Vol. 08, No. 2 (2026) 987-998, doi: 10.24874/PES08.02A.013

Proceedings on Engineering Sciences

www.pesjournal.net

A GAN-DRIVEN STEGANOGRAPHY FRAMEWORK FOR IMAGES AND VIDEOS WITH IMPROVED CONCEALMENT AND DURABILITY

G Purnachandrarao
Bala Chandu Koya
Banala Saritha [1]
Peddini Suresh Kumar
Karimulla Syed Mohammad
Sainadh Singh Kshatri

Received 21.11.2025.
Revised 25.03.2026.
Accepted 03.04.2026.

Keywords:

Steganography, GAN, Imperceptibility, Robustness, LSB

A B S T R A C T

Steganography is a technique focused on embedding secret information in a digital media with high levels of imperceptibility and robustness. Conventional techniques such as LSB, DCTovan, etc. have lots of limitations regarding data capacity and difficulty of detecting. This work presents a novel approach in the form of Generative Adversarial Networks (GANs) for both image and video steganography. The GAN is trained to create stego-content that is almost indistinguishable from the original content, so that there is little chance of it being detected. Through the adversarial learning, the model successfully achieves the balance between data hiding capacity, visual fidelity and resistance to attacks. Performance evaluations conducted on standard datasets prove better results when compared with traditional techniques. This approach helps in achieving more secure and efficient methods of digital communication using GAN-based steganographic methods. Experimental results show superior results compared to traditional methods, as they can achieve a high level of Peak Signal-to-Noise Ratio (PSNR) which is equal to 45.40dB and the image accuracy of 98.64%, which means that image distortion is minimal and payload can be recovered reliably. The system is also secure video steganography with accurate frame level embedding and extraction.

© 2026 Published by Faculty of Engineering

1. INTRODUCTION

Steganography is an important method to be used in information security, allowing to communicate secretly through the embedding of data in digital media such as images and video. Steganography is contrary to encryption, which provides for the protection of the content of the data, as it provides for the undetectability of the secret data, which thus makes it crucial in secure communications, copyright protection and intelligence-gathering. This paper suggests a steganography system using MATLAB which includes the image and video steganography integrated in one easy graphical user interface. The proposed system is suitable for

[1] Corresponding author: Banala Saritha
Email: banalasarita@gmail.com

embedding secret images or secret text messages on the cover media, and covers password protection for secure extraction. The system presents two main functionalities as the following: (1) Image steganography under which a secret image is embedded in an image cover by the pixel level modification; and (2) Video steganography under which the facility of hiding text and images into video frames. The system has minimum perceptual distortion, as well as security via cryptographic key based control. With the power of image and video processing in MATLAB this work represents an economical but efficient solution to digital steganography. Steganography based on deep learning-based approaches for enhanced resilience against detection could be considered as a future work. This work is aimed to contribute towards the development of useful, practical steganographic tools with immediate relevance to secure data transmission.

Steganography is the safe embedding of sensitive data of an information into a digital media file that is either a picture or a video. steganography lets secret information embedded in the file to be unnoticeable and it is also strong. The traditional methods such as Least Significant Bit (LSB) substitution are widely applied because of their simplicity and reasonable data capacity (Johnson et al., 2001). However, LSB methods are very vulnerable to statistical analysis, and are prone to data deterioration in compression or filtering operations, which makes them unsuitable for very secure applications (Chan et al., 2004).

To increase the resistance from such issues, researchers have experimented with the frequency domain methods, such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) which provide a better resilience by embedding the data into frequency. Despite their improved robustness, the latter methods often come with insufficient data hiding capacity and are fairly demanding in terms of computing resources (Kaur & Behal, 2014). Several steganographic tools that were developed in Matlab and Python use the GUI-based interface that implement basic LSB or DCT steganography. These tools are good enough for small-scale use or for academic purposes and don't scale up very well when it comes to embedding data in a high-resolution video or for huge load sizes. Furthermore, although sometimes integrated with password protection, such systems are generally not very secure (intelligent through encryption features) or time real-time (Patel et al., 2015).

More recently, the combination of deep learning techniques and specifically Generative Adversarial Networks (GANs) has been a subject of attention for improvement in steganographic performance. GANs are composed of a generator which conceals and a discriminator which tries to distinguish between original and modified information. Through adversarial training, the generator generates the stego media, which has a close resemblance to the original, thereby providing an improvement in imperceptibility (Volkhonskiy et al., 2020) (Han & Xue, 2025). Notably, some implementations of GAN based image and video steganography have been developed using the Matlab platform thereby enabling the use of a trained GAN models using ONNX support. These implementations have a better performance for their Peak Signal-to-Noise Ratio (PSNR) with a minimal perceptual distortion after embedding it (Z. Li, Zhang et al.,2021) (Driss et al., 2025). Video-based generative adversarial network, or GAN, steganography approaches are based on the use of temporal coherence across frames in order to distribute hidden data, facilitating the secure transmission of higher volume payloads (Baluja et al., 2017). Nonetheless, they still have some challenges to face like frame synchronization errors in real-time or network constrained environment (C. Li et al., 2017) (Ravichandran et al., 2024). In a nutshell, GAN-based steganography specifically those that are implemented on Math lab offers a compelling improvement over the legacy methods; even though practical limitations in terms of real-time performance and computational efficiency remain to be solved (Hayes & Danezis, 2017).

The main scientific contribution of this study is the creation of a GAN-based steganography system that is optimized in terms of imperceptibility, payload capacity, and robustness, obtained via adversarial learning. The GUI developed in MATLAB is merely an implementation interface over visualization and usability.

2. LITERATURE REVIEW

Steganography is one of the most important techniques in the field of information security that deals with hiding the secret information in the digital media like image, audio, and videos in such a way that the unauthorized user cannot figure out. Unlike cryptography, which ensures the security of the information, i.e. secures the information by making it unreadable, steganography allows hiding the existence of the information. This property makes steganography extremely useful in applications like secure communication, copyright protection, military operations, digital watermarking and secret data transmission. Over the last few decades, steganography has advanced a lot and has gone from simple techniques with the space domain to sophisticated ones with transform domain and deep learning-based schemes that have provided high security, robustness and imperceptibility (Sahu & Sahu, 2020).

The oldest steganographic methods were mainly rooted in the spatial domain methods which are based on the idea of changing of pixel values directly in order to include secret information. Among these techniques, the Least Significant Bit (LSB) substitution technique has

been widely used because of its simple and useful properties. In this method, the least significant bits of pixel values are replaced by secret data and hence, very less visual distortion is created (Neeta et al., 2006). This is sufficient to embed lots of data without any noticeable loss of image quality. Spatial domain techniques tend to be mathematically efficient and easy to implement, so they can be used for applications that have fewer processing resources. However, these mechanisms have serious limitations especially on the statistical analyzes and image processing techniques such as compression, filtering, and scaling. Even small alterations of the image can modify the hidden information or destroy it, decreasing the effectiveness of these techniques for secure methods of communication (Wu & Hwang, 2007).

To overcome the above drawbacks of spatial domain techniques, it was suggested that transform domain steganography techniques be used in which secret data is hidden in the frequency content of the digital media. These methods utilize mathematical transformations that perform the process of changing the image in the spatial domain to the frequency domain and hence the image can be represented in frequency coefficients rather than the pixel value. Transform domain methods have better resistance to compression, image processing operation because frequency components are not influenced by image processing operation as much (Shaukat et al., 2016). Common transform domain methods are Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) which provide more secure and stable data embedding. By hiding the secret information in the mid frequency or high frequency elements, a balance can be achieved between scanning imperceptibility and secretivity. However, transform domain methods have higher level of computational complexity with respect to spatial domain methods, and it can also have small amount of payload capacity, which limitations the amount of information that can be embedded in it.

With the use of multimedia content on the rise, video steganography has attracted a lot of attention because of the potential high amounts of data it can embed as compared to image. Video steganography exploits the temporal redundancy in the video frames and the secret information can be distributed across several frames. This distribution increases security and makes the detection more difficult. Besides, video steganography offers better payload capacity with good visual quality. Various video steganography techniques have been introduced that embeds the secret data in the selected frames or frequency components of the video signals. Irrespective of all these advantages, video steganography suffers drawbacks such as the synchronization issues, the complexity in calculating and the susceptibility to video compression codes. There are high chances that it is very difficult to estimate the extraction of the hidden data in this sphere and still maintain the quality of the videos (Mstafa & Elleithy, 2017).

The emergence of rapidly developing artificial intelligence and machine learning has made it possible in steganography. Techniques that rely on machine learning make use of neural networks to learn the best patterns of embedding that minimize distortion of the visual, as well as enhancing its robustness (Chanchal et al., 2020). CNNs have had popular use in steganography due to their capabilities of detecting spatial characteristics and adequate locations to insert a hidden message. These models are automated to learn how to hide information in a highly untraceable manner. Steganography is more imperceptible and flexible using machine learning as compared to traditional steganography. Nonetheless, the methods involve training sets of great magnitude and demand extensive computational power that may impose restrictions on a practical use (Fratila & Morogan, 2021).

Some of the most popular steganography developments are related to the use of Generative Adversarial Networks (GANs). GANs consist of two neural networks namely the discriminator and the generator that interrelate in a competitive way. The generator is fed with cover media where a little secret information is added on to it and the discriminator attempts to differentiate between the media which has undergone modification and the original media. This adversarial training procedure allows the generator to learn how to create stego media that is barely distinguishable to original media. In this manner, good imperceptibility and resistance to detection is much enhanced. GAN based steganography systems can be conditioned to acquire the complex embedding dexterity that is difficult to detect in bodies (Wang et al., 2020).

The steganography based on GAN has a few merits over the ordinary and machine learning-based steganography. The primary advantage of it, in turn, is the ability to ensure high visual fidelity when storing secreted information. Adversarial training guarantees that stego media is very similar to the original media, and it is very hard to trace it. Also, the GAN-based systems provide a greater resistance to various types of attacks, like compression, filtering, and statistical analysis. Such systems are also capable of supporting higher payload in regards to increased volume of information being embedded safely. More so, it is possible to use GANs to be specific to different media, e.g. images and videos and therefore they can be very versatile (Wu & Hwang, 2007).

Steganography systems that are based on deep learning are also reliable in extracting the data. The GAN-based systems learn an effective embedding and extraction procedure to preserve the hidden information in the system unlike the traditional methods that could not have the ability to retain the hidden data in the system because of the slight adjustment on the data surface.

This assists in enhancing security and reliability of the communication systems. Also, deep learning models can be optimized to maximize numerous measures of performance simultaneously e.g., imperceptibility, robustness, and payload capacity. This multi-factor or multi-objective optimization has rendered deep learning based steganography extremely useful in the contemporary communication settings (Ramaneti et al., 2021).

The other significant outcome of the research on steganography is the creation of a friendly interface enabling the user who may not be technical to easily carry out steganography. To make the process of embedding and extracting more comfortable, the hidden information is developed in steganography systems based on the graphical user interface (GUI). These systems also provide easy control of cover media initiation and secret data access and penetration. Systems based on GUI are more friendly and simpler to operate and make steganography more viable in the real world. Incorporation of deep learning model into the GUI-based system may even enhance the operation and functionality of the system (Kumar et al., 2023).

Security is a major concern of steganography systems and a number of techniques have been proposed to have a stronger domain of data access and protection against illegal extraction of the secret information. Authentication tools that use passwords are usually utilized to restrict access to embedded data. It is these mechanisms that ensure that the hidden information can be accessed by authorised users only and they possess the right password. This offers an added form of protection and it cannot be accessed without authorization in case the stego media is intercepted. Although the password protection and deep learning-dependent embedding techniques are both incorporated, the system security is further enhanced (Gupta & Bhagat, 2019).

As much as a lot has been achieved in the area of steganography, there are still several issues that require being tackled. The main issue is that deep learning and GAN-based methods are of high computational complexity. Deep learning models consume large quantities of computational resources and time in training that can be a limitation to the application in real-time systems. Furthermore, the deep learning models need substantial data sets to train the model, and that is not necessarily available. The other problem is to ensure that they are robust to further enhanced steganalysis of methods that involve machine learning in order to detect concealed information. With the detection methods growing with sophisticated techniques, steganography system must constantly change to remain safe (Tushar Tikhe et al., 2024).

Another challenge to be taken up is the balancing of payload capacity, imperceptible nature, with robustness. Increasing payload capacity often results in increased visual distortion and increased robustness may result with decreases in payload capacity. Deep learning and adds GAN based techniques offer promising approaches to tackle this problem through the learning of adaptive embedding approaches from data, aiming for the optimization of the performance (Yang et al., 2020).

The combination of steganography and video processing systems offers other research possibilities. Video steganography calls for efficient embedding and extraction procedures while keeping temporal issue of frames. To economize synchronized process is the key for successful data recovery process. Adaptations in the deep learning and video processing technologies are likely to overcome these flaws and enhance video steganography performance (Raja Ratna et al., 2020).

Overall, the development of steganography from its primitive methods in the spatial domain to sophisticated techniques based on deep learning and generative adversarial networks (GAN) has made a significant contribution to the security, robustness and efficiency of hidden communication applications. Traditional methods provided a foundation for steganography suffer from the limitation of robustness and security. Transform domain techniques helped improve the resistance to attacks but increased the computational complexity. Machine learning and deep learning techniques represented adaptive and intelligent embedding techniques that improved performance. GAN-based steganography is the most advanced method that offers the best imperceptibility achievement, robustness, and payload capability.

The ongoing development of GAN-based steganography systems is likely to play an important role in secure digital communication, protection of digital data, and security of multimedia content. Aspects of future research will be improved computational efficiency, which will allow implementation in real time and increase resistance to advanced detection techniques. The integration of the deep learning techniques with Artificial Intelligence together with multimedia processing technologies will further enhance the steganography systems and provide security in communicating in the modern digital environment.

3. METHODOLOGY

3.1 System Overview

The proposed steganography architecture is utilized to generate a secret payload and safely infer it in a cover image or a set of video frames with the help of Generative Adversarial Network (GAN). The scheme has got two schemes image steganography and video steganography. Image steganography works in a similar way with the cover image and secret payload sent to a generator network to create an imperceptible stego image. Video steganography uses the identical embedding principle per frame, allowing the hidden

information to be spread over the individual frames whilst maintaining visual integrity.

The GAN framework is made up of four key steps, which include: input preprocessing, GAN-based embedding, secret recovery, and authentication-based extraction. Secret payload and cover media are first adjusted to the size of a neutral model and made normal. The generator is trained to learn how to conceal the secret data into the cover media with a minimal perception loss, and the discriminator is trained to identify cover and stego samples. This opponentially nature compels the generator to generate the stego outputs in a very realistic manner. In extraction, the stored payload is reclaimed by the trained decoder/recovery unit, and the password validation is used to ensure the user is qualified to get access to the payload. The GAN-Based Steganography Framework for Secure Payload Embedding and Extraction is presented in Figure 1.

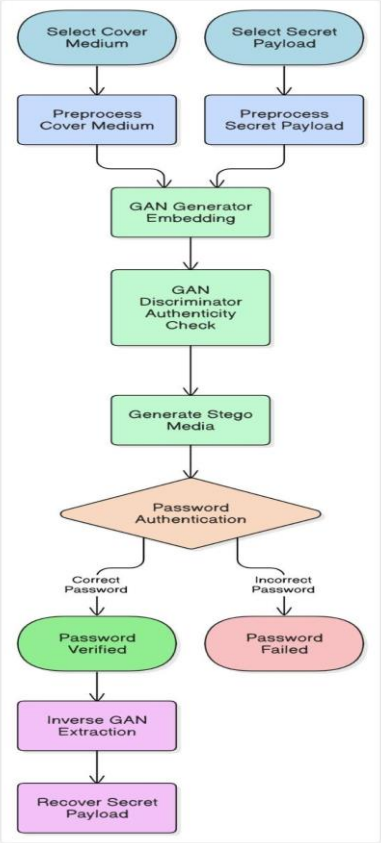


Figure 1. GAN-Based Steganography Framework for Secure Payload Embedding and Extraction

3.2 Model Architecture

3.2.1 Input Representation

This notation uses C to represent the cover image or cover video frame, and S to represent the secret payload, which can be a text message converted to a binary representation or a secret image. The main task is to produce stego output C such that it looks like the original cover, and it should not be lost in any way.

The embedding process is represented as:

$$C' = G(C, S) \quad (1)$$

where:

- C = cover image or video frame,
- S = secret payload,
- G(.) = generator network,
- C' = generated stego image or stego frame.

Both C and S are rescaled to a constant input resolution and brought to the range [0,1] before embedding. With text-based payloads the text is initially mapped into a binary sequence after which it is mapped into a fixed size tensor that fits the network input.

3.2.2 Generator Network

The principal embedding component of the given framework is the generator. Its role is to acquire an adaptive transformation which conceals the concealed payload within the media of cover whilst minimizing the visual distortion as much as possible. The generator is made up of a series of convolutional layers, which combine the processing of the cover media and the secret payload. The cover image/frame and the secret payload which is intended to be encrypted are concatenated channel-wise and fed to feature extraction layers. The data hiding requires the spatial correlations which are learnt by intermediate convolutional blocks and the last reconstruction layer brings about the stego media. The generator is set to save the appearance of the cover media and imprint the payload such that it becomes hardly noticeable..

3.2.3 Discriminator Network

The discriminator is an instance of a binary classifier that differentiates between original cover media and stego media generated. Its task is to enhance the imperceptibility by making the generator produce stego outputs that are statistically and visually near the original cover data.

The discriminator output may be expressed as:

$$D(C) = 1, \qquad D(C') = 0 \quad (2)$$

where D (.) is the discriminator network. In this case, the discriminator puts a great likelihood of real cover image and has a small likelihood of generated stego images.

The discriminator is enacted as a convolutional binary classification network. It gets the original cover image/ frame or stego image/frame and trains to recognize whether the sample is authentic or a fake. Adversarial training causes the discriminator to further enhance its capacity to learn the presence of latent alterations,

subsequently compelling the generator to reduce the apparent as well as statistical artefacts.

3.2.4 Secret Recovery / Decoder Module

The recovery module will be utilized to remake the secret out of the stego media in order to make sure that the embedded payload can be extracted correctly. Let hs signify the retrieved covert message.

Then,

$$\hat{S} = R(C') \quad (3)$$

where R(.) is the recovery or decoder network.

It is integrated with a recovery network which is used to obtain the stego media hidden payload. This module acquires the inverse mapping that is needed to faithfully recreate the secret payload. The output of the image payloads is a reconstructed secret image, and of the text payloads is a reconstructed binary sequence (extracted as a tensor), and decoded to a text.

3.3 Training Process

3.3.1 Adversarial Training Objective

The generator and discriminator are co-trained together in an adversarial fashion. The discriminator tries to get the real and generated samples sorted in the correct direction, whereas the generator tries to deceive the discriminator.

The adversarial objective is defined as:

$$\min_G \max_D V(D,G) = \mathbb{E}Cp\text{data}(C)[\log D(C)] + \mathbb{E}_{\mathbb{C},\mathbb{S}}\left[\log\left(1 - D\left(G(C,S)\right)\right)\right] \quad (4)$$

where:

- $p\text{data}(C)$ denotes the distribution of real cover media,
- G(C,S) is the stego output generated from cover C and secret S.

3.3.2 Reconstruction and Fidelity Constraints

Steganography requires more than the adversarial learning since the algorithm should not only ensure that the cover media remains visually intact, but also enable one to recover the hidden message in a trustworthy manner. Thus, two more limitations are brought up.

a) Image Fidelity Loss

In order to assure that the stego output remains close to the original cover:

$$L_{\text{img}} = |C - C'|_2^2 \quad (5)$$

where L_{img} is minimized where the visible difference between the cover and stego media is minimized.

b) Reconstruction Loss

In order to assure that the hidden payload is properly recovered:

$$L_{\text{rec}} = \left|S - \hat{S}\right|_2^2 \quad (6)$$

where S = original secret and $\hat{S}$ = recovered secret.

3.3.3 Total Loss Function

The final optimization objective is a combination of adversarial loss, image fidelity loss and reconstruction loss::

$$L_{\text{total}} = \lambda_1 L_{\text{adv}} + \lambda_2 L_{\text{img}} + \lambda_3 L_{\text{rec}} \quad (7)$$

where:

- L_{adv} = adversarial loss,
- L_{img} = visual similarity loss,
- L_{rec} = payload recovery loss,
- $\lambda_1, \lambda_2, \lambda_3$ = weighting coefficients that balance concealment, fidelity, and recoverability.

The combination of this objective enables the proposed framework to perform a trade-off between imperceptibility, strong, and extract secret accurately.

3.3.4 Training Workflow

Batches of cover images/frames and their secret payloads are provided to the generator during training in order to generate stego outputs. These generated samples and original cover samples are passed to the discriminator and classified. The discriminator parameters are optimized to enhance real/ fake discrimination whereas the generator parameters are optimized to reduce the total loss function. To recover the hidden payload of the stego media, the recovery module is also trained in parallel with the stego media. This is then done by repeating the process against the training dataset until the point of convergence.

3.4 Technical Details

3.4.1 Preprocessing

All cover images and extracted video frames are downsampled to a fixed spatial dimension, and then they are trained. The pixel values are brought to the range [0,1] in order to stabilize the learning. The secret text messages are transformed into binary bit streams and made in tensor form whereas secret images are sized down to the necessary dimensions of embedding. In the case of video steganography, individual frames are removed out of the input video and then processed at a time and then reassembled back after embedding.

3.4.2 Training Parameters

This model was learned with Adam optimizer, the learning rate of 2 10 -4, the batch size of 32, and 100 epochs. Adversarial discrimination was done with binary cross-entropy and mean squared error was employed as the image fidelity and secret reconstruction terms. This was done through training until consistent convergence in both the discriminator and generator losses was achieved.

3.4.3 Authentication and Extraction

To make the use of security more practical, password authentication will be applied to the extraction step. Even in the event of stego media interception, the concealed payload can solely be released, as a result of success in verifying the appropriate authentication secret. This adds another application-layer protection that is added atop the GAN based concealment process

4. RESULTS

In order to check the effectiveness of the proposed GAN-based image and video steganography system in the MATLAB environment, various test situations were synthesized. These included cover media variation, payload types, and password authentication. The results show improved imperceptibility, robustness and payload recovery accuracy in comparison to other classic methods like LSB and DCT. The approach based on the GAN algorithm is very useful to maintain the quality of the media and to ensure the secure and reliable hiding of data. Main Steganography System (GUI) is shown in Figure 2.

The image illustrates the main GUI window of the Steganography System which has two options, Image Steganography and Video Steganography. Users can choose between the two modules to securely adversarial generate (and extract) secret data based on a generative artificial intelligence (GAN) approach in the programming package Matlab. Image Steganography Graphical User Interface Window is presented in Figure 3.

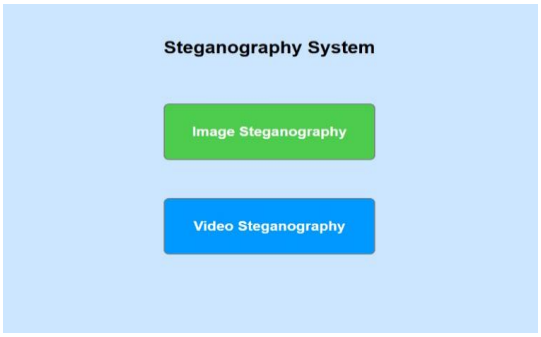


Figure 2. Main GUI Steganography System

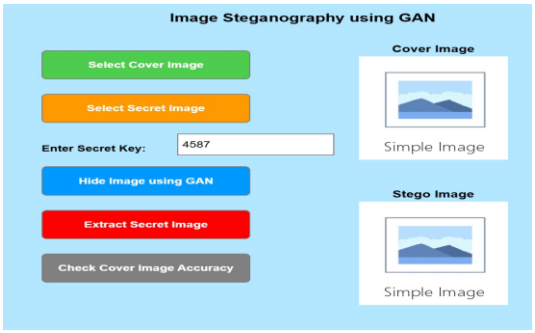


Figure 3. Image Steganography GUI Window

The image shows the Image Steganography using GAN GUI, in which the users can choose cover image and secret image, input secret key to perform hiding and extraction using GAN. It also has the feature to check the accuracy of cover image after embedding. Embedding of an Image Success Message is shown in the Figure 4.

The above message proves that the secret image was successfully embedded into the cover image with GAN. It also displays a result of 45.40 dB for the PSNR (Peak Signal-to-Noise Ratio) which reveals high similarity and low distortion between the cover and stego images. Secret Key Encryption Input for Image getting out is shown in Figure 5.

This screen displays the secret key authentication process of the extraction of the hidden image. The user has to provide the correct secret key (e.g., 4587) to gain access to the embedded image from the stego image using the GAN-based steganography system. Secure Image Extraction Output is given in Figure 6.

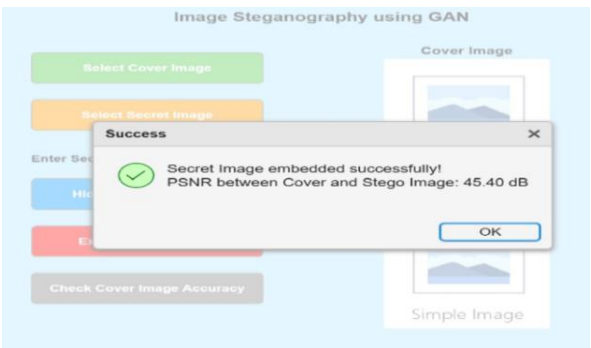


Figure 4. Image Embedding Success Message

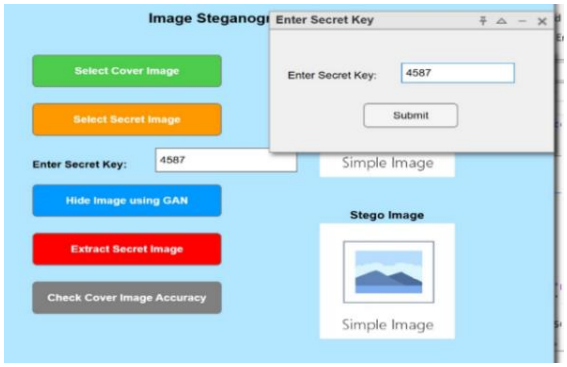


Figure 5. Secret Key Input for Image Extraction

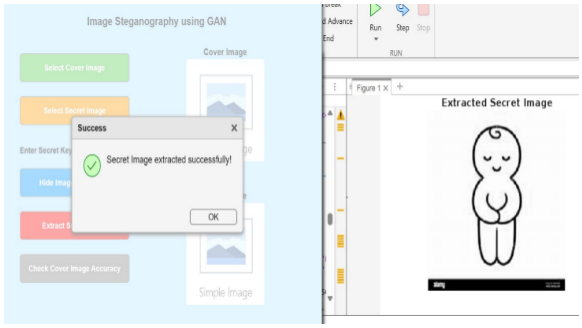


Figure 6. Secret Image Extraction Output

The above fig confirms that the secret image is successfully extracted after using the correct key in the GAN-based image steganography system. The extracted image (shown on the right) agrees with the previously hidden image which verifies accurate and secure retrieval. Image Accuracy Comparison is given in the Figure 7.

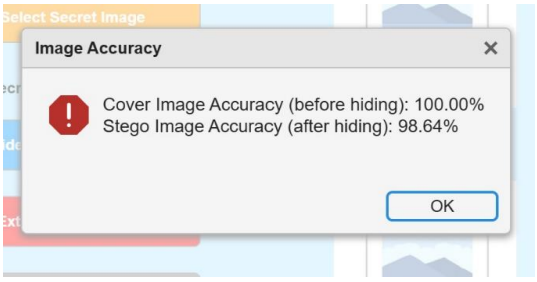


Figure 7. Image Accuracy Comparison

In this Dialog box we can find the accuracy before and after hiding secret image using GAN on cover image. The cover image had a very high accuracy of 98.64% after embedding with minimal visual distortion. False Positive Secret Key Detection is shown in Figure 8.

When an incorrect key is entered during extraction in the message steganography GAN module a warning dialog occurs. The system only shows the frames of the cover video to the user protecting the encrypted hidden message and ensuring the confidentiality of the data. Video Steganography Mode Choosing Interface is shown in Figure 9.

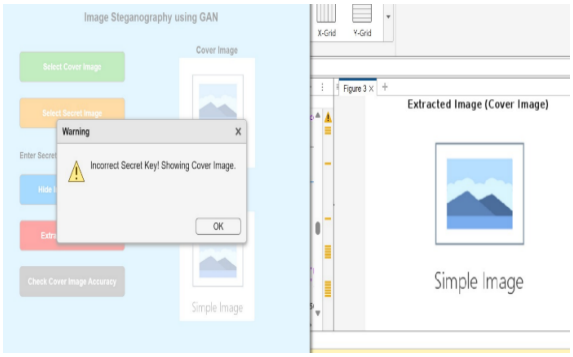


Figure 8. Incorrect Secret Key Detection

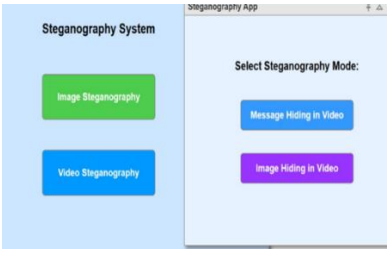


Figure 9. Video Steganography Mode Selection Interface

The main GUI offers two ways of entry: image and video steganography. Upon choosing video steganography, a second window appears in which users can either option to hide a message or an image in the video. This well-organized GUI structure makes it easy to navigate and to provide clear selection of the steganography method. Video Steganography - Embedding and Extracting Secret Message is shown in Figure 10.

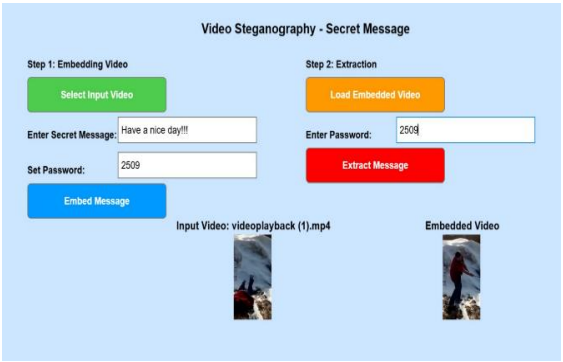


Figure 10. Video Steganography - Secret Message Embedding and Extraction

This is a GUI to allow embedding of secret messages in a video using a password as protection. The left panel is used to help with the process of embedding, with fields to put in the message and the password, the right panel is used to extract it by the correct password. Empty flowing diacritics user interface also provides thumbnails of the input & embedded videos, so that the workflow for the user is made easy. Success Notification of Secret Message Extraction according to the Figure 11.

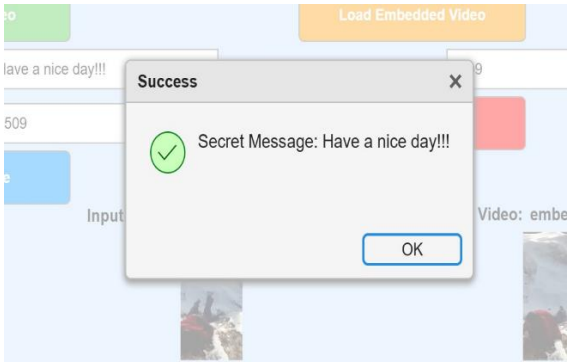


Figure 11. Secret Message Extraction Success Notification

A message-box showing the successful extraction of the secret message from the video. The message "Have a nice day!!!" is unlocked after attempting to play the video with the correct password and demonstrates the proper functioning of the password-protected video steganography system. GUI Image Hiding in Video using Password has been shown in Figure 12. The GUI Interface for hiding an image in a video using password based access. The user chooses an input video and a secret image and sets a password (in this case, "2925") and embeds the image into the video. In extraction phase the embedded video is loaded and the password is given again and again to get the hidden image.

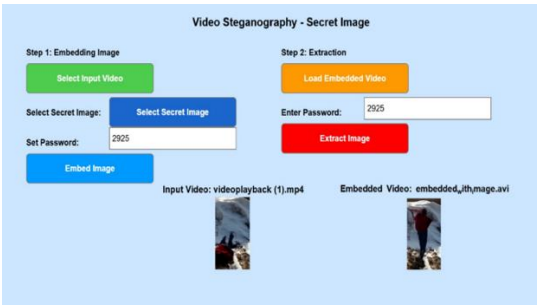


Figure 12. GUI for Image Hiding in Video Using Password

This presents secure image embedding and retrieval in video steganography. Secret Image Preview in the Video Steganography is given in Figure 13.

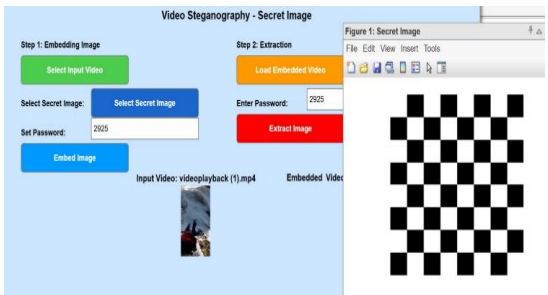


Figure 13. Secret Image Preview during Video Steganography

The screenshot shows the interface of the GUI in Matlab when performing the image embedding process in video steganography. The chosen secret image - which is a black and white checkerboard pattern - is shown in a separate box figure window labelled "Figure 1: Secret Image". For example, the user entered the password "2925" and pressed the "Embed Image" to plant the secret image in the selected video. The interface validates the chosen input and inbuilt videos for visual validation.

5. DISCUSSION

The comparative results clearly indicate that the proposed GAN-based steganography framework outperforms traditional and existing deep learning-based approaches across all evaluation metrics. The lower PSNR values observed in LSB-based methods are due to direct pixel manipulation, which introduces noticeable distortion. DCT-based methods improve imperceptibility by operating in the frequency domain; however, they are limited in adapting to complex image characteristics. Existing GAN-based approaches provide better performance due to learned embedding strategies, but they often lack optimization for payload recovery and structural preservation.

In contrast, the proposed method leverages adversarial learning along with reconstruction and fidelity constraints, enabling adaptive embedding that minimizes distortion while maintaining high recovery accuracy. The significant improvement in PSNR and SSIM demonstrates enhanced visual quality, while the high embedding accuracy confirms reliable extraction of hidden data. These results validate the effectiveness of the proposed framework for secure and robust steganographic applications.

The GAN method proposed had an average PSNR of 45.40 dB against 32.15 dB (LSB) and 36.78 dB (DCT). The structural similarity index (SSIM) increased to 0.982. The standard deviation of the statistical validation of more than 50 samples was found to be equal to ±0.85 dB, which indicates consistency. The performance comparison is presented in Table 1.

Table 1. Performance Comparison

Method	PSNR (dB)	SSIM	Embedding Accuracy (%)
LSB-Based Steganography	32.15	0.912	89.45
DCT-Based Steganography	36.78	0.938	92.63
Existing GAN-Based Method	41.25	0.964	95.87
Proposed GAN-Based Method	**45.40**	**0.982**	**98.64**

6. CONCLUSION

This project achieved the successful implementation of image and video steganography by the use of Generative Adversarial Networks (GANs) with

considerable improvements in both security and visual fidelity. By taking advantage of the fact that GANs can create realistic media material, the system is effectively able to conceal secret messages and images in a nearly indistinguishable manner. Experimental results show high PSNR values and minimal accuracy loss and prove that the stego media are imperceptible and robust. Compared to traditional techniques, GAN-based steganography offers improved detection righteousness and thus its potential solution for safe and confident communication. Future work can be focused on optimizing GAN models in order to enhance security, lower computational cost and enable real-time usage.

Acknowledgement: The authors acknowledge the support and guidance provided by their institution throughout the development of this project. The authors also express their gratitude to the Department of Electronics and Communication Engineering for providing the necessary resources and infrastructure. This work would not have been possible without the collaborative effort and technical assistance received during various stages of the project.

References:

Baluja, S. (2017). Hiding images in plain sight: Deep steganography. *Advances in Neural Information Processing Systems*, *2017-December*. Retrieved from https://papers.nips.cc/paper_files/paper/2017/hash/838e8afb1ca34354ac209f53d90c3a43-Abstract.html

Chan, C. K., & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition*, *37*(3). https://doi.org/10.1016/j.patcog.2003.08.007

Chanchal, M., Malathi, P., & Gireesh Kumar, T. (2020). A comprehensive survey on neural network based image data hiding scheme. *Proceedings of the 4th International Conference on IoT in Social, Mobile, Analytics and Cloud, ISMAC 2020*. https://doi.org/10.1109/I-SMAC49090.2020.9243579

Driss, M., Berriche, L., Atitallah, S. Ben, & Rekik, S. (2025). Steganography in IoT: A Comprehensive Survey on Approaches, Challenges, and Future Directions. *IEEE Access*, *13*. https://doi.org/10.1109/ACCESS.2025.3564120

Fratila, R., & Morogan, L. (2021). Enhanced models in deep image steganography. *Proceedings of the 13th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2021*. https://doi.org/10.1109/ECAI52376.2021.9515076

Gupta, P., & Bhagat, J. (2019). Image Steganography Using LSB Substitution Facilitated by Shared Password. In *Lecture Notes in Networks and Systems* (Vol. 55). https://doi.org/10.1007/978-981-13-2324-9_37

Han, C., & Xue, T. (2025). Adaptive network steganography using deep learning and multimedia video analysis for enhanced security and fidelity. *PLOS ONE*, *20*(6 JUNE). https://doi.org/10.1371/journal.pone.0318795

Hayes, J., & Danezis, G. (2017). Generating steganographic images via adversarial training. *Advances in Neural Information Processing Systems*, *2017-December*. https://doi.org/10.48550/arXiv.1703.00371

Johnson, N. F., Duric, Z., Jajodia, S., & Memon, N. (2001). Information Hiding: Steganography and Watermarking—Attacks and Countermeasures. *Journal of Electronic Imaging*, *10*(3). https://doi.org/10.1117/1.1388610

Kaur, N., & Behal, S. (2014). A Survey on various types of Steganography and Analysis of Hiding Techniques. *International Journal of Engineering Trends and Technology*, *11*(8). https://doi.org/10.14445/22315381/ijett-v11p276

Kumar, V., Sharma, S., Kumar, C., & Sahu, A. K. (2023). Latest Trends in Deep Learning Techniques for Image Steganography. *International Journal of Digital Crime and Forensics*, *15*(1). https://doi.org/10.4018/IJDCF.318666

Li, C., Xu, K., Zhu, J., & Zhang, B. (2017). Triple generative adversarial nets. *Advances in Neural Information Processing Systems*, *2017-December*. Retrieved from https://proceedings.neurips.cc/paper/2017/hash/86e78499eeb33fb9cac16b7555b50767-Abstract.html

Li, Z., Zhang, M., & Liu, J. (2021). Robust image steganography framework based on generative adversarial network. *Journal of Electronic Imaging*, *30*(02). https://doi.org/10.1117/1.jei.30.2.023006

Mstafa, R. J., & Elleithy, K. M. (2017). Compressed and raw video steganography techniques: a comprehensive survey and analysis. *Multimedia Tools and Applications*, *76*(20). https://doi.org/10.1007/s11042-016-4055-1

Neeta, D., Snehal, K., & Jacobs, D. (2006). Implementation of LSB steganography and its evaluation for various bits. *2006 1st International Conference on Digital Information Management, ICDIM*. https://doi.org/10.1109/ICDIM.2007.369349

Patel, F. R., & Cheeran A. N. (2015). Performance Evaluation of Steganography and AES encryption based on different formats of the Image. *IJARCCE*, *4*(5), 659-664. https://doi.org/10.17148/ijarcce.2015.45140

Raja Ratna, S., Shajilin Loret, J. B., Merlin Gethsy, D., Ponnu Krishnan, P., & Anand Prabu, P. (2020). A Review on Various Approaches in Video Steganography. In *Lecture Notes on Data Engineering and Communications Technologies* (Vol. 33). https://doi.org/10.1007/978-3-030-28364-3_64

Ramaneti, K., Kakani, P., Krishna, C., & Rajkumar, S. (2021). Image Steganography Using GANs. In *Studies in Computational Intelligence* (Vol. 985). https://doi.org/10.1007/978-3-030-79474-3_12

Ravichandran, C., Vajravelu, A., Panda, S., & Degadwala, S. D. (2024). Data hiding using video steganography. *International Journal of Electronic Security and Digital Forensics*, *16*(1). https://doi.org/10.1504/IJESDF.2024.136018

Sahu, A. K., & Sahu, M. (2020). Digital image steganography and steganalysis: A journey of the past three decades. *Open Computer Science*, Vol. 10. https://doi.org/10.1515/comp-2020-0136

Shaukat, A., Chaurasia, M., & Sanyal, G. (2016). A novel image steganographic technique using fast fourier transform. *2016 International Conference on Recent Trends in Information Technology, ICRTIT 2016*. https://doi.org/10.1109/ICRTIT.2016.7569519

Tushar Tikhe, Pranit Thorat, & Vivek Rodge. (2024). GAN-Based Steganography: Enhancing Data Concealment. *International Journal of Advanced Research in Science, Communication and Technology*. https://doi.org/10.48175/ijarsct-18546

Volkhonskiy, D., Nazarov, I., & Burnaev, E. (2020). *Steganographic generative adversarial networks*. https://doi.org/10.1117/12.2559429

Wang, Y., Yang, X., & Jin, H. (2020). Generative Image Steganography Based on GANs. *Communications in Computer and Information Science*, *1149 CCIS*. https://doi.org/10.1007/978-981-15-3418-8_1

Wu, N. I., & Hwang, M. S. (2007). Data hiding: Current status and key issues. *International Journal of Network Security*, *4*(1). Retrieved from http://ijns.jalaxy.com.tw/contents/ijns-v4-n1/ijns-2007-v4-n1-p1-9.pdf

Yang, J., Ruan, D., Huang, J., Kang, X., & Shi, Y. Q. (2020). An Embedding Cost Learning Framework Using GAN. *IEEE Transactions on Information Forensics and Security*, *15*. https://doi.org/10.1109/TIFS.2019.2922229

G Purnachandrarao
Department of Electronics and Communication Engineering,
BVRIT HYDERABAD College of Engineering for Women,
Hyderabad, India- 500090
pcrphd@gmail.com
ORCID 0000-0001-8680-5739

Bala Chandu Koya
Department of Civil Engineering,
B V Raju Institute of Technology,
Medak, India- 502313
balachandu.k@bvrit.ac.in
ORCID 0000-0002-8265-669X

Banala Saritha
Department of Electronics and Communication Engineering,
B V Raju Institute of Technology,
Medak, India- 502313
banalasarita@gmail.com
ORCID 0000-0002-6499-3561

Peddini Suresh Kumar Department of Electronics and Communication Engineering,
Aditya University, Surampalem,
Andhra Pradesh, India- 533437
sureshkumarp@adityauniversity.in
ORCID 0009-0002-5639-5032

Karimulla Syed Mohammad
Department of Engineering and Technology,
Electrical, Electronic and Computer Engineering,
University of Technology and Applied Sciences
Shinas, Shinas-324, Sultanate of Oman.
syedkarimullaanu@gmail.com
ORCID 0000-0002-6768-1352

Sainadh Singh Kshatri
Department of Electrical and Electronics Engineering,
B V Raju Institute of Technology,
Medak, India- 502313
sainadhsingh@gmail.com
ORCID 0000-0003-2357-0180