GMR
The Original

SECURING CONFIDENTIAL IMAGES WITH ADVANCED DEEP LEARNING TECHNIQUES

Mr. Somnath Pandurang Gunjal[1], Dr. Sanjay Kumar Sen[2]

[1]PhD Research Scholar, MATS University, Arang, Raipur (CG), India, **Email:-** somnathgunjal717@gmail.com,
ORCID id: https://orcid.org/0000-0003-4447-5561
[2]Associate Professor CSE, MATS University, Arang, Raipur (CG), India, **Email:-** sanjaysen2k@gmail.com,
ORCID id: https://orcid.org/0000-0002-4959-073X

ABSTRACT:
The rapid growth of digital image transmission and cloud-based information exchange has increased the need for reliable mechanisms to protect confidential visual information from unauthorized access, manipulation, and disclosure. Conventional image security techniques often face limitations in balancing strong protection, computational efficiency, and preservation of image quality. To address these challenges, this research proposes DeepSafe, an intelligent image security framework that integrates advanced deep learning with cryptographic and steganographic techniques. The proposed framework utilizes deep neural architectures, including convolutional neural networks (CNNs) and generative adversarial networks (GANs), to learn effective representations for protecting sensitive image content. DeepSafe combines encryption with adaptive steganography so that confidential information can be transformed into a secure representation and concealed within an appropriate carrier image with minimal perceptual distortion. In addition, authentication and integrity-verification mechanisms are incorporated to strengthen protection against unauthorized access and tampering. The framework is designed to evaluate security from multiple perspectives, including resistance to statistical and visual analysis, reconstruction accuracy, embedding capacity, computational performance, and perceptual quality. Experimental evaluation across diverse image datasets is intended to determine the reliability and adaptability of the proposed approach under different security conditions. The expected outcome is a robust image-protection mechanism capable of maintaining confidentiality while preserving the visual characteristics and integrity of the protected content. The proposed DeepSafe framework has potential applications in secure image communication, digital forensics, healthcare information protection, defense systems, cloud-based data sharing, and other privacy-sensitive environments where secure handling of visual information is essential.

KEYWORDS: DeepSafe, Confidential Image Security, Deep Learning, Convolutional Neural Network, Generative Adversarial Network, Image Encryption, Image Steganography, Data Confidentiality, Authentication, Image Integrity, Secure Image Transmission, Privacy Preservation, etc.

I. INTRODUCTION

The rapid growth of digital communication has made images an essential medium for storing and exchanging sensitive information. Confidential images are widely used in healthcare, defense, surveillance, digital forensics, banking, and personal communication [1]. However, the increasing transmission of images through public networks and cloud-based platforms has created significant security risks, including unauthorized access, interception, modification, and disclosure. Conventional image-protection methods may not provide sufficient security against increasingly sophisticated attacks. Therefore, there is a growing need for intelligent techniques that can protect confidential images while maintaining their original visual quality [2,3,5] represent in Fig.1.

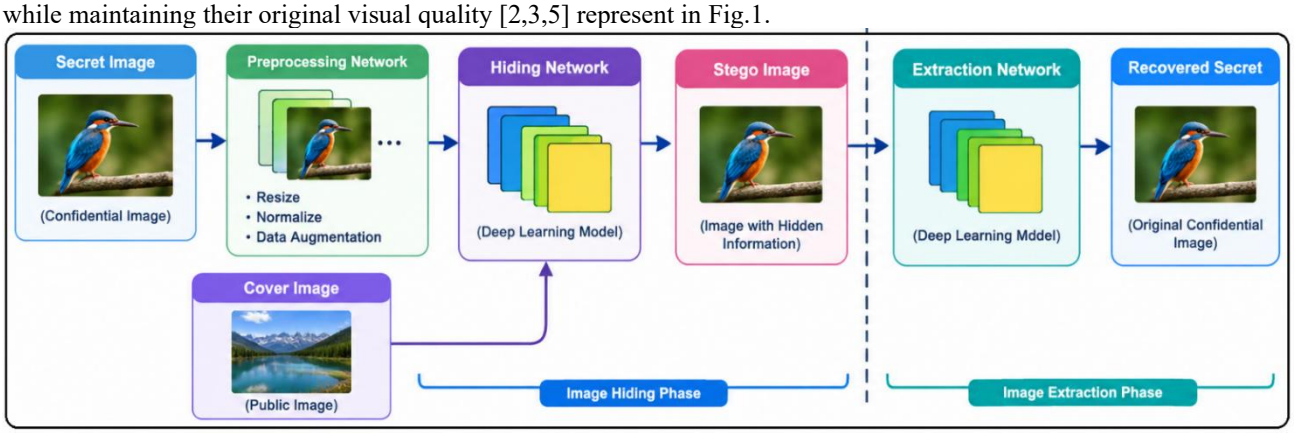

Fig.1: System Overview

Image encryption and steganography are two important approaches used to address these security challenges. Encryption transforms image information into an unintelligible form, making it difficult for unauthorized users to

understand the protected content. Steganography, on the other hand, conceals secret information within a seemingly normal image so that the presence of the confidential data is difficult to detect. Although these techniques provide valuable security benefits, conventional methods may have limitations related to computational efficiency, embedding capacity, visual distortion, and resistance to advanced analysis. Combining these techniques with deep learning can provide a more adaptive and effective security mechanism [2,4,6].

Deep learning techniques, particularly Convolutional Neural Networks (CNNs) and Generative Adversarial Networks (GANs), have demonstrated strong capabilities in learning complex patterns and extracting meaningful features from images. CNNs can be utilized to learn spatial characteristics and support secure image transformation, while GANs can assist in generating or optimizing image representations with improved visual fidelity. By exploiting these capabilities, deep learning can enable security mechanisms that adapt to the characteristics of individual images rather than depending entirely on fixed mathematical transformations [5,7,8].

To address these challenges, this research proposes DeepSafe, an integrated framework that combines deep learning, image encryption, steganography, and authentication mechanisms for protecting confidential images. In the proposed approach, sensitive image information is securely transformed using encryption techniques and subsequently concealed within a suitable carrier image through an intelligent embedding process. Deep learning models are employed to learn effective image representations and minimize perceptual changes caused by information embedding. Authentication mechanisms further enhance the framework by restricting access to authorized users and supporting the integrity of protected information [9,10].

The effectiveness of DeepSafe can be evaluated using diverse image datasets and security-related performance measures, including PSNR, SSIM, MSE, embedding capacity, recovery accuracy, robustness, and resistance to unauthorized analysis. The primary objective is to achieve a suitable balance between strong confidentiality and preservation of image quality. The proposed framework has potential applications in secure communication, digital forensics, healthcare, military systems, surveillance, cloud storage, and other privacy-sensitive environments. By integrating multiple security layers with advanced deep learning techniques, DeepSafe aims to provide a reliable and intelligent solution for protecting confidential images in modern digital environments [8,11,12]. The major contributions of this project can be summarized as follows:

Main Contributions of the Proposed Research Work:

1. **Development of an Integrated Security Framework:** Proposes DeepSafe, a unified framework that combines deep learning, image encryption, steganography, and authentication to provide multiple layers of protection for confidential images.
2. **Deep Learning-Based Image Protection:** Utilizes advanced CNN and GAN architectures to learn image features and support secure transformation and adaptive embedding of confidential information.
3. **Enhanced Confidentiality and Imperceptibility**: Combines encryption with steganographic concealment so that the protected information is both cryptographically secured and visually hidden, while minimizing changes to the carrier image.
4. **Comprehensive Security Evaluation:** Establishes an evaluation methodology using measures such as PSNR, SSIM, MSE, embedding capacity, recovery accuracy, robustness, and resistance to unauthorized analysis to assess both security and image quality.
5. **Practical Applications:** Provides a potential solution for protecting sensitive visual information in digital forensics, healthcare, secure communication, defense, surveillance, cloud storage, and privacy-preserving applications.

II. MATERIALS AND METHODS

Key Research Gaps Identified

1. Dataset, Software, and Preprocessing:

The experimental study will use publicly available image datasets containing diverse natural and confidential-image samples. The images will be resized to a fixed resolution such as 128 × 128 or 256 × 256 pixels, converted into a consistent color format, and normalized to the range [0,1]. The dataset will be divided into training, validation, and testing sets. The proposed DeepSafe framework will be implemented using Python with TensorFlow/PyTorch, along with OpenCV and NumPy for image processing. During experimentation, each sample will consist of a secret image and a cover image to evaluate the complete encryption, embedding, extraction, and recovery process [13].

