IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Steganography: Concealing Information In Image, Audio And Video

[1]Ayush Gupta, [2]Khalid Quadri, [3]Vedant Patil, [4]Prasad Unecha, [5]Mr. Naman V. Buradkar, [6]Mr. Ganesh S. Pise

[1234]Student, [56]Assistant Professor

Department of Information Technology, SCTR'S Pune Institute of Computer Technology

Pune, India

Abstract: Steganography is the process of hiding secret information, be it text, images, or videos, within digital media in a manner imperceptible to human eyes. The rise of deep learning technology has marked a powerful advancement in various applications, including steganography, attracting significant attention and fostering extensive research. This paper presents a concise review of diverse steganography technologies, encompassing both traditional methods and the latest emerging deep learning techniques. Spatial domain technologies like Least Significant Bit (LSB), and transform domain technologies such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), are explored alongside deep learning technologies like Convolutional Neural Networks (CNN) and Generative Adversarial Networks (GAN) in the context of steganography. The discussion extends to various datasets used in steganography research, including BossBase, ImageNet, and MNIST. This paper aims to provide valuable insights for fellow researchers by reviewing contemporary trends and offering potential directions for the future of steganography research.

Index Terms - Steganography, GAN steganography, CNN steganography, Data hiding, Spatial-domain steganography, Transform-domain steganography.

I. INTRODUCTION

Technology has evolved to a great extent over the past years, leading to the widespread use of multimedia for data transfer. However, the main concern arises when these transfers occur over insecure network channels, emphasizing the need for secure transmission. While the internet has become a popular means of exchanging information, its advantages are marred by significant drawbacks in terms of security, privacy, and data integrity. The vulnerability of data to security threats and eavesdropping poses a substantial risk.

The rapid development of the internet has resulted in an exponential increase in the use of images, audio, and videos as mediums for information exchange. Despite the familiarity with techniques for information hiding in the past, their popularity has surged recently due to the escalating data traffic in social media and the internet.

Steganography, one such technique for information concealment, facilitates secure communication by embedding hidden messages within images, audio, and videos as carrier mediums, effectively concealing the presence of the hidden data. The term 'steganography' originates from the Greek word 'steganographia,' combining 'steganos,' meaning covered or concealed, and '-graphia,' denoting writing. In essence, steganography translates to hidden writing. The primary objective of steganography is to secure the communication of concealed messages.

Steganography shares similarities with cryptography but with a subtle difference. In cryptography, the focus is on making data unbreakable and unreadable, resulting in visible ciphertext that may raise suspicion. On the other hand, steganography hides information within digital media like images, audio, and videos, making it less conspicuous. The advantage of steganography over cryptography lies in the fact that the hidden message does not attract attention.

1.1 Mediums of Steganography: Various steganography techniques exist, depending on the item to be protected for achieving security.

1.1.1 Text Steganography: This simple form involves hiding text within other text, altering existing text formats, changing words, using context-free grammar, or generating random characters.

1.1.2 Image Steganography: Here, the cover medium is an image, and the message is hidden by manipulating pixel densities.

1.1.3 Audio Steganography: This significant medium, driven by the demand for Voice Over Internet Protocol (VOIP), involves hiding information within audio files, mainly using formats like WAVE and MPEG.

1.1.4 Video Steganography: Information is concealed within digital video formats like Mp4 and AVI, using images that remain inconspicuous to the human eye.

Among all steganography mediums, images are the most widely used carriers of secret information.

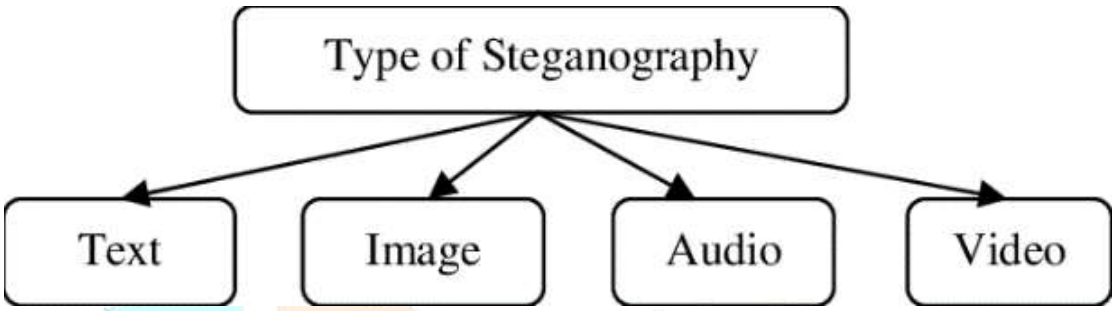

Figure 1: Steganography Mediums.

