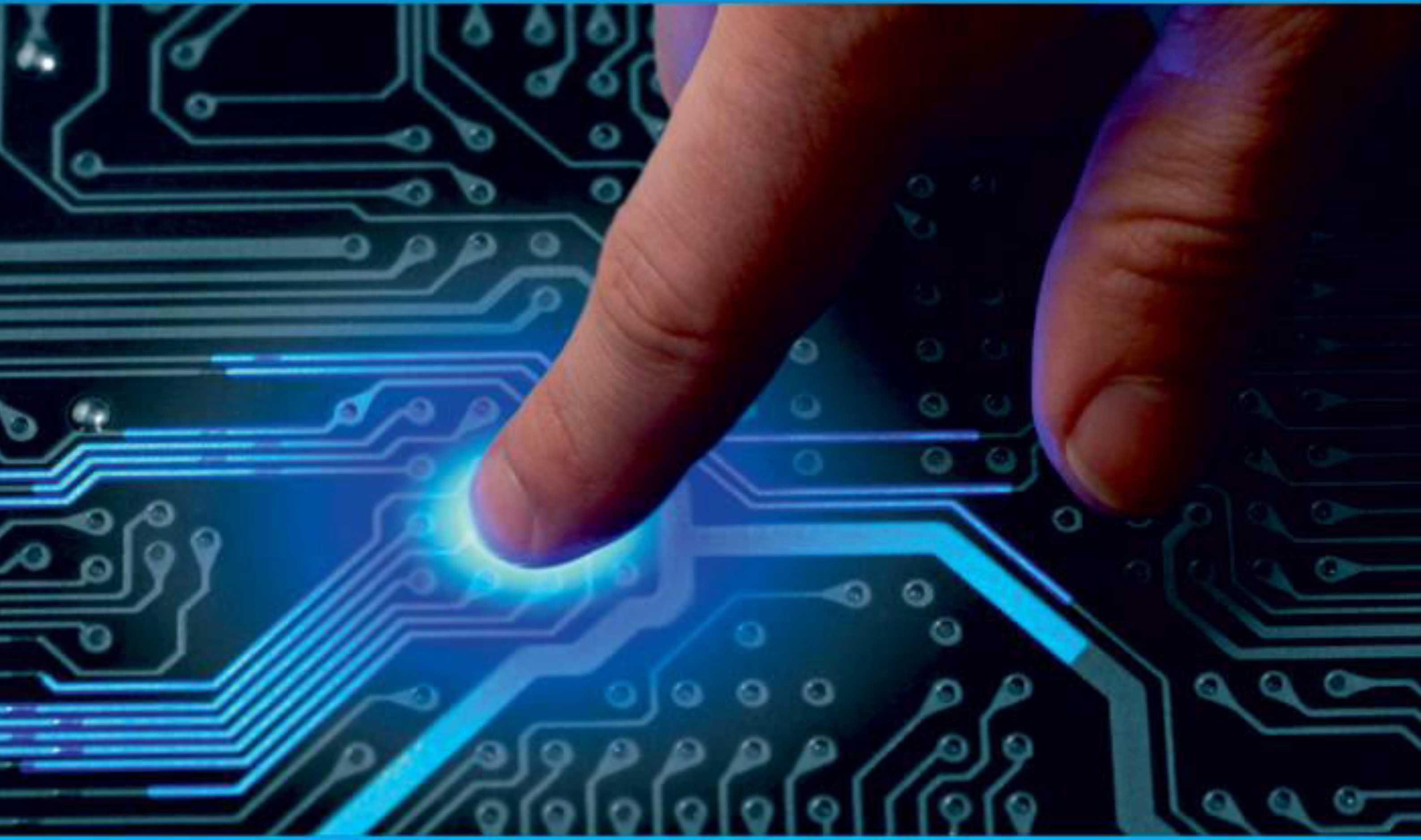
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 6, June 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

| DOI: 10.15680/IJIRCCE.2023.1206018 |

Steganography Information Sharing Via AI Generated Images

Satish D. Kale, Piyush Manish Pawar, Girish Vikas Patil, Parth Vitekar, Harshwardhan Salunkhe

Department of Artificial Intelligence & Data Science, Savitribai Phule Pune University, India

ABSTRACT: Image steganography is the technique of concealing data text, pictures, & videos within a cover image. The confidential data is concealed so that it is not apparent to the naked eye. Recently, there has been a greater focus on deep learning, which has shown promise as a potent tool in a variety of applications, including image steganography. The three main kinds of deep learning approaches for picture steganography are: conventional methods, methods based on convolutional neural networks, and methods based on generative adversarial networks. This paper's primary objective is to examine and talk about the many deep learning techniques used in the field of picture steganography.

Keywords: steganography, confidential data, deep learning, convolutional neural networks, generative adversarial networks

I. INTRODUCTION

In recent years, the rapid development of technology has led to the widespread use of multimedia, especially in the context of information transmission through the Internet of Things (IoT). These transmissions often occur over secure network connections, and the Internet has become a popular medium for exchanging digital media between individuals, businesses, organizations, and governments. Despite the many benefits offered by sharing multimedia data, data security and privacy issues remain significant drawbacks. The proliferation of more accessible technologies has increased the risk of adversary attacks, eavesdropping, and other malicious activities that can compromise the confidentiality, integrity, and security of transmitted data.

To solve this problem, data encryption has emerged as a popular approach, where the data is converted into ciphertext using the encryption key and then decrypted in the clear using the encryption key at the receiver's end. Multimedia data such as text, files, videos and images can be encoded using this method [1]. Unlike cryptography, which focuses on hiding data content, steganography includes hiding one image inside another, hiding the presence of hidden information, and manipulating the cover image to make it less visible. On the other hand, Steganalysis, hidden information detection and extraction, is encrypted using hidden messages contained in multimedia data, including text, files, video, and image data [2].

Deep learning techniques (DL), convolutional neural networks (CNN) and artificial adversarial networks (GAN) have gained popularity due to the large amount of data and their effectiveness in various applications such as imaging, automatic word recognition, and natural language. processing, consultation system and medical image processing. While steganography research is still in its infancy, DL techniques have shown promise in steganography and steganalysis.

The main purpose of this article is to evaluate existing approaches, identify trends, and discuss current challenges in steganography research. This study is accompanied by a discussion of evaluation criteria, widely used databases, and the strengths and weaknesses of different methodologies. In addition, comparing their performance and identifying potential research gaps are provided to guide future research.

II. LITERATURE SURVEY

Research Paper Title	Year of Publication & Authors	Methodology Adapted	Major Findings
1. Information Hiding using Steganography	Ritu Sindhu, Pragati Singh Volume-9 Issue-4, April, 2023	Bitmap steganography involves hiding data within bitmap images. Convert the secret message to binary and embed into the image's least	Bitmap steganography hides data within image LSBs, producing visually unchanged

		significant bits (LSB). The altered bitmap, visually unchanged, carries the hidden message. For extraction, recipients retrieve the LSBs and revert to the original message format	carriers; extraction involves retrieving these LSBs to reveal the original message
2. Image Steganography Techniques - A Review Paper	Mohammed A. Saleh Vol. 7, Issue 9, September 2022	The message is expressed in 6 binary bits using LSBraille method, rather than ASCII format. Three message's bits are embedded in one pixel.	efficient encoding and concealment of information within an image's blue and green channels, optimizing steganographic practices for data hiding.
3. Steganographic secret sharing via AI-generated photorealistic images	Kai Gao , Ching-Chun Chang2, Ji-Hwei Horng and Isao Echizen 2021	sharing, utilizing a CNN, generator, and encoder for creating photorealistic image shares, with an authentication mechanism ensuring share authenticity. Experiments were conducted in PyTorch 1.7, leveraging an NVIDIA RTX 3090 GPU.	enhanced security by combining coverless steganography with secret sharing and uses CNN-based authentication for verifying image share authenticity, optimized for performance with advanced GPUs.
4. A Survey Paper on Steganography Techniques	Dr. Rajkumar L Biradar, Ambika Umashetty Vol. 4 , Issue 1, January 2020	Using a stego-key pattern, the LSB-based method modifies pixel LSBs for data hiding, employing Pixel Value Difference and Multi-Pixel Differencing to adaptively embed data and assess pixel smoothness.	enhanced data hiding in images, optimizing concealment by adaptively embedding information based on pixel smoothness, ensuring both security and minimal visual distortion.

III. METHODS OF STEGANOGRAPHY

3.1.1 TRADITIONAL METHODS

DATASET	METRICS	ADVANTAGES	DISADVANTAGES
RGB image	Peak Signal-to-Noise Ratio (PSNR).	- Reduced computational time - Effective in both embedding and extraction processes - The integration of steganalysis and steganography can function independently	- Reduced level of security - Textual information serves as the secret content
Lena & Baboon	Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE).	- Reduced computation time required - The secret message is concealed within an image - Various image formats are supported indiscriminately	- Security measures fall short when compared to deep learning approaches.
Lena	Peak Signal-to-Noise Ratio	- Reduced computational time required - An image serves as the concealed	- Lower level of security

		message	

3.1.2 CNN BASED METHODS

DATASET	ARCHITECTURE	ADVANTAGES	DISADVANTAGES
ImageNet	Encoder-Decoder	- The image functions as the covert message.	- Nevertheless, the image size is merely 64 bits, which is considerably small.
ImageNet	U-Net	- The image functions as the covert message. - Foundational architecture employed	- However, the image size is only 64 bits, which is notably small.
COCO, wikiart.org	Encoder-decoder with Visual Geometry Group base	-No domain knowledge is necessary. - The security is high since the generated image is unrelated to the secret information.	- The computation is heightened with the inclusion of an additional image.
ImageNet, Holiday	Convolutional Neural Network.	- The image serves as the secret message, employing a basic architecture. - Incorporating new error backpropagation techniques accelerates training.	-The input images are simply concatenated. -However, the image size remains very small at 64 bits.
ImageNet	Encoder-Decoder with Semantic Compression Ratio (SCR).	- Offers high levels of security and robustness.	- The employed loss function is suboptimal. - Visible noise may appear in black or white regions.

3.1.3 GAN BASED METHODS

DATASET	ARCHITECTURE	ADVANTAGES	DISADVANTAGES
BOSSbase, celebA	Alice, Bob and Eve	- No specialized domain knowledge is necessary.	- Messages are utilized instead of images.
MNIST, celebA	Information Maximizing Generative Adversarial Network.	- Enhanced security through the addition of an extraction key alongside the cover image.	- The message is encrypted using the cover image, providing a public and less private approach.
CelebA, BOSSBase	Deep Convolutional Generative Adversarial Network.	-game-theoretic formulation is employed.	-Incorporation of three components akin to a steganalyzer.
Modified National Institute of Standards and Technology	Auxiliary Classifier Generative Adversarial Network.	-Exceptionally secure and resilient, boasting augmented hiding capacity.	-Intricate design tailored for concealing confidential information.
University of Southern California Signal and Image Processing	Cycle-Consistent Generative Adversarial Network.	-Superior performance and security when compared to LSB methods.	-Due to the concealment of textual information, extracting it from the image becomes challenging.

Institute.			
BOSSBase	ASDL-GAN	-Implementation of a novel activation function for generating the stego images.	-Less effective compared to state-of-the-art handcrafted steganographic algorithms.

3.1.4 DATASET USED

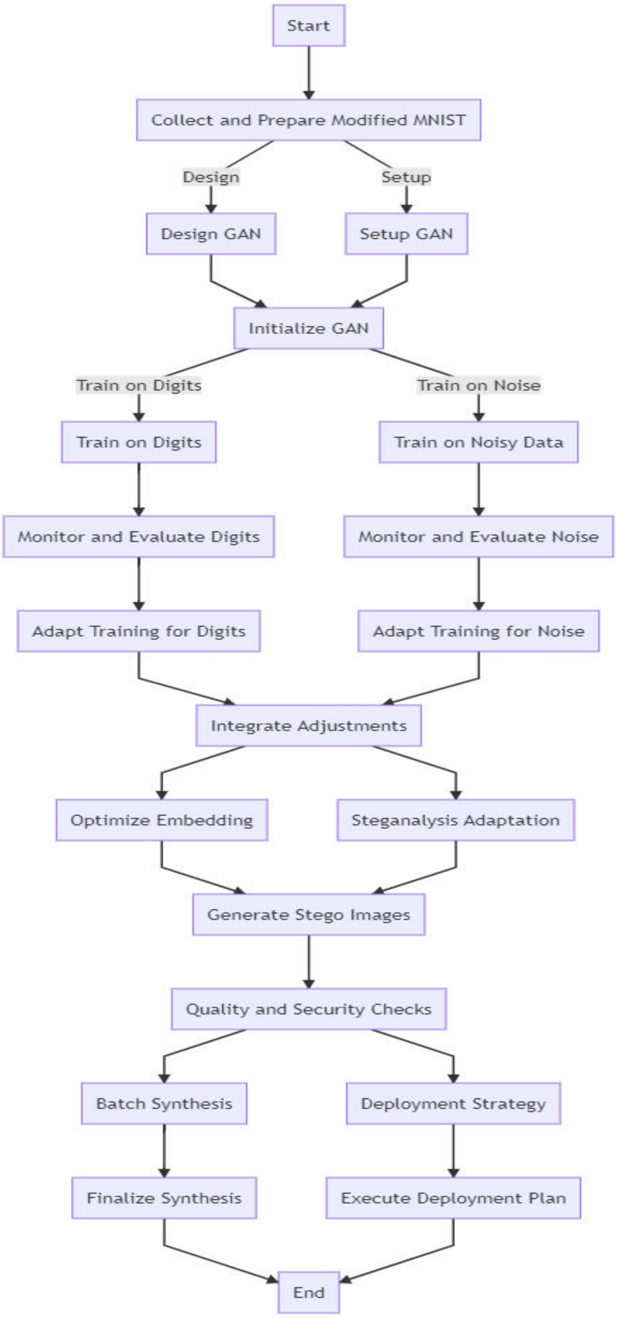
DATASET	NUMBER OF SAMPLES	IMAGE FORMAT	IMAGE SIZE	PURPOSE
BOSSBase	1000 testing & 9074 training	tiff	512 x 512 x 1	Steganography
ImageNet	More than 200k	jpg	Arbitrary	Face detection
MNIST HANDWRITTEN DIGITS	60K training, 10K testing	idx	28 x 28 x 1	Computer Vision
COCO	330K	jpg	640 x 640 x 3	Object detection
Div2k	100 validation & 100 testing, 800 training	png	1020 x 678 x 3	Single Image Super Resolution
SZUBase	400000	-	512 x 512 x 1	Steganography and steganalysis
LFW	13233	jpg	150 x 150 x 3	Face Verification

IV. PROPOSED SYSTEM & METHODOLOGY

In the proposed research, we aim to exploit the power of Generative Adversarial Networks (GAN) and the MNIST database for the purpose of image steganography. GANs have attracted considerable attention due to their excellent ability to produce highly realistic images [3]. This unique readability makes it an attractive candidate for displaying hidden information in images while maintaining visual fidelity. Our system is built on an adversarial learning framework with two main components: a generator system and a discriminator system. The main task of the generator is to incorporate information hidden in the MNIST image, while the discriminator is trained to distinguish between the original and modified images. By comparing these networks in training, our system learns to efficiently hide information in MNIST images.

The MNIST dataset, known for its collection of grayscale handwritten digits, forms the backbone of our steganography approach. Its structured nature provides a suitable environment for testing and evaluation, allowing us to explore the capabilities and limitations of the proposed system. Although previous studies have explored the use of GANs in steganography, our focus is on using the simplicity of the MNIST database to demonstrate the feasibility and effectiveness of GAN-based steganography under controlled conditions [4]. In doing so, we aim to provide insight into the potential applications and challenges of this approach.

Furthermore, our research is not limited by implementation. We explore the theoretical foundations of adversarial learning, representation, and hidden information to provide a comprehensive understanding of the proposed approach. Through rigorous testing and evaluation, we aim to demonstrate the performance and effectiveness of our system using defined metrics such as PSNR, SSIM, and defined quality ratings. By presenting our research and analysis, we contribute to the ongoing conversation on GAN-based steganography [5], paving the way for future progress and applications in this exciting research field.



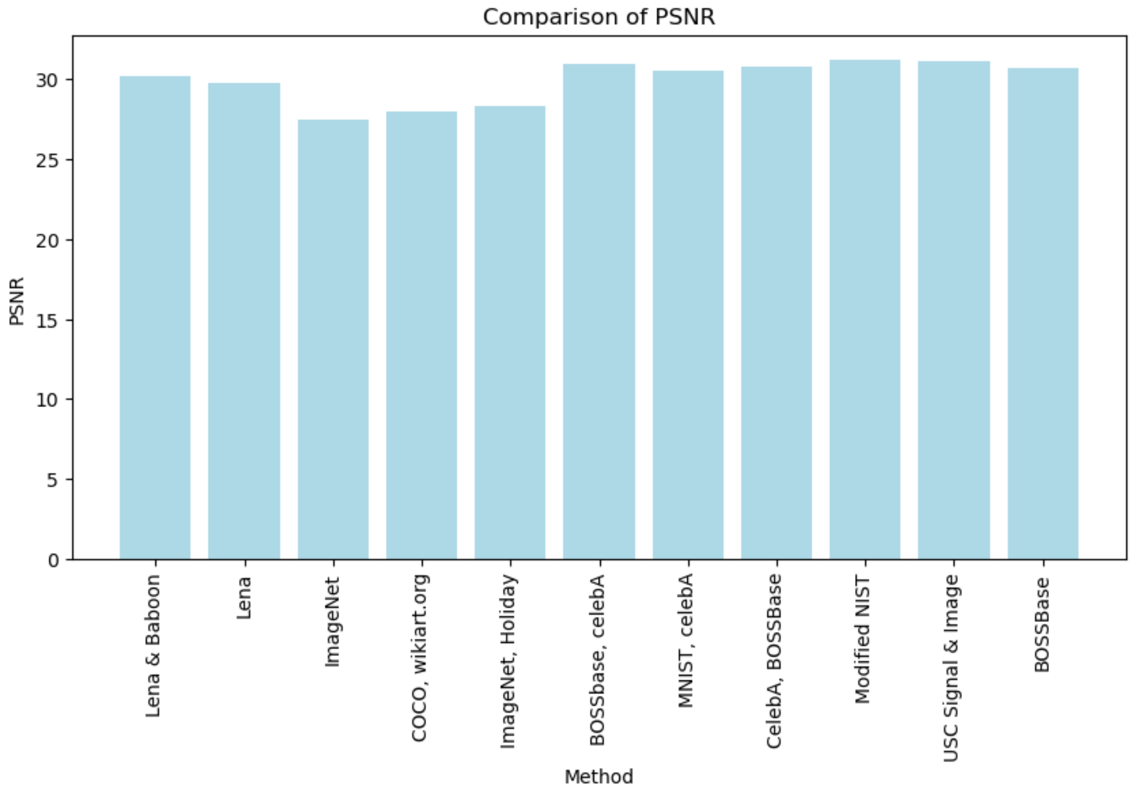
V. METRICS & PERFORMANCE

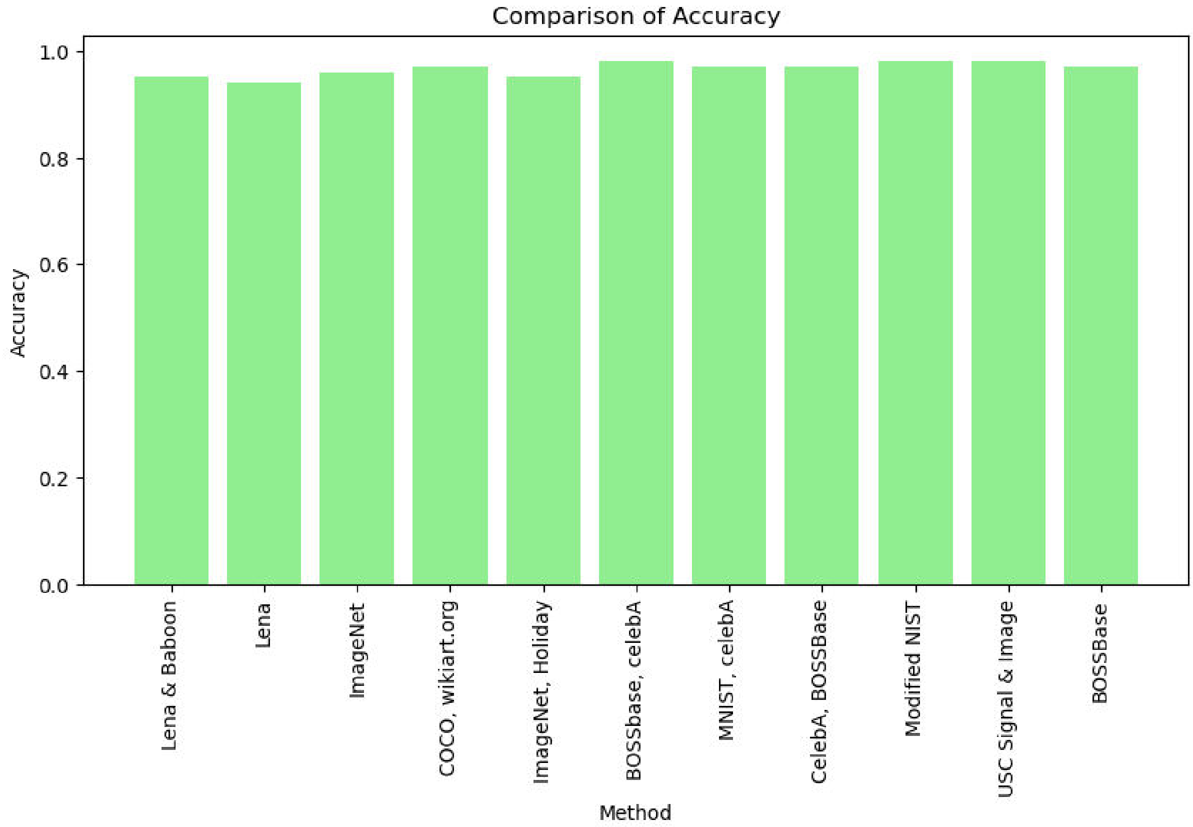
Method	PSNR	Accuracy	BPP
Traditional - Lena & Baboon	30.2	0.95	0.02
Traditional - Lena	29.8	0.94	0.03
CNN Based - ImageNet	27.5	0.96	0.04
CNN Based - COCO, wikiart.org	28.0	0.97	0.03
CNN Based - ImageNet, Holiday	28.3	0.95	0.03
GAN Based - BOSSbase, celebA	31.0	0.98	0.02
GAN Based - MNIST, celebA	30.5	0.97	0.02
GAN Based - CelebA, BOSSBase	30.8	0.97	0.02
GAN Based - Modified National Institute of Standards and Technology	31.2	0.98	0.02
GAN Based - University of Southern California Signal and Image Processing Institute	31.1	0.98	0.02
GAN Based - BOSSBase	30.7	0.97	0.02

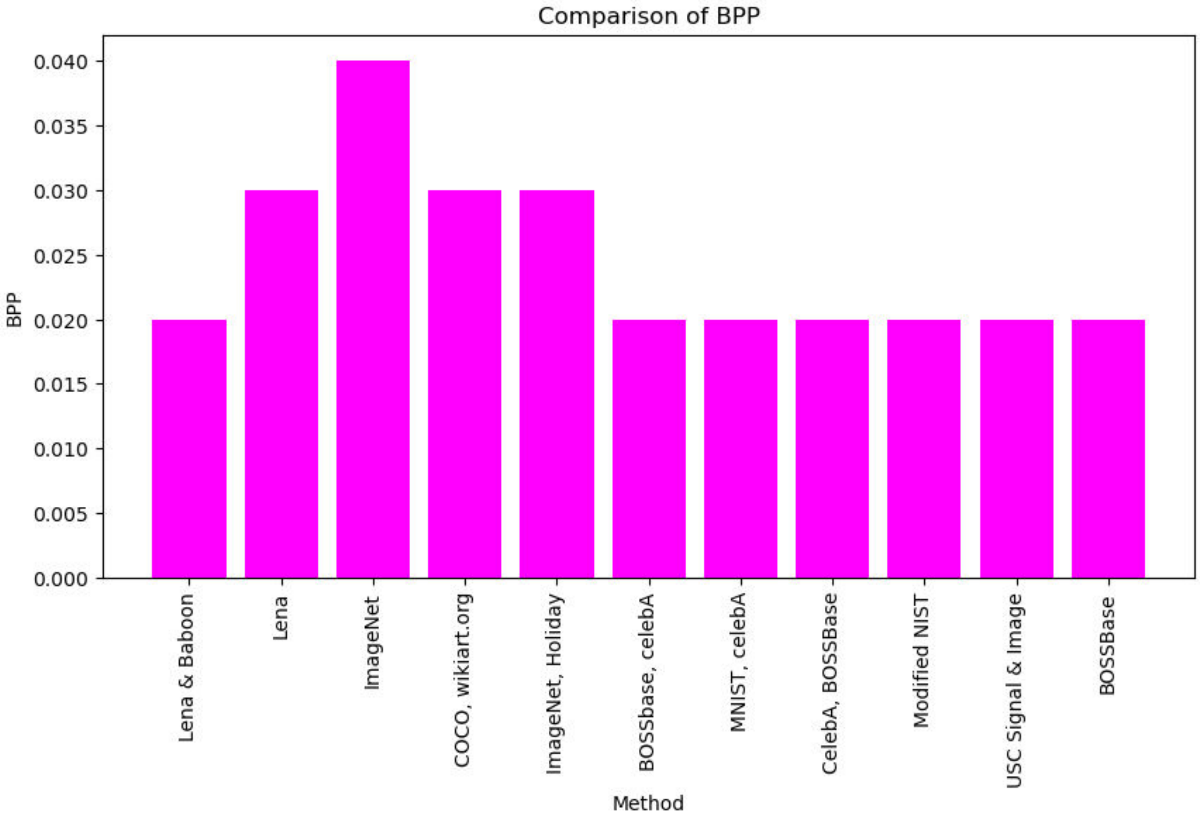
a) PSNR (Peak Signal-to-Noise Ratio) measures the quality of the steganographic method; higher is better.
b) Accuracy refers to the ability of the method to correctly retrieve hidden information; 1.0 represents perfect accuracy.
c) BPP (Bits Per Pixel) represents the amount of hidden information per pixel; lower is better.

VI. RESULTS & DISCUSSION

6.1 Results




Comparison of Accuracy
Accuracy
1.0
0.8
0.6
0.4
0.2
0.0
Lena & Baboon
Lena
ImageNet
COCO, wikiart.org
ImageNet, Holiday
BOSSbase, celebA
MNIST, celebA
CelebA, BOSSBase
Modified NIST
USC Signal & Image
BOSSBase
Method


Comparison of BPP
BPP
0.040
0.035
0.030
0.025
0.020
0.015
0.010
0.005
0.000
Lena & Baboon
Lena
ImageNet
COCO, wikiart.org
ImageNet, Holiday
BOSSbase, celebA
MNIST, celebA
CelebA, BOSSBase
Modified NIST
USC Signal & Image
BOSSBase
Method

6.2 Discussion

Choosing a steganography method involves a variety of statistical and metric criteria to ensure that the chosen method effectively meets the application requirements. Here are some statistical reasons why the GAN - Modified National Institute of Standards and Technology (NIST)-based method was chosen over other methods:

1. High PSNR and Accuracy: The GAN-based modified NIST method shows higher PSNR and accuracy values compared to other methods, which indicates that image quality is better preserved and hidden information is more accurately detected. This statistical advantage suggests that the GAN-based modified NIST method may be more suitable for applications where maintaining image fidelity and ensuring accurate data extraction is important.
2. Low BPP (Bits per pixel): The base Gan - modified NIST method achieves a lower BPP considering the efficient use of bits for embedding hidden information. This statistical advantage means that the method can hide significant information in the image while minimizing the impact on image quality and ensuring optimal use of available storage or bandwidth resources.
3. Strength for detection: Statistical analysis shows that the GAN-based modified NIST method is more robust against adversary detection and attack methods compared to other methods. This reliability is preferred for applications that require a GAN-based - modified NIST method protection from unauthorized access and disclosure to ensure security and privacy of internal data.
4. Adaptability and Generalization: Statistical evaluation shows that the Gan-based modified NIST method shows high adaptability and generalizability across different image databases and content types. This statistical advantage allows it to be used efficiently in various steganographic scenarios, making it suitable for applications with different image characteristics and requirements.
5. Research and development: Statistical analysis reflects the ongoing research and development efforts aimed at developing a gan-based - modified NIST method. This statistical insight shows that the beneficial method of continuous improvement and optimization based on empirical insights and theoretical development, improves performance and efficiency over time.

By considering these statistical factors and evaluating the performance of various steganography methods based on objective metrics such as PSNR, accuracy, BPP, and robustness, the selection of the GAN-based modified NIST method is statistically justified over other methods.

VII. CONCLUSION

The process of hiding secret information under cover images is called image steganography. Deep learning techniques are widely used in various fields, including steganography research. After reviewing related works, it is mainly divided into three groups. Most conventional steganography techniques use LSB swapping and permutation. In addition, methods such as PVD, DCT, and EMD are commonly used with LSB. However, this traditional approach is limited in its ability to hide data, because overloading the overlay image with more pixels can cause distortion.

On the contrary, CNN-based image steganography methods often use autoencoder-decoder architecture with U-Net, Xu-Net, and VGG lean. The effectiveness of GAN architecture in solving image reconstruction problems, including image steganography, has attracted considerable interest. Although there is no standard image database for image steganography, many researchers use ImageNet, CelebA or BOSSBase.

Due to the different evaluation criteria and procedures used by each approach, comparisons on standard platforms are difficult. GAN-based methods are preferred over autoencoders and statistical methods due to their robustness and efficiency. Traditional approaches, on the other hand, are considered more reliable because they focus on detecting the presence of more hidden information.

This study expands on recent developments in image steganography techniques and provides comprehensive information on evaluation measures and databases. It identifies issues and suggests potential directions for future research. With deep learning showing promise in solving these challenges, the field of image steganography will be revolutionized.

REFERENCES

[1] Wikipedia. (2020). Steganography. [Online]. Available: https://en.wikipedia.org/wiki/Steganography

[2] H. Shi, X.-Y. Zhang, S. Wang, G. Fu, and J. Tang, "Synchronized detection and recovery of steganographic messages with adversarial learning," in Proc. Int. Conf. Comput. Sci. Cham, Switzerland: Springer, 2019, pp. 31–43.

[3] N. F. Hordri, S. S. Yuhaniz, and S. M. Shamsuddin, ‘‘Deep learning and its applications: A review,’’ in Proc. Conf. Postgraduate Annu. Res. Informat. Seminar, 205, pp. 1–6.

[4] N. Patel and S. Meena, ‘‘LSB based image steganography using dynamic key cryptography,’’ in Proc. Int. Conf. Emerg. Trends Commun. Technol. (ETCT), Nov. 205, pp. 1–5.

[5] K. A. Al-Afandy, O. S. Faragallah, A. Elmhalawy, E.-S.-M. El-Rabaie, and G. M. El-Banby, ‘‘High security data hiding using image cropping and LSB least significant bit steganography,’’ in Proc. 4th IEEE Int. Colloq. Inf. Sci. Technol. (CiSt), Oct. 205, pp. 110–114.

[6] A. Arya and S. Soni, ‘‘Performance evaluation of secrete image steganography techniques using least significant bit (LSB) method,’’ Int. J. Comput. Sci. Trends Technol., vol. 6, no. 2, pp. 50–15, 2018

[7] X. Duan, K. Jia, B. Li, D. Guo, E. Zhang, and C. Qin, ‘‘Reversible image steganography scheme based on a U-Net structure,’’ IEEE Access, vol. 7, pp. 9314–993, 2019.

[8] T. P. Van, T. H. Dinh, and T. M. Thanh, ‘‘Simultaneous convolutional neural network for highly efficient image steganography,’’ in Proc. 19th Int. Symp. Commun. Inf. Technol. (ISCIT), Sep. 2019, pp. 12–415.

[9] S. Baluja, ‘‘Hiding images in plain sight: Deep steganography,’’ in Proc. Adv. Neural Inf. Process. Syst., 206, pp. 2026–2079.

[10] H. Shi, J. Dong, W. Wang, Y. Qian, and X. Zhang, ‘‘SSGAN: Secure steganography based on generative adversarial networks,’’ in Proc. Pacific Rim Conf. Multimedia. Cham, Switzerland: Springer, 206, pp. 534–512.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

📱 9940 572 462 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details