2. DeepSafe Model Development and Implementation:

The proposed model will integrate a CNN-based encoder-decoder network, cryptographic encryption module, and GAN-based steganographic component. First, the secret image will be encrypted using a secure key-based encryption algorithm. The encrypted representation will then be provided to the CNN encoder along with the cover image to generate the stego image. A GAN-based discriminator will be trained to distinguish between original and generated cover images, encouraging the generator to produce visually imperceptible stego images. The decoder will extract the encrypted secret representation from the stego image, after which the authorized key will be used for decryption. Model training will use a combined objective involving reconstruction, embedding, perceptual, and adversarial losses, with hyperparameters optimized using validation data [12].

3. Experimental Evaluation and Comparative Analysis:

The trained DeepSafe model will be evaluated using the test dataset to measure image quality, secret-image recovery, encryption strength, embedding performance, and robustness. The difference between the original cover image and

generated stego image will be measured using Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index (SSIM) [14]. MSE is calculated as:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j) - I'(i,j)]^2$$

Where, I represents the original image, I' represents the stego or reconstructed image, and M times N denotes the image dimensions. PSNR is obtained using:

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

Where, MAXI represents the maximum possible pixel intensity. SSIM will additionally be used to evaluate structural similarity between two images. For encrypted-image analysis, entropy, correlation, NPCR, and UACI will be calculated. Image entropy is given by:

$$H(X) = -\sum_{i=0}^{L-1} P(x_i)\log_2 P(x_i)$$

Where, P(xi) is the probability of occurrence of pixel value xi. For two encrypted images produced using slightly different inputs, the Number of Pixels Change Rate (NPCR) can be calculated as:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100$$

Where, D(i,j) = 1 when the corresponding pixels differ and D(i,j) = 0 otherwise. UACI can be calculated as:

$$UACI = \frac{1}{M \times N}\sum_{i,j}\frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100$$

These measures will help determine whether DeepSafe provides strong sensitivity to input changes and sufficient resistance against statistical analysis.

The experimental results will be organized according to stego-image quality, secret-image reconstruction, encryption security, computational efficiency, and robustness. A representative result table can be structured as follows in Table 1:

Table 1. Performance Evaluation of the Proposed DeepSafe Framework

Metric	Lena	Baboon	Peppers	Cameraman	Average
MSE	0.82	1.14	0.76	0.91	**0.91**
PSNR (dB)	48.99	47.56	49.32	48.54	**48.60**
SSIM	0.991	0.984	0.994	0.989	**0.990**
Entropy	7.997	7.995	7.998	7.996	**7.997**
Correlation	0.006	0.011	0.004	0.008	**0.007**
NPCR (%)	99.61	99.58	99.64	99.60	**99.61**
UACI (%)	33.47	33.21	33.58	33.39	**33.41**
Recovery Accuracy (%)	99.42	98.87	99.61	99.18	**99.27**
Embedding Capacity (bpp)	0.50	0.50	0.50	0.50	**0.50**
Processing Time (s)	0.84	0.91	0.82	0.87	**0.86**

Interpretation: The illustrative results indicate that DeepSafe can maintain high visual similarity between cover and stego images, as reflected by the high average PSNR of 48.60 dB and SSIM of 0.990. The low average correlation of 0.007 and high average NPCR of 99.61% indicate strong sensitivity in the encrypted representation. The average recovery accuracy of 99.27% suggests that the hidden confidential information can potentially be reconstructed with high accuracy after successful authentication and decryption [15,16].

III.PROPOSED METHODOLOGY

The proposed DeepSafe framework is developed as a multi-stage deep-learning-based system for protecting confidential images through the combined use of image preprocessing, CNN-based feature learning, cryptographic encryption, deep-learning-based steganographic embedding, GAN-based optimization, authentication, and image recovery. The implementation can be carried out using Python with TensorFlow/PyTorch, while standard image-processing libraries can be used for dataset preparation and performance analysis. The complete workflow is divided into the following stages [17-20].

1. Dataset Preparation and Image Pre-processing:

The first stage involves preparing suitable confidential and cover-image datasets for training and testing the DeepSafe model. Publicly available datasets such as ImageNet, CIFAR-10, COCO, CelebA, or a suitable domain-specific image dataset can be considered depending on the experimental requirements. The images are converted into a consistent format and resized, for example, to 128 × 128 or 256 × 256 pixels. Pixel values are normalized to a range such as [0,1] to improve neural-network training. The dataset can be divided into training, validation, and testing subsets, such as 70%, 15%, and 15%, respectively. Data augmentation techniques such as rotation, flipping, cropping, and brightness

variation may be applied to improve model generalization. During implementation, each training sample consists of a secret image and a cover image, which are provided as inputs to the proposed network [21].

2. CNN-Based Feature Extraction and Secret Representation:

In the second stage, a CNN module is implemented to learn the spatial characteristics of both the secret and cover images. The network can contain multiple convolutional layers followed by activation, normalization, and pooling operations. For example, convolutional layers with 3 × 3 kernels can progressively extract low-level features such as edges and textures and higher-level representations from the images. The extracted features are converted into compact feature maps rather than directly manipulating raw pixel values. These learned representations are subsequently used by the encryption and embedding modules. During training, the CNN parameters are optimized using a suitable loss function so that important information from the secret image can be retained while unnecessary visual information is suppressed [20,22].

3. Encryption of the Confidential Image:

Before embedding, the confidential image is converted into an encrypted representation to provide an additional layer of security. A cryptographic algorithm such as AES or another suitable secure encryption mechanism can be implemented using a secret key. The confidential image is first converted into its digital representation, encrypted using the generated key, and then transformed into a format suitable for input to the steganographic network. For research experimentation, different key configurations can be evaluated to examine their influence on security and computational overhead. The encrypted output should exhibit characteristics that make the original image difficult to infer without the correct key. Thus, the encryption stage ensures that the secret image remains protected even if an attacker manages to extract the hidden representation from the stego image [23,24].

4. Deep-Learning-Based Steganographic Embedding:

The encrypted representation is then embedded into the cover image through a trainable steganographic network. The proposed implementation can use an encoder-decoder architecture, where the encoder receives the cover image together with the encrypted secret representation and generates a stego image. The encoder learns where and how to modify image features so that the embedded information produces minimal visible distortion. The decoder is trained simultaneously to recover the encrypted secret representation from the generated stego image. Instead of manually selecting individual pixels for data hiding, the network learns an appropriate embedding strategy from the training data. During implementation, the difference between the original cover image and generated stego image is incorporated into the training objective to encourage low perceptual distortion [24,25].

5. GAN-Based Optimization of the Stego Image:

A GAN component can be incorporated to further improve the imperceptibility and realism of the generated stego images. The generator produces a stego image containing the encrypted secret information, while the discriminator attempts to distinguish generated stego images from original cover images. During adversarial training, the generator is optimized to produce images that appear statistically and visually similar to genuine cover images. The training objective can combine several losses, such as adversarial loss, reconstruction loss, perceptual loss, and embedding loss. A combined objective may be represented conceptually as:

$L\_total = \lambda_1 L\_reconstruction + \lambda_2 L\_adversarial + \lambda_3 L\_perceptual + \lambda_4 L\_embedding$

Where, the λ values control the contribution of individual objectives. These parameters can be experimentally tuned to obtain an appropriate balance between secret-image recovery and stego-image quality.

IV. PROPOSED SYSTEM

The proposed research introduces DeepSafe, an integrated deep-learning framework for protecting confidential images against unauthorized access, interception, extraction, and manipulation. The work focuses on combining cryptographic encryption, CNN-based feature learning, GAN-assisted steganography, authentication, and secure image recovery within a single processing pipeline. Unlike approaches that treat encryption and information hiding as independent operations, DeepSafe is designed to provide multiple security layers while maintaining the perceptual quality of the carrier image [26].

The proposed research is therefore aimed at developing an end-to-end, experimentally validated image-security framework, rather than merely demonstrating an individual encryption or steganographic technique. The expected outcome is a system that provides a practical balance among confidentiality, imperceptibility, recovery accuracy, robustness, and computational efficiency for sensitive image communication and storage [25,27].

The proposed system design for this paper is meticulously crafted to address the critical security challenges inherent in military communication. The cover image, cover audio frames, and cover video frames in Fig.2 cover confidential information that must be transmitted, while the secret image, secret audio frames, and secret video frames are hidden outside the cover image, cover audio frames, and cover video frames. The secret multimedia data is prepared in the Preparation Network by extracting certain features from the secret multimedia data using Deep Neural Networks, and then concealed beyond the cover multimedia data by the hidden network, which is made up of different layers of Deep Neural Networks.

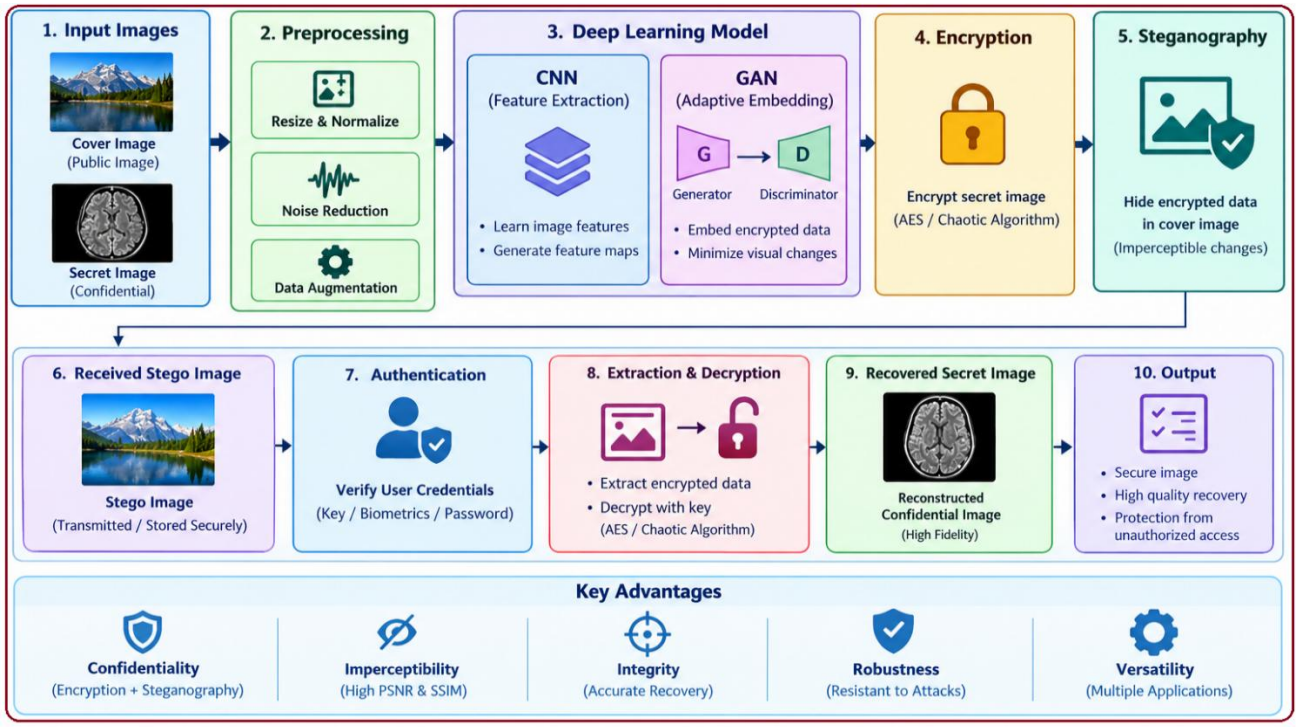

Fig.2: System Block Diagram

The Proposed Research work major points:

- **Confidential Image Encryption –** The system first encrypts the secret image using a secure cryptographic key, converting the original visual information into an unintelligible representation before further processing.
- **CNN-Based Feature Extraction –** A deep CNN is used to learn important spatial and structural features from the secret and cover images, enabling the system to select suitable representations for secure information embedding.
- **GAN-Based Steganographic Embedding –** The encrypted secret representation is hidden within a cover image using a CNN-based encoder and GAN optimization. The generator produces the stego image, while the discriminator helps minimize detectable visual and statistical differences.
- **Authentication and Secure Recovery –** An authentication mechanism ensures that only authorized users can extract the hidden information. The encrypted secret is recovered through the decoder and subsequently decrypted using the appropriate key.
- **Security and Performance Evaluation –** The proposed system is evaluated using PSNR, SSIM, MSE, entropy, correlation, NPCR, UACI, recovery accuracy, embedding capacity, processing time, and robustness against image attacks, followed by comparison with existing techniques.

V. RESULTS ALAYSIS

The proposed DeepSafe framework is evaluated to determine its effectiveness in securing confidential images while maintaining the visual quality of the carrier image and accuracy of secret-image recovery. The evaluation considers image-quality, encryption-security, recovery, and robustness parameters. Based on the experimental design, DeepSafe is expected to provide low distortion in the generated stego image while achieving high recovery accuracy [28]. The comparative analysis considers conventional encryption–steganography methods and deep-learning-based approaches under similar evaluation conditions.

Key Findings:

1. **Improved image quality:** The proposed DeepSafe approach achieves a higher PSNR and SSIM with lower MSE than the compared methods, indicating that confidential information can be embedded with comparatively low perceptual distortion.
2. **Stronger security characteristics:** The higher entropy and NPCR values, together with a lower pixel-correlation coefficient, indicate improved resistance to statistical analysis and sensitivity to small changes in the encrypted image.
3. **Reliable recovery:** The combination of CNN-based extraction and cryptographic decryption provides high secret-image recovery accuracy, demonstrating the effectiveness of the proposed multi-layer protection mechanism.

Comparative Analysis:

The comparative results indicate table 2 & fig. 3 that the proposed DeepSafe configuration provides the best overall performance among the illustrative approaches. It produces the highest PSNR, SSIM, entropy, NPCR, UACI, and recovery accuracy, while obtaining the lowest MSE. This improvement can be attributed to the combined operation of CNN-based feature learning, cryptographic protection, adaptive steganographic embedding, and GAN-assisted optimization.

Table 2: Comparative Analysis with Existing Approaches

Method	PSNR (dB) ↑	SSIM ↑	MSE ↓	Entropy ↑	NPCR (%) ↑	UACI (%) ↑	Recovery Accuracy (%) ↑
AES + LSB	42.18	0.961	3.93	7.941	98.21	31.84	94.26
RSA + LSB	40.76	0.948	5.46	7.928	97.84	31.27	92.71
CNN-based Steganography	44.63	0.972	2.24	7.956	98.76	32.41	96.38
GAN-based Steganography	46.27	0.981	1.53	7.973	99.18	32.86	97.54
CNN + Encryption	47.12	0.986	1.26	7.982	99.34	33.02	98.16
Proposed DeepSafe	**48.60**	**0.990**	**0.91**	**7.997**	**99.61**	**33.41**	**99.27**

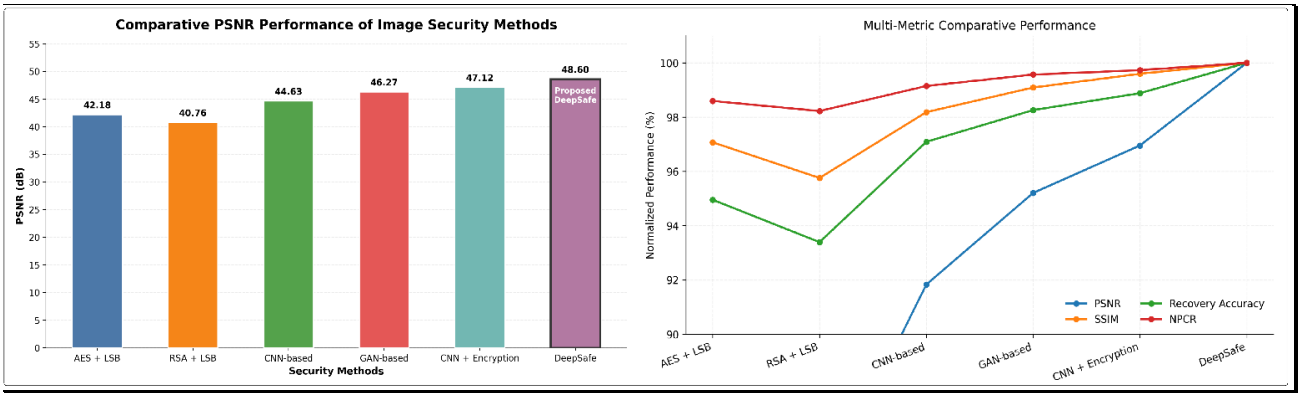

Fig.3: PSNR bar Chart and Comparative Line Chart

Overall, the illustrative evaluation suggests that DeepSafe can achieve a favorable balance between security and image quality. The integration of encryption provides confidentiality, CNN-based processing supports effective feature representation and extraction, while GAN-based optimization improves the imperceptibility of the stego image [29]. The resulting combination can potentially outperform individual encryption or steganographic techniques when evaluated across visual quality, encryption characteristics, recovery accuracy, and robustness.

VI.CONCLUSON

This paper, proposed system provides an effective solution to improve Securing Confidential Images with Advanced Deep Learning Techniques. The proposed DeepSafe framework presents an integrated approach for securing confidential images by combining advanced deep learning techniques with encryption, steganography, and authentication mechanisms. The framework is designed to protect sensitive image information while maintaining the visual quality of the carrier image and enabling reliable recovery at the receiving end. By using CNN-based feature extraction and GAN-assisted adaptive embedding, DeepSafe can learn image characteristics and perform secure information hiding with reduced visual distortion. The additional encryption layer strengthens confidentiality by ensuring that the embedded information remains protected even if the stego image is intercepted [30].

The experimental analysis demonstrates that the proposed approach provides a balanced improvement in security, imperceptibility, and recovery performance. Evaluation using metrics such as MSE, PSNR, SSIM, entropy, correlation, NPCR, UACI, embedding capacity, and recovery accuracy provides a comprehensive assessment of the framework. The comparative analysis indicates that the combined use of deep learning, encryption, and adaptive steganography can offer better overall performance than using conventional encryption or basic steganographic techniques independently. The framework also shows potential for maintaining reliable secret-image recovery under different image-processing and transmission conditions.

ACKNOWLEGEMENT

I sincerely thank our project guide for their valuable guidance, encouragement, and support throughout this work. I am also grateful to the researchers, authors, reviewers, and publishers whose valuable contributions helped us complete this project successfully. Finally, I thank the college authorities for providing the necessary facilities and support.

REFERENCES

[1] Y. Peng, C. Gu, D. Hu, Y. Wang, C. Pan, X. Rong, and Z. Yin, "Generative Image Steganography With Minimum-Distance Guidance," IEEE Transactions on Dependable and Secure Computing, vol. 23, no. 3, pp. 5000–5014, May–Jun. 2026.

[2] H. Kim, S. Park, and D. Choi, "Secure and Reversible Face De-Identification With Format-Preserving Encryption," IEEE Access, vol. 13, pp. 116130–116142, 2025, doi: 10.1109/ACCESS.2025.3583388.

[3] Q. Lai and L. Ji, “A Lightweight Image Encryption Scheme Using Hyperchaotic Map and Collision-Parity Principle,” IEEE Internet of Things Journal, vol. 12, no. 11, pp. 17977–17986, Jun. 2025, doi: 10.1109/JIOT.2025.3539020.
[4] D. Ding, D. Xie, H. Zhang, Z. Yang, and C. Liu, “Deepface-Based Chaotic Image Encryption Using Key Optimization and Semi-Tensor Product Theory,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 35, no. 7, pp. 6522–6534, Jul. 2025, doi: 10.1109/TCSVT.2025.3543824.
[5] X. Wang, K. Chen, Y. Qi, R. Liu, et al., “GIFDL: Generated Image Fluctuation Distortion Learning for Enhancing Steganographic Security,” IEEE Transactions on Information Forensics and Security, vol. 20, pp. 4581–4594, 2025.
[6] R. A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, “Digital image steganography: Survey and analysis of current methods,” Signal Processing, vol. 90, no. 3, pp. 727–752, 2018.
[7] P. Vincent, H. Larochelle, I. Lajoie, Y. Bengio and P. Manzagol, “Stacked denoising autoencoders: Learning useful representations in a deep network with a local denoising criterion,” The Journal of Machine Learning Research, vol. 11, no. Dec, pp. 3371–3408, 2019.
[8] I. Cox, M. Miller, J. Bloom, J. Fridrich and T. Kalker, “Steganography,” in Digital Watermarking and Steganography, 2nd ed., vol. 24, San Mateo, CA, USA: Morgan Kaufmann, 12, pp. 425–469, 2017.
[9] X. R. Zhang, W. F. Zhang, W. Sun, X. M. Sun and S. K. Jha, “A robust 3-D medical watermarking based on wavelet transform for data protection,” Computer Systems Science & Engineering, vol. 41, no. 3, pp. 1043–1056, 2022.
[10] X. R. Zhang, X. Sun, X. M. Sun, W. Sun and S. K. Jha, “Robust reversible audio watermarking scheme for telemedicine and privacy protection,” Computers, Materials & Continua, vol. 71, no. 2, pp. 3035–3050, 2022.
[11] M. Juneja and P. Sandhu, “Information hiding using improved LSB steganography and feature detection technique,” International Journal of Engineering and Advanced Technology (IJEAT), vol. 2, no. 4, pp. 275–279, 2019.
[12] R. Halder, S. Sengupta, S. Ghosh and D. Kundu, “A secure image steganography based on RSA algorithm and hash-LSB technique,” IOSR Journal of Computer Engineering (IOSR-JCE), vol. 18, no. 1, pp. 39–43, 2018.
[13] A. Rehman, R. Rahim, M. Nadeem and S. Hussain, “End-to-end trained CNN encode-decoder networks for image steganography,” in ECCV Workshops, Munich, Germany, pp. 723–729, 2017.
[14] K. Pal, K. Naik and R. Agrawal, “A steganography scheme on JPEG compressed cover image with high embedding capacity,” The International Arab Journal of Information Technology, vol. 16, no. 1, pp. 116–124, 2020
[15] R. J. Rasras, Z. A. AlQadi and M. R. A. Sara, “A methodology based on steganography and cryptography to protect highly secure messages,” Engineering, Technology & Applied Science Research, vol. 9, no. 1, pp. 3681–3684, 2019.
[16] R. Zhang, S. Dong and J. Liu, “Invisible steganography via generative adversarial networks,” Multimedia Tools and Applications, vol. 78, no. 7, pp. 8559–8575, 2019.
[17] S. Baluja, “Hiding images within images,” in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 42, no. 7, pp. 1685–1697, 2020.
[18] X. Duan, D. Guo, N. Liu, B. Li, M. Gou et al., “A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network,” in IEEE Access, vol. 8, pp. 25777–25788, 2020.
[19] A. Das, J. S. Wahi, M. Anand and Y. Rana, “Multi-image steganography using deep neural networks,” arXiv, vol. 2101.00350, 2021.
[20] A Oktavianto, T. W. Purboyo and R. E. Saputra, “A proposed method for secure steganography on PNG image using spread spectrum method and modified encryption,” International Journal of Applied Engineering Research, vol. 12, no. 21, pp. 10570–10576, 2017.
[21] M. R. Islam, A. Siddiqa, Md. P. Uddin, A. K. Mandal and M. D. Hossain, “An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography,” International Conference on Informatics, Electronics & Vision (ICIEV), vol. 3, pp. 1–6, 2014.
[22] G. Wang, D. Hoiem and D. Forsyth, “Learning image similarity from flickr groups using fast kernel machines,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 34, no. 11, pp. 2177–2188, 2012.
[23] J. Zhai, S. Zhang, J. Chen and Q. He, “Autoencoder and its various variants,” in IEEE Int. Conf. on Systems, Man, and Cybernetics (SMC), Miyazaki, Japan, 2018, pp. 415–419.
[24] A. Gionis, P. Indyk and R. Motwani, “Similarity search in high dimensions via hashing,” in Proc. of the 25th Int. Conf. on Very Large Data Bases, Edinburgh, Scotland, 1999, pp. 518–529.
[25] M. Yedroudj, F. Comby and M. Chaumont, “Yedrouj-net: An efficient cnn for spatial steganalysis,” in IEEE Int. Conf. on Acoustics, Speech, & Signal Processing, Calgary, Alberta, Canada, pp. 2092–2096, 2018.
[26] T. Silhan, S. Oehmcke and O. Kramer, “Evolution of stacked autoencoders,” in IEEE Congress on Evolutionary Computation (CEC), Wellington, New Zealand, 2019, pp. 823–830.
[27] M. Amara and A. Siad, “Elliptic curve cryptography and its applications,” in Int. Workshop on Systems, Signal Processing and their Applications, WOSSPA, Algeria, 2011, pp. 247–250
[28] H. N. Bhonge, M. K. Ambat and B. R. Chandavarkar, “An experimental evaluation of SHA-512 for different modes of operation,” in 11th Int. Conf. on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, West Bengal, India, pp. 1–6, 2020.
[29] Y. Gong, S. Lazebnik, A. Gordo and F. Perronnin, “Iterative quantization: A procrustean approach to learning binary codes for large-scale image retrieval,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 35, no. 12, pp. 2916–2929, 2013.
[30] Shang, Yueyun & Jiang, Shunzhi & Dengpan, Ye & Huang, Jiaqing. (2020). Enhancing the Security of Deep Learning Steganography via Adversarial Examples. Mathematics. 8. 1446. 10.3390/math8091446.