Steganography operates by hiding information in a manner that avoids suspicion. One widely used technique is the Least Significant Bit (LSB) method, which embeds secret information in the least significant bits of the media file. For instance, in an image pixel containing three bytes of data corresponding to red, green, and blue colors, the LSB alters the last bit to hide one bit of data. The modification in the last bit doesn't affect the perceptibility of the picture to human eyes.

The same LSB method can be extended to other digital media, such as audio and videos, ensuring that hidden data does not result in changes in sound or visual output. Besides LSB, spatial domain methods and transform domain methods, including Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), are also employed for steganography. Additionally, deep learning methods, such as Convolutional Neural Network (CNN), Deep Convolutional Neural Network (DCNN), and Generative Adversarial Network (GAN), are used for steganography.

This paper provides a brief review of different steganography techniques employed for information concealment in various media. The paper is organized as follows: Section 2 presents related work on different steganography methods. In Section 3, we describe various proposed methodologies of steganography. Section 4 outlines different datasets used for research on steganography, and Section 5 concludes the paper.

II. Related Work

In their research, HUNG-JUI KO et al. [1] introduced a steganography method based on a magic cube and modulo operation. This approach involves three main phases: Preliminary, Embedding, and Extraction. During the preliminary phase, the cover image is divided into non-overlapping blocks of 2x2 pixels, and an NxNxN magic cube is generated using a pseudo-key. In the Embedding phase, the message is concealed within the image, resulting in a stego-image. Finally, the Extraction phase involves dividing the stego-image into 2x2 pixel blocks, obtaining NxNxN using a pseudo-random key, and extracting the secret message from the image. The results of this method demonstrate an increase in carrying capacity and a reduction in computational overhead.

YING-QIAN ZHANG et al. [2] proposed a steganography method based on the Discrete Hadamard Transform. In this technique, the cover image is converted into an NxN matrix (HC), and embedded values are scaled to a range of coefficient values to reduce distortion. The embedding process is adapted for both positive and negative coefficient values. The stego-image matrix is obtained by applying Inverse DHT on the matrix HC, and after converting pixel values to integers, the final stego-image is achieved. The extraction process involves retrieving embedded data from DHT coefficients. Results indicate the method's efficiency in achieving good visual quality and higher hiding capacity, along with high imperceptibility and security.

SACHIN DHAWAN et al. [3] proposed a steganography approach that combines different algorithms to enhance the security of secret data. The method utilizes Binary Bit-Plane Decomposition-based encryption and Salp Swarm Optimization-based embedding, with a Hybrid Fuzzy Neural Network used to improve the quality of the stego-image. The process involves four stages: encryption, embedding, quality enhancement, and extraction. This results in increased data security, integrity, confidentiality, and payload capacity.

C. ZHANG et al. [4] presented a high-quality steganography technique using Optical Phase Encoding for hiding and the Transport of Intensity Equation for extracting the secret image perfectly.

M. ANWAR et al. [5] proposed an audio steganography technique employing Lifting Wavelet Transform (LWT) and Dynamic Key. The confidential data is encrypted using AES encryption, and a dynamic key is generated under an Android application using a Pseudo-Random Number Generator (PRNG). Results show that 20% data can be inserted relative to the audio size without a change in audio quality.

S.T. ABDULRAZZAQ et al. [6] proposed a steganography technique aiming to increase carrier medium capacity by hiding images into audio files. This technique uses WAV audio format based on the LSB algorithm, and image compression is performed using the GMPR technique, which is based on Discrete Cosine Transform (DCT) and High-frequency minimization encoding algorithm.

P. YADAV et al. [7] introduced a method to enhance peak signal-to-noise ratio and minimize mean squared error using spread spectrum image steganography. The approach follows a three-level security model, involving RSA for the security of hidden text, data compression using Run-length Encoding, and LSB spatial-domain technique for hiding data inside the image.

F. SHADAMAD et al. [8] addressed a model to encode secret messages in face portraits and decode hidden messages from physically printed photos of Identity Documents (ID) and Machine-Readable Travel Documents (MRTDs). The encoded face, called Code Face, is used to encode and decode the secret message in the context of facial images. The encoder and decoder are trained using a GAN network, providing high robustness in decoding and stability in encoding messages up to the size of 120 bits.

R. WAZIRALI et al. [9] proposed a steganography technique using Genetic Algorithms (GAs) and introduced a new operation to increase LSB matching between the carrier and stego-image. The main objective is to embed the secret image at the best possible position in the cover image to increase LSB matching. The process involves six stages: scanning the image to find the best position for embedding, circular shifting of pixels without loss, matrix transformation, flipping bits in the opposite direction, LSB matching to check values between the carrier and stego-image, and embedding the message in the least significant bits of the carrier image. Extraction is performed in the reverse order of embedding, resulting in higher PSNR, increased embedding capacity, and maintained image quality after embedding.

J. WANG et al. [10] proposed a novel approach to video steganography based on Intra-prediction mode (IPM). The method introduces a cover selection rule combined with Coding Unit (CU) and Prediction Unit (PU) coding information, resulting in improved security performance. Matrix coding is used to implement steganography on High-Efficiency Video Coding (HEVC) video streams, ensuring quality maintenance and ease of implementation.

Q.P. HUU et al. [11] presented a deep learning-based method to hide secret audio inside digital images. The approach involves two sub-models: one for encoding and another for decoding the message. The method maintains the integrity of audio and video, improving the length of hidden audio. Data preprocessing is followed by building a Deep Neural Network (DNN) model to hide audio into an image. The characteristics of the audio are observed and hidden in the image, with the decoder extracting the original message. The average correlation is observed to be above 99%, and the method offers better hiding capacity compared to the LSB technique, without compromising image quality.

G. XIE et al. [12] proposed a two-step cost function for adaptive steganography. The method identifies the cover image and embeds the secret message using the Spread Transform Coding (STC) method. The 2D-SSA algorithm allows for the selection of different high-frequency components, and the Weighted Message Flip (WMF) helps achieve smooth images. The method provides secure performance for payload greater than 0.3 and faster processing.

R. THABIT et al. [13] introduced the Color and Spacing Normalization Stego (CSNTSteg) model to address low capacity and invisibility problems. The model utilizes RGB coding, character spacing, and Huffman coding to increase hiding capacity. CSNT utilizes all letters, numbers, and symbols as cover, excluding white space. Normalization is applied to achieve high invisibility. The method works in two phases: embedding and extraction. In embedding, the secret message is framed, compressed, split into blocks, and normalized to increase invisibility. In extraction, tampering is checked, and the hidden message is extracted using color and spacing extraction and secret block retrieval. Results show a capacity ratio of 98.85% and offer higher invisibility.

M.ALORAINI et al. [14] proposed a framework for spatial steganography and developed a statistical framework for JPEG steganography, where the message and cover are modeled by a multivariate Gaussian distribution. The model improves security and outperforms state-of-the-art JPEG algorithms.

A.S. ANSARI et al. [15] presented a steganography algorithm that works for cover images of multiple formats. This algorithm applies uniform security policies to JPEG, Bitmap, TIFF, and PNG images, selecting the most suitable cover based on data length, bandwidth, and allowable distortion.

M.KALITA et al. [16] introduced a spatial domain method for grayscale images. The method proposed the use of neighboring pixel pair difference value and Least Significant Bit (LSB) substitution to provide enhanced embedding capacity. The process is based on a 3x3 block structure to divide the cover image into non-overlapping blocks, with K-LSBs of pixels replaced by k secret bits. The difference between neighboring and center pixels is used to determine secret bits embedded in pixel pairs. Results show high embedding capacity and good PSNR value.

S.S.M. THAN et al. [17] proposed the use of Least Significant Bit (LSB) enforced with high compression using Huffman chunk coding method. The aim is to increase security and embedding capacity. LSB data is inserted in existing bits without adding additional bytes, and Huffman coding is used for data compression to achieve high-capacity embedding. To ensure security and robustness in data transmission, ciphertext is embedded using a confidence key.

K.RAJALAKSHMI et al. [18] introduced a method to conceal existing messages to make them tricky to notice. The proposed work hides a video in another video using Patch Wise Code Formation techniques. In preprocessing, the Fuzzy Adaptive Median Technique (FAMF) is used to eliminate impulse noise and increase quality. The embedding is done by LSB substitution, and the Patch Wise Code Formation (PCF) technique is implemented to provide security for the video. The encoded video is converted into an encoded format using the PCF technique.

These research efforts explore various steganography methods, employing different techniques and algorithms to enhance security, increase hiding capacity, and maintain the quality of cover media after embedding hidden information.

III. Material And Methods

After reviewing the methodologies, they are classified into mainly three categories, namely Spatial Domain Methods, Transform Domain Methods, and Deep Learning methods. Spatial Domain Methods include LSB coding, Parity coding, etc., while Transform domain includes techniques like Spread spectrum, Phase coding, Discrete Wavelet Transform (DWT), and Discrete Cosine Transform (DCT). Deep learning Methods are based on Convolutional Neural Network and Generative Adversarial Network.

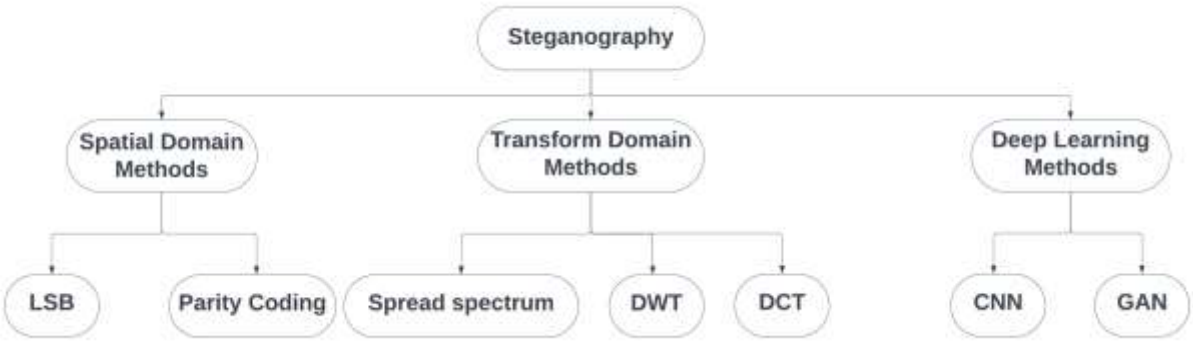

Fig 2: Steganography Methodologies

3.1 Spatial Domain Methods:

In S. TEOTIA et al. [19], spatial domain techniques for audio and video Steganography were proposed. The Least Significant Bit Coding is one of the most popular and widely used spatial-domain techniques proposed in the paper. It is also a simple and popular method for inserting data in an audio file. In this method, the binary pattern of each specimen of digitized audio is changed with the binary correspondent of the confidential message. It also offers an increase in embedding capacity. They also proposed Parity Coding, which is one of the robust techniques mainly used in audio steganography. Instead of breaking one signal into different parts, it breaks into different samples and inserts each bit of the message from the parity bit. If the parity bit of the selected area does not match the message bit to be inserted, then it inverts the LSB of one specimen in the area. Hence, it provides more options in encoding confidential bit.

In S.P. RAJPUT et al. [20], a Least Significant Bit technique is proposed, but not in the traditional fashion, which includes converting the message to binary form and replacing each bit linearly. However, it

does not bring capacity and robustness. The proposed method embeds secret values in a different fashion than the traditional way. It introduces two algorithms. In Algorithm-I, two bits of secret data are embedded at a time on LSB positions of carrier audio based on 3 MSBs of carrier audio, while in Algorithm-II, two bits are embedded in LSB but based on the complement of 3 MSBs of carrier audio.

In M. KALITA et al. [21], a spatial domain method for grayscale images is proposed. It works on pixel pair difference and LSB substitution, providing enhanced embedding capacity. It works by dividing the cover image into 3x3 blocks; K LSBs are replaced by K bits of secret data. The cover image is divided into 3x3 blocks horizontally, and the secret message is embedded 3-bits in each pixel pair.

In J.R. JAYAPANDIAN et al. [22], the enhancement in the existing Least Significant Bit algorithm is proposed. This technique focuses on the embedding part of the steganography process and leads to the number of bits used in the cover image for storing the secret message. The existing method uses one-to-one byte representation, meaning one byte is replaced with another byte. The proposed system focuses on optimizing the way secret messages are embedded.

In M.M. MAHMOUD et al. [23], a novel LSB method is proposed to overcome the limitations of the traditional LSB method for steganography. It uses Huffman coding for message compression and then encryption using the AES-128 standard. To enhance security, it proposes the use of BMSE mechanism to hide the message in random samples and thereafter in random blocks and bytes to ensure a high degree of randomness, complexity, and ultimately protection. It solves two problems of the traditional approach; the message hidden in the proposed method is not sequential as that of the traditional approach, and BMSE is used to enhance security. Even for a large message, BMSE bit representation is not large. Hence, the proposed algorithm provides higher capacity.

3.2 Transform Domain Methods:

In L.M. MARVEL et al. [24], a proposed digital steganography method based on spread spectrum Image steganography. This method hides and recovers messages from digital images while maintaining image size and dynamic range. SSIS includes techniques for error control and image restoration. The basic concept is to hide information within noise added to the digital cover. The low-rate-error-encoding is applied to the signal before encoding. It proposes spread spectrum, which describes the process of bandwidth spreading of a narrow bandwidth signal across wide band frequencies. This can be achieved by a narrowband waveform.

In A.A. KRISHNAN et al. [25], an audio steganography scheme on Direct Sequence Spread Spectrum (DSSS) with enhanced security is proposed. The text message is embedded in the audio file. During encryption, the Vigenere algorithm is used for encryption of the message, and the Cipher text is embedded using DSSS algorithm. The spread spectrum spreads data across the audio signal, resulting in increased bandwidth occupation.

In O.F.A. WAHAB et al. [26], a proposed Discrete Wavelet Transform technique for image converting to a series of wavelets and stored more efficiently. It is important in the case of image compression, ensuring no information loss from the picture. It offers lossless compression. Wavelet transform is an emerging and widely used powerful tool for image compression. With DWT, it uses RSA for encryption and LSB for embedding the message into the cover media.

In M. BEZIYAD et al. [27], Discrete Cosine Transform (DCT) is used for expressing the temporal vector, which will contain highly correlated pixels. Therefore, DCT can express the vector within a few DCT coefficients, leaving insignificant ones. The vector is associated with every pixel in the video and points to the direction of pixel movement.

In J. KUNHOTH et al. [28], reviewed transform domain techniques, Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) along with the LSB method. DWT decomposes the signal into sets with significant and insignificant information. Significant information is low-frequency DWT coefficients, and insignificant are high-frequency DWT coefficients. DCT is also like DWT, which divides the image into spectral sub-bands. It differs from DWT; DCT generates more frequency bands, and DWT generates fewer frequency bands compared to DCT.

3.3 Deep Learning Methods:

The Deep Learning methods mainly include Convolutional Neural Network-based methods and Generative Adversarial Network methods.

3.3.1 Convolutional Neural Network based Methods:

In N. MANOHAR et al. [29], a method is proposed based on Neural Network, Fuzzy Logic, and LSB. The Neural Network is applied to it, which basically provides input and outputs. The Neural Network is proposed to provide the network with a corresponding set of data inputs and outputs. It is a combination of multiple nodes to accomplish particular values and weights in several components.

In E. VENUGOPAL et al. [30], a Modified CNN-based steganalyzer for images obtained by applying steganography with inserting a key of one kind is proposed. The proposed design implants fewer convolutions with bigger channels in the last Convolutional Layer and can manage a bigger image and lower payload.

In J. WU et al. [31], a CNN-based method is proposed, which works by training a steganalytic network and uses these pre-trained models to generate the stegos. The proposed method is based on enhancing the performance by fooling the steganalyzer through adversarial attacks. The adversarial attacks are done in an iterative manner to fool the steganalyzer.

In Z. XIANG et al. [32], a CNN-based approach with two contributions is proposed. In the first method, they proposed a new arrangement of Convolutional and Pooling layers for processing local information better than the existing CNN model. For the second method, they proposed the method of adding global average pooling before fully connected layers, pooling is placed at a better position for steganalysis.

In W. TANG et al. [33], a steganographic scheme called Adversarial Embedding is proposed, which hides stego message and at the same time fools CNN-based steganalyzer. It works under the framework of distortion minimization. This works by adjusting the cost of image elements modifications according to gradients back propagated from CNN steganalyzer.

In P. WU et al. [34], a proposed deep convolutional neural network method with image-to-image steganography. Proposed encoder-decoder architecture. The DCNN multi-level high-order transformations are suggested, where high-level features use less information to present complex visual patterns.

3.3.2 Generative Adversarial Network based Methods:

In Q. LI et al. [35], the use of Generative Adversarial Network to produce more realistic stego images is proposed. General Adversarial Networks are used to produce the quality stego image and train a discriminative network using the distribution of generated images and real images. The goal of GAN is to estimate the potential distribution of real data and accordingly generate new data samples with the same distribution.

In Z. ZHANG et al. [36], a method based on GAN for image steganography is proposed. In the proposed model Synthetic Semantics Stego-GAN (SSS-GAN) is used to generate stego images from a secret message. In the first phase, the model is trained with a semantic label on collected images. In the second phase, the trained model is used to generate a large number of images from a stego image dataset. In the third phase, the sender segments secret information and maps information segmentation to a semantic label and then uses an image generator to generate a stego-image.

In S. F. KAZEROONI et al. [37], a proposed GAN tunnel which generates traffic that mimics a decoy application and encapsulates actual user traffic. The basic working is the user sending traffic packets to a GAN client, and it encapsulates it for transmission. In the proposed model, Wasserstein GAN.

In L. CHEN et al. [38], a GAN-based audio steganography framework that could learn to generate steganographic cover audio for a message is proposed. The proposed method consists of three parts: generator, discriminator, and steganalyzer. They proposed spectral normalization technique proposed in spectral normalization GAN. It generates cover audio of better quality. The proposed discriminator has 9 convolutional layers and 1 fully connected layer. The discriminator distinguishes original audio from cover audio.

In J. LIU et al. [39], reviewed GAN-based steganography according to different strategies like cover selection, cover modification, and cover synthesis. They proposed GAN-based cover modification (GAN-CMO), which focuses on the adversarial game between analyzer and steganographer. The GAN-based cover selection aims to establish a mapping relationship between the message and the cover. The GAN-based cover synthesis (GAN-CSY) creates a stego image by a generator trained by GAN.

Title	Authors	Methodology Used	Advantages/Findings	Future Work
Enhancing Audio and Video Steganography Technique Using Hybrid Algorithm	S.TEOTIA et al. [19]	Least Significant Bit, Parity Coding.	Reduced error in audio and video steganography and better PSNR and MSE values.	More better and secure algorithm can be implemented for reducing distortion and increase in security.
An Efficient Audio Steganography Technique to Hide Text in Audio	S.P. RAJPUT et al. [20]	Enhanced Least Significant Bit Algorithm and Most significant Bit.	Increase in embedding capacity and increase in security. File size not changed after embedding.	Performance can be evolved using random embedding data bits according to secret pattern.
A Spatial Domain Steganographic Approach Using Pixel Pair Differencing and LSB Substitution	M.KALITA et al. [21]	Pixel pair difference and Least Significant Bit.	Higher embedding capacity with good PSNR value.	Advanced compression methods can be adopted to enhance capacity without compromising quality.
Enhanced Least Significant Bