public keys, m is the plaintext, and q is a modulus.

The CNN is used to incorporate hidden messages into the cover image. The embedding strategy guarantees the safe integration of the hidden data. Then, during the extraction phase, the hidden message is recovered from NTRU, represented by the equation:

$$m = e * g^{-1}(modp) \quad (6)$$

Where g is another hidden key that is a derivation of f and h, and p is a modulus, but smaller in size. The above steganographic technique guarantees greater security and effectiveness through the application of a combination of CNNs and NTRU cryptography. The technique aims to preserve the integrity of the cover image and protect the embedded data.

Proposed Methodology

Thecryptographic, steganographic, and hybrid models designed in this study are presented in this section.

1. Cryptographic model

The model presented in this part for the protection of data utilizes the NTRU encryption scheme that is resistant to quantum attacks. First, the system is initialized, and then secret data that is to be transmitted securely is fed into the system. This secret information is then encrypted by utilizing the NTRU encryption algorithm, resulting in the encrypted data, also known as cipher text, as shown in Fig. 5. Then, the cipher text is sent to the recipient over a communication channel. The recipient, on receiving such encrypted data, uses the NTRU decryption algorithm to decrypt it and get back the original secret information.

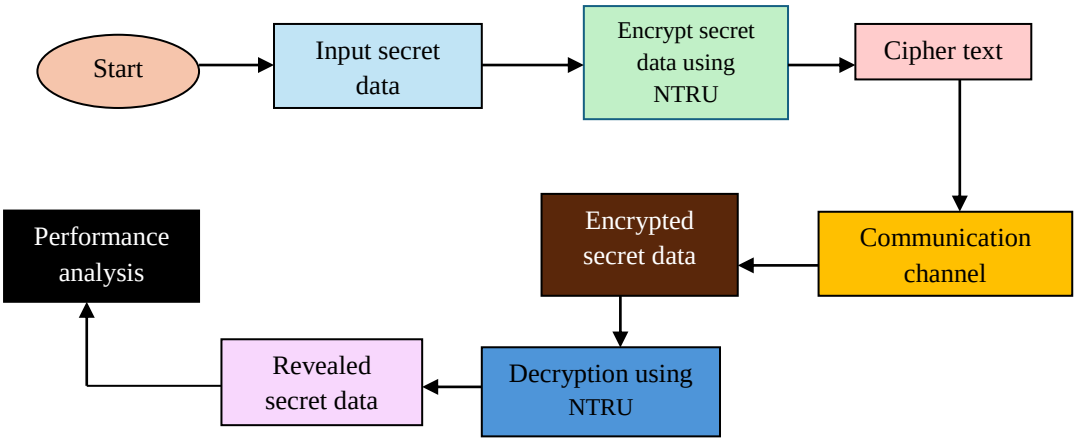

Fig 5: Proposed cryptographic framework

Algorithm 1: Cryptographic Model

Step 1: Start
Initialize the process.
Step 2: Input Secret Data
Let S be the secret data that needs to be securely transmitted.
Step 3: Encrypt Secret Data Using NTRU
Apply the NTRU encryption algorithm to S to generate the encrypted data E.
E = NTRU_Encrypt(S)
Step 4: Generate Cipher Text
The result of the encryption process E is the ciphertext.
Step 5: Transmit Over the Communication Channel
Send the cipher text E over the communication channel to the intended recipient.
Step 6: Decrypt Using NTRU
Upon receiving E, the recipient uses the NTRU decryption algorithm to retrieve the original secret data S.
S' = NTRU_Decrypt(E)
Step 7: Revealed Secret Data
The decrypted data S' should match the original secret data S.
Step 8: Performance Analysis
Analyze the performance of the encryption and decryption processes using standard performance evaluation metrics.

End

2. Steganography model

The proposed steganographic model guarantees that secret information can be embedded or extracted inside a cover image safely by using advanced steganographic techniques for improved security and robustness. The first step is to find the right cover image in which the secret data would be hidden. Secret data is then given in the system to be securely embedded into the cover image. Before being embedded, the secret data is subjected to Arnold scrambling, a process that transforms it into a seemingly random and unrecognizable form, thus enhancing its security. Then, the secret data is embedded using a steganography encoder to insert this scrambled secret data into the cover image, resulting in visually similar images. Output from this encoding process is referred to as a stego image, which contains secret data, as shown in Fig. 6.

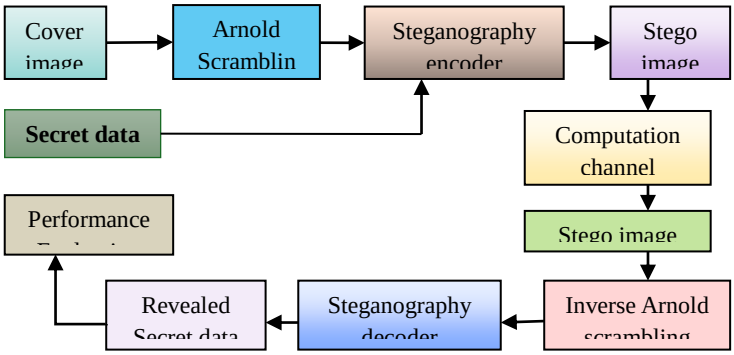

Fig 6: Proposed Steganographic framework

Algorithm 2: Steganographic Model

Step 1: **Start**
Initialize the process.
Step 2: **Select Cover Image and Input Secret Data**
Let C be the cover image.
Let S be the secret data to be embedded.
Step 3: **Apply Arnold Scrambling**
Scramble the secret data S using Arnold scrambling to get S_scrambled.
S_scrambled = Arnold_Scramble(S)
Step 4: **Steganographic Encoding**
Embed S_scrambled into C using the steganographic encoder to generate the stego image C_stego.
C_stego = Stego_Encode(C, S_scrambled)
Step 5: **Transmit Stego Image**
Send the stego image C_stego over the communication channel.
Step 6: **Receive Stego Image**
Receive the stego image C_stego.
Step 7: **Steganographic Decoding**
Extract the scrambled secret data S_scrambled from C_stego using the steganographic decoder.
S_scrambled = Stego_Decode(C_stego)
Step 8: **Apply Inverse Arnold Scrambling**
Revert S_scrambled to its original form S using inverse Arnold scrambling.
S = Inverse_Arnold_Scramble(S_scrambled)
Step 9: **Revealed Secret Data**
The decoded data S should match the original secret data.
Step 10: **Performance Analysis**
Analyze the performance using standard performance evaluation metrics.
End

3. Hybrid Crypto-Stego model

The proposed hybrid crypto-stego approach amalgamates the strongest crypto and stego processes for secure embedding and extraction of digital data. Firstly, the cover image is selected and is made more suitable for data embedding by compressing it through a GAN. At the same time, the data is also prepared for secure transmission as depicted in Fig.7.

The encrypted and scrambled information is then passed on to the Hiding Network, where the CNNs are applied for the data-hiding procedure. The Hiding Network using the CNNs successfully embeds the encrypted information within the compressed cover image and thereby creates the stego-image. The following is the model diagram of the stego-image creation using the Hiding Network and the application of the CNNs. The stego-image model diagram explains the concept of creating the stego-image using the Hiding Network and the application of the CNNs within the stego-image creation. The following diagram explains the stego-image creation.

The stego image that holds the secret information is transmitted through a communication channel to the receiver party. The stego image is then processed for data recovery through the Revealing Network. The Revealing Network undoes the embedding process done by the Hiding Network and unscrambles and decrypts the data.

This data is then processed using the inverse Arnold Transform, resulting in the descrambled

data being unveiled in its original form. This data is decrypted using the decryption algorithm of NTRU to obtain the original secret data. This procedure ensures that the data is secure and undetectable during transmission. The performance of this whole model is also verified through validation as well as testing. The performance of the model is further measured through validation of parameters such as embedding capacity, steganographic measures, steganalysis attack, and computational efficiency.

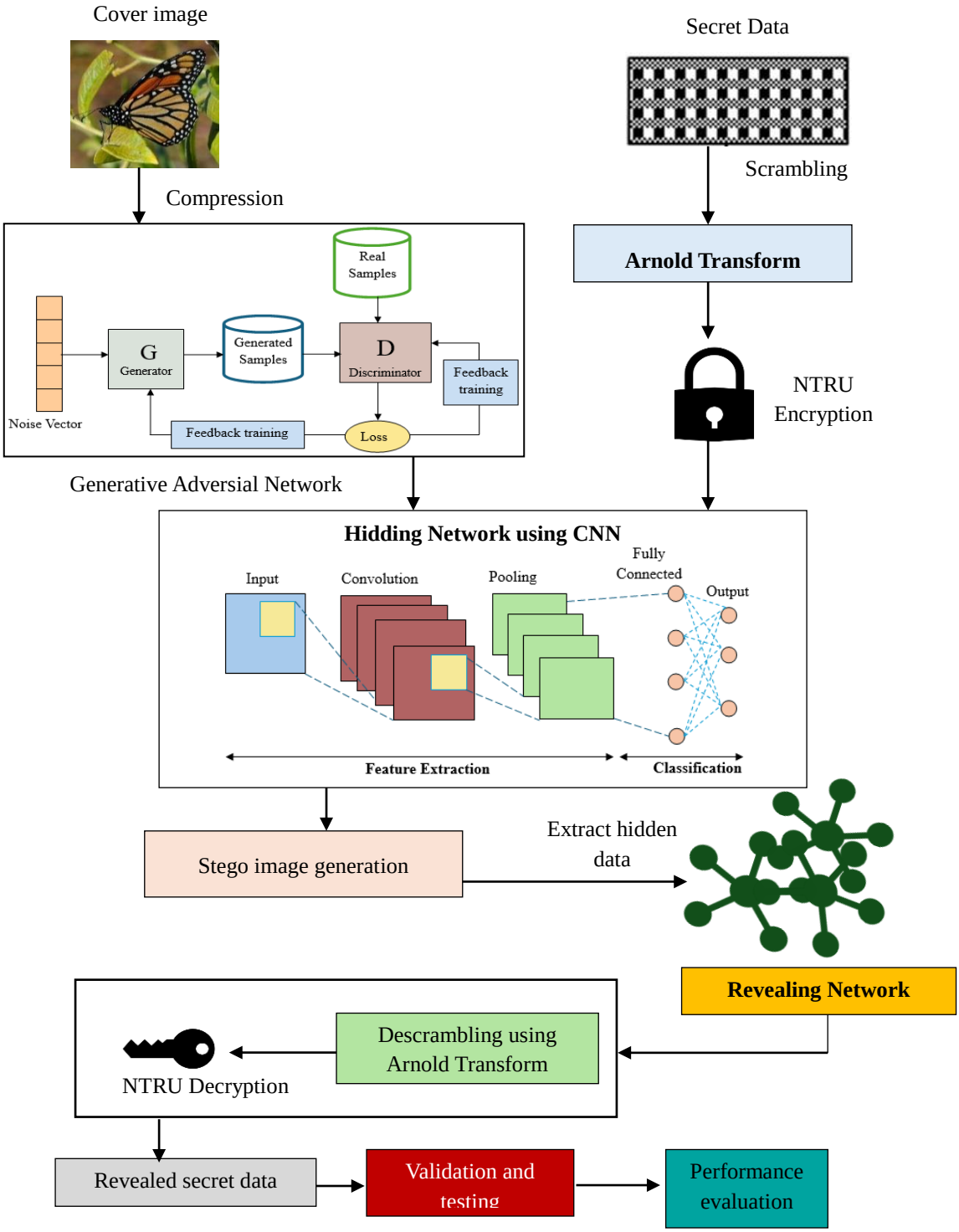

Fig 7: Proposed Hybrid crypto-Stagno framework

Algorithm 3:Efficient Crypto-Stagno approach

Start

Step 1:Image Dataset and Secret Image Preparation

Image Dataset Preparation :

Dataset: Use a set of high-quality cover images

$$\boldsymbol{I} = \{\boldsymbol{i_1}, \boldsymbol{i_2}, \ldots\ldots \boldsymbol{i_n}\}$$

Secret Image Dataset Preparation:

Dataset: Use a set of secret data

$$\boldsymbol{S} = \{\boldsymbol{S_1}, \boldsymbol{S_2}, \ldots\ldots, \boldsymbol{S_m}\}$$

Step 2:Pre-processing Process

Scrambling of Secret Image Data:

Arnold Transform: Apply the Arnold Transform to scramble each secret data **S**.

Transformation Formula: For data of size N×N, the Arnold Transform is defined as:

$$\begin{pmatrix} \boldsymbol{x'} \\ \boldsymbol{y'} \end{pmatrix} = \begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} \end{pmatrix} \begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{y} \end{pmatrix} \boldsymbol{mod N}$$

Iteration: Iterate this process for a fixed number of times to scramble the image.

Step 3:Compression and encryption

1 **Compression using GAN:**

Training: Train a GAN to compress cover images using the DIV2K dataset. Let **G** be the generator, and **D** be the discriminator.

Loss Function:

$$\boldsymbol{L = E_{x\sim Pdata}(x)[logD(x)] + E_{z\sim Pz}(z)[log(1 - D(G(Z)))]}$$

Compression: Use **G** to compress each image **I** to a lower-dimensional representation.

2 **Encryption of Secret Image Data using NTRU:**

Encryption: Let **P** be the plaintext, and $\mathbf{E_k(P)}$ be the encryption using NTRU.

The encrypted data is $\mathbf{C = E_k(P).}$

Step 4:Hiding Network using CNN

1 **CNN Model:**

Design: Develop a CNN to embed encrypted secret images into cover images using the COCO dataset.

Input and Output: Let **H** be the hiding network. The input is$\hat{\boldsymbol{I}}, and \mathbf{C}$ (encrypted secret data), and the output is the stego image **S**.

$$\boldsymbol{S = H(\hat{I}, C)}$$

Step 5:Stego Image Generation

Generation of Stego Image:

Reconstruction: Reconstruct the Stego image $\boldsymbol{S'}$.

Visual Quality: Ensure $\boldsymbol{S'}$is visually indistinguishable from the cover image **I.**

Step 6:Revealing Network

Extraction using Revealing Network:

Network Design: Design a revealing network **R** to extract hidden data from the stego images.

For each stego frame **S**, the network recovers the encrypted data $\hat{\boldsymbol{c}}$:

$$\hat{\boldsymbol{c}} = \boldsymbol{R(S)}$$

Step 7:Post-processing

Decryption and Descrambling:

Decryption: Decrypt the extracted secret data $\hat{\boldsymbol{c}}$using NTRU decryption:

$$\hat{\mathrm{P}} = \mathrm{D_k}(\hat{\boldsymbol{c}})$$

Descrambling: Apply the inverse Arnold Transform to descramble :

$$\begin{pmatrix} \mathrm{x} \\ \mathrm{y} \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} \mathrm{x'} \\ \mathrm{y'} \end{pmatrix} \bmod \mathrm{N}$$

Step 8:Validation and testing

Robustness Testing:

Operations: Apply common image processing operations on **S**.

Recovery: Measure the ability to recover hidden data after these operations.

Security Analysis:

Assessment: Employ machine learning-based detection techniques to evaluate resilience against steganalysis assaults.

Capacity Testing:

Testing: Ascertain the maximum data volume that can be safely concealed inside various picture formats without compromising visual integrity.

Step 9:Performance Evaluation
Metrics: Evaluate the system based on metrics like Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), etc., to assess the quality of the steganographic process.
End

Evaluation Parameters
The performance of the three recommended models is evaluated using three key metrics: PSNR, SSIM, and Payload, which are given as follows:

1. PSNR
The greater the PSNR value, the closer the stego image is to the original image, i.e., the embedding did not severely degrade the image quality. It is estimated as:

$$\text{PSNR} = 10 \cdot \log_{10}\left(\frac{\text{MAX}_I^2}{\text{MSE}}\right) \quad (7)$$

Here, MAX_I denotes the maximum possible pixel intensity, while MSE represents the mean squared error.

2. SSIM
SSIM is intended to better reflect human visual perception than PSNR. The SSIM is expressed by the formula:

$$\text{SSIM}(x,y) = \frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)} \quad (8)$$

Here, μ_x and μ_y represent the mean values, σ_x and σ_y denote the standard deviations, and $\sigma_x y$ indicates the covariance between images x and y.

3. Payload capacity
It refers to the quantity of hidden data that can be embedded in the cover image without affecting its visual quality or effectiveness. The payload capacity is often quantified in terms of Bits Per Pixel (BPP).

$$\text{Payload Capacity} = \frac{\text{Number of secret bits embedded}}{\text{Total no.of pixels in cover image}} \quad (9)$$

A rise in the payload capacity would result in a considerable decrease in the PSNR value.

Results and Discussion

1. Tool used
This section presents the major tools used in this study:
(i)Python
Python has been selected as the base programmatic language in this study to apply a secure data embedding and extraction system. TensorFlow and Keras libraries supported deep model training, and the Python library PyCryptodome supported NTRU encryption for protecting data securely. Image processing operations like scrambling and embedding were handled by OpenCV and PIL, and Matplotlib and Seaborn offered tools to visualize performance metrics. The interlinking of these libraries supported smooth interaction between cryptographic methods and deep learning models.
(ii)Google Colab
It has native Jupyter Notebook support and pre-installed packages, and hence ranks among the choice tools used by developers and researchers. Its cloud computing environment doesn't require local device setup, and hence users don't need to worry about the development and testing of the model, even remotely.

System Configuration
Experiments to validate the suggested secure digital data embedding and extraction system were performed using the following hardware configuration as shown in table 1.

Table 1: System Configuration

Component	Specification
Processor (CPU)	Intel Core i7-12700K (12 Cores, 3.6 GHz)
GPU	NVIDIA GeForce RTX 3090 (24 GB GDDR6X)
RAM	32 GB DDR4
Storage	1 TB NVMe SSD
Operating System	Windows 11 Pro (64-bit)
Programming Language	Python 3.9
Frameworks/Libraries	TensorFlow 2.10, Keras, OpenCV, PyCryptodome
Image Processing	PIL, NumPy, Matplotlib, Seaborn
Development IDE	PyCharm, Jupyter Notebook

2. Hyperparameters
Table 2 discussed the hyperparameter of the cryptographic, steganographic and hybrid Crypto-Stegano model.

Table 2: Hyperparameters

Model	Hyperparameter	Value
Cryptographic Model	Encryption Scheme	NTRU
	Key Size	256 bits
	Polynomial Degree (N)	251
	Cipher Block Size	128 bits
	Execution Iterations	1000
Steganographic Model	Image Size	512 × 512 pixels
	Scrambling Method	Arnold Transform
	Iterations (Arnold)	10
	Embedding Capacity	30% of the cover image size
	PSNR Threshold	≥ 35 dB
	SSIM Threshold	≥ 0.95
Hybrid Crypto-Stegano	GAN Learning Rate	0.0002
	Batch Size	32
	CNN Layers	5
	Activation Function	LeakyReLU
	Optimizer	Adam
	Epochs	50
	Loss Function (GAN)	Binary Cross-Entropy
	Embedding Capacity	45% of the cover image size
	Stego Image Size	512 × 512 pixels
	PSNR Threshold	≥ 42 dB
	SSIM Threshold	≥ 0.98

3. Result Analysis

Table 3 and table 4 shows the performance evaluation of the utilized secured digital data embedding techniques, including only cryptographic, only steganographic, and hybrid crypto-stego, was carried out based on encryption/decryption time, embedding capacity, image quality, security strength, and attack resistance.

Table 3: Result Analysis with parameters

Sr. No.	Parameters	Analysis
1.	Encryption/Decryption time	The cryptographic model demonstrated fast encryption of 2.1 ms and decryption of 1.9 ms, whereas the hybrid approach took slightly longer, 2.4 ms encryption, and 2.2 ms decryption due to the additional embedding process.
2.	Embedding Capacity	In terms of embedding capacity, the cryptographic model does not support data hiding, while the steganographic model allows for 150 KB. The hybrid approach improves on this by achieving 200 KB, making it a more efficient method for data concealment.
3.	Image Quality	The quality of images, as approximated based on PSNR and SSIM, was improved in the hybrid model compared to the steganographic model with minimal visual deterioration and higher fidelity.
4.	Security Strength	From a security perspective, the cryptography model is rated with good encryption, followed by the steganographic model, which scores lower as it solely utilizes information hiding without encryption. By using both methods together, the hybrid method achieves a high security score, making it the most secure method among the three methods.
5.	Attack Resistance	The hybrid method also employs the highest level of resistance against attacks than cryptography and steganography since it takes advantage of both encryption and data hiding.

Table 4: Performance analysis of utilized approaches

Metric	Only Crypto	Only Stego	Hybrid
Encryption Time (ms)	2.1	-	2.4

Decryption Time (ms)	1.9	-	2.2
Embedding Capacity (KB)	0	150	200
PSNR (dB)	-	38.5	67.2
SSIM	-	0.92	0.95
Security Strength (1-10)	9	5	10
Resistance to Attacks (1-10)	8	6	10

4. Comparative analysis

Comparative performance analysis of Cover/Stegovs Secret/Reconstructed image pairs displays substantial divergence in the performance of different methods between DIV2K and COCO datasets as measured by PSNR and SSIM scores as shown in table 3.

Table 3: Comparison for Cover/Stego Image on DIV2K and COCO datasets

Author	Methods	DIV2K		COCO	
		PSNR (dB)	SSIM	PSNR (dB)	SSIM
Liang et al., (2025) [15]	cINN	42.6257	0.9851	41.3457	0.9824
Huo et al., (2024) [16]	CHASE_WO	35.98	0.94	33.59	0.92
	CHASE	33.09	0.91	31.34	0.90
Jing et al., (2021) [17]	HiNet	48.99	0.9971	46.52	0.9961
Our Study	Hybrid Crypto-stego NTRU+(GAN-CNN)	57.50	0.9986	53.81	0.9979

Conclusion

The observed results highlight the robustness of integrating cryptography and steganography through deep learning. Although the cryptography model ensures good encryption and the steganographic model ensures concealment, the integration approach effectively withstands the trade-off between visual quality and security. Even in the case of the detection of hidden data, without the decryption key, it is not possible to decode it, which renders the system highly resistant to attack. Further, GAN-compressed cover image deployment helps improve resistance to steganalysis without compromising payload. The evaluation is evidence that supports that the hybrid crypto-stego model offers an applicable real-world digital communication practical, secure, and efficient solution superior to single-component approaches in ensuring confidentiality and data integrity.

Acknowledgment

I express my profound gratitude for the essential assistance and support from my Research Advisory Committee members, Dr. Ajay Surwade and Dr. Ajay Patil. Their insightful suggestions, critical feedback, and encouragement have played a significant role in shaping the quality of this research work. I extend my heartfelt gratitude to my research guide, Dr. Monali Khachane, for her continuous supervision, expert advice, and constant motivation throughout the research process. Her profound attention, patience, and insightful contributions have been vital to the effective completion of this project. I remain deeply thankful to all of them for their time, efforts, and contributions that have guided this research to fruition.

References

[1] Abirami, Ms Nagamany, and M. S. Anbarasi. "An Efficient Multilayer approach for Securing E-Healthcare Data in Cloud using Crypto–Stego Technique." International Research Journal on Advanced Science Hub 6, no. 06 (2024): 135-143.

[2] Jan, Aiman, Shabir A. Parah, Bilal A. Malik, and Mamoon Rashid. "Secure data transmission in IoTs based on CLoG edge detection." Future Generation Computer Systems 121 (2021): 59-73.

[3] Abiodun, Oludare Isaac, Esther OmolaraAbiodun, MoatsumAlawida, Rami S. Alkhawaldeh, and HumairaArshad. "A review on the security of the internet of things: Challenges and solutions." Wireless Personal Communications 119 (2021): 2603-2637.

[4] Khan, Wazir Zada, Mohammed Y. Aalsalem, Muhammad Khurram Khan, and Quratulain Arshad. "Data and privacy: Getting consumers to trust products enabled by the Internet of Things." IEEE Consumer Electronics Magazine 8, no. 2 (2019): 35-38.

[5] Sujan Hiregundagal Gopal Rao. (2023). A Review of Intrusion Detection Methods for In-Vehicle Networks at the Semiconductor Level. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(10s), 1032–1036. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/8000.

[6] Al-Roithy, BudoorObid, and Adnan Gutub. "Remodeling randomness prioritization to boost security of RGB image encryption." Multimedia Tools and Applications 80, no. 18 (2021): 28521-28581.

[7] Parah, Shabir A., Javaid A. Sheikh, Umer I. Assad, and Ghulam M. Bhat. "Hiding in encrypted images: a three tier security data hiding technique." Multidimensional Systems and Signal Processing 28 (2017): 549-572.

[8] Luo, Yuqin, Jin Yu, Wenrui Lai, and Lingfeng Liu. "A novel chaotic image encryption algorithm based on improved baker map and logistic map." Multimedia tools and applications 78 (2019): 22023-22043.

[9] Jan, Aiman, Shabir A. Parah, and Bilal A. Malik. "Logistic map-based image steganography using edge detection." In Innovations in Computational Intelligence and Computer Vision: Proceedings of ICICV 2020, pp. 447-454. Springer Singapore, 2021.

[10] Muhammad, Khan, Muhammad Sajjad, IrfanMehmood, Seungmin Rho, and Sung Wook Baik. "Image steganography using uncorrelated color space and its application for security of visual contents in online social networks." Future Generation Computer Systems 86 (2018): 951-960.

[11] Hassan, Fatuma, Saeid, and Adnan Gutub. "Novel embedding secrecy within images utilizing an improved interpolation-based reversible data hiding scheme." Journal of King Saud University-Computer and Information Sciences 34, no. 5 (2022): 2017-2030.

[12] Kim, Cheonshik, Ching-Nung Yang, and Lu Leng. "High-capacity data hiding for ABTC-EQ-based compressed image." Electronics 9, no. 4 (2020): 644.

[13] Hassan, Fatuma, Saeid, and Adnan Gutub. "Improving data hiding within colour images using hue component of HSV colour space." CAAI Transactions on Intelligence Technology 7, no. 1 (2022): 56-68.

[14] Hussan, Muzamil, Shabir A. Parah, Solihah Gull, and G. J. Qureshi. "Tamper detection and self-recovery of medical imagery for smart health." Arabian Journal for Science and Engineering 46 (2021): 3465-3481.

[15] Loan, Nazir A., Nasir N. Hurrah, Shabir A. Parah, Jong Weon Lee, Javaid A. Sheikh, and G. Mohiuddin Bhat. "Secure and robust digital image watermarking using coefficient differencing and chaotic encryption." IEEE Access 6 (2018): 19876-19897.

[16] Prasad, Shiv, and Arup Kumar Pal. "An RGB colour image steganography scheme using overlapping block-based pixel-value differencing." Royal Society open science 4, no. 4 (2017): 161066.

[17] Alkhudaydi, Malak, and Adnan Gutub. "Securing data via cryptography and arabic text steganography." SN Computer Science 2, no. 1 (2021): 46.

[18] Gutub, Adnan, and Nouf Al-Juaid. "Multi-bit stego-system for hiding text in multimedia images based on user security priority." Journal of computer hardware engineering 1, no. 2 (2018): 1-9.

[19] Biswas, Rajib, Imon Mukherjee, and Samir Kumar Bandyopadhyay. "Image feature-based high-capacity steganographic algorithm." Multimedia Tools and Applications 78 (2019): 20019-20036.

[20] Arya, Anupriya, and Sarita Soni. "Performance evaluation of secret image steganography techniques using the least significant bit (LSB) method." Int. J. Comput. Sci. Trends Technol 6, no. 2 (2018): 160-165.

[21] Melman, Anna, and Oleg Evsutin. "On the efficiency of metaheuristic optimization for adaptive image steganography in the dft domain." In 2021 XVII International Symposium" Problems of Redundancy in Information and Control Systems"(REDUNDANCY), pp. 49-54. IEEE, 2021.

[22] Emmanuel, G., G. G. Hungil, J. Maiga, and A. J. Santoso. "Information hiding in images using Discrete Cosine Transform." In IOP Conference Series: Materials Science and Engineering, vol. 1098, no. 5, p. 052083. IOP Publishing, 2021.

[23] Sabeti, Vajiheh, and MahsaAmerehei. "Secure and Imperceptible Image Steganography in Discrete Wavelet Transform Using the XOR Logical Function and Genetic Algorithm." ISeCure 14, no. 2 (2022).

[24] Patel, Sunil Kumar, and Chandran Saravanan. "Performance analysis of hybrid edge detector scheme and magic cube-based scheme for steganography application." In the 2018 international

conference on communication, computing and Internet of things (IC3IoT), pp. 299-303. IEEE, 2018.

[25] Desai, Latika, and Suresh Mali. "Crypto-Stego-Real-Time (CSRT) System for Secure Reversible Data Hiding." VLSI Design 2018, no. 1 (2018): 4804729.

[26] Sharma, Divya, and Chander Prabha. "Hybrid security of EMI using edge-based steganography and three-layered cryptography." In Applied Data Science and Smart Systems, pp. 278-290. CRC Press, 2024.

[27] Jan, Aiman, Shabir A. Parah, Muzamil Hussan, and Bilal A. Malik. "Double-layer security using crypto-stego techniques: a comprehensive review." Health and Technology 12, no. 1 (2022): 9-31.

[28] Das, Indrajit, Shalini Singh, Sonali Gupta, Amogh Banerjee, Md Golam Mohiuddin, and Shubham Tiwary. "Design and implementation of secure ATM system using machine learning and crypto–stego methodology." SN Applied Sciences 1, no. 9 (2019): 976.

[29] Rehman, Waheed. "A novel approach to image steganography using generative adversarial networks." arXiv preprint arXiv:2412.00094 (2024).

[30] Bao, Zhenjie, and Ru Xue. "Survey on deep learning applications in digital image security." Optical Engineering 60, no. 12 (2021): 120901-120901.

[31] Sanjalawe, Yousef, Salam Al-E'mari, Salam Fraihat, MoslehAbualhaj, and Emran Alzubi. "A deep learning-driven multi-layered steganographic approach for enhanced data security." Scientific Reports 15, no. 1 (2025): 4761.

[32] Ramadhan, IrsyadFikriansyah, Ntivuguruzwa Jean De La Croix, Tohari Ahmad, and Andre Uzamurengera. "Huffman coding-based data reduction and quadristego logic for secure image steganography." Engineering Science and Technology, an International Journal 65 (2025): 102033.

[33] Priya, S., S. P. Abirami, B. Arunkumar, and B. Mishachandar. "Super-resolution deep neural network (SRDNN) based multi-image steganography for highly secured lossless image transmission." Scientific Reports 14, no. 1 (2024): 6104.

[34] Huo, Lin, Ruipei Chen, Jie Wei, and Lang Huang. "A high-capacity and high-security image steganography network based on chaotic mapping and generative adversarial networks." Applied Sciences 14, no. 3 (2024): 1225.

[35] Mawla, Noura A., and Hussein K. Khafaji. "Enhancing data security: A cutting-edge approach utilizing protein chains in cryptography and steganography." Computers 12, no. 8 (2023): 166.

[36] Kosuru, SNVJ Devi, Anita Pradhan, K. Abdul Basith, Reshma Sonar, and Gandharba Swain. "Digital image steganography with error correction on extracted data." IEEE Access 11 (2023): 80945-80957.

[37] Rathore, Manjari Singh, M. Poongodi, PraneetSaurabh, Umesh Kumar Lilhore, Sami Bourouis, WajdiAlhakami, Jude Osamor, and MounirHamdi. "A novel trust-based security and privacy model for the Internet of vehicles using encryption and steganography." Computers and Electrical Engineering 102 (2022): 108205.

[38] Awadh, WidAkeel, Ali Salah Alasady, and Alaa Khalaf Hamoud. "Hybrid information security system via combination of compression, cryptography, and image steganography." International Journal of Electrical and Computer Engineering 12, no. 6 (2022): 6574-6584.

[39] Mahmoud, Mahmoud M., and Huwaida T. Elshoush. "Enhancing LSB using binary message size encoding for high capacity, transparent and secure audio steganography–an innovative approach." IEEE Access 10 (2022): 29954-29971.

[40] Wahab, Osama Fouad Abdel, Ashraf AM Khalaf, Aziza I. Hussein, and Hesham FA Hamed. "Hiding data using an efficient combination of RSA cryptography and compression steganography techniques." IEEE access 9 (2021): 31805-31815.

[41] Rakshit, Pranati, Sreeparna Ganguly, Souvik Pal, and Ayman A. Aly. "Securing Technique Using Pattern-Based LSB Audio Steganography and Intensity-Based Visual Cryptography." Computers, Materials & Continua 67, no. 1 (2021).

[42] https://www.kaggle.com/datasets/sharansmenon/div2k

[43] https://www.kaggle.com/datasets/awsaf49/coco-2017-dataset

[44] Hu, Donghui, Liang Wang, Wenjie Jiang, Shuli Zheng, and Bin Li. "A novel image steganography method via deep convolutional generative adversarial networks." IEEE Access 6 (2018): 38303-38314.

[45] Shieh, Chin-Shiuh, Thanh-Tuan Nguyen, Wan-Wei Lin, Wei Kuang Lai, Mong-Fong Horng, and Denis Miu. "Detection of adversarial ddos attacks using symmetric defense generative adversarial networks." Electronics 11, no. 13 (2022): 1977.

[46] Subramaniyan, Venkatesh, Vignesh Sivakumar, A. K. Vagheesan, S. Sakthivelan, K. J. Kumar, and K. K. Nagarajan. "GANash--A GAN approach to steganography." arXiv preprint arXiv:2110.13650 (2021).

[47] Abdulmunem, Inas Ali, Eman S. Harba, and Hind S. Harba. "Advanced Intelligent Data Hiding Using Video Stego and Convolutional Neural Networks." Baghdad Science Journal 18, no. 4 (2021): 1317-1317.

[48] Alsaleh, Ahmad, and CahitPerkgoz. "A space and time efficient convolutional neural network for age group estimation from facial images." PeerJ Computer Science 9 (2023): e1395.

[49] Thakur, Abhinav, Harbinder Singh, and Shikha Sharda. "Secure video steganography based on discrete wavelet transform and arnold transform." International Journal of Computer Applications 123, no. 11 (2015).

[50] Al-Taweel, Sadik Ali, Muhammed Husain Al-Hada, and Ahmed Mahmoud Nasser. "Image in image steganography technique based on Arnold transform and LSB algorithms." International Journal of Computer Applications 181, no. 10 (2018): 32-39.

[51] Boukari, Souley, and JaafaruBobbo. "An Improved Cybersecurity Model using Cryptography and Steganography with NTRU-LSB Algorithm." SAR Journal-Science and Research 3, no. 2 (2020): 71-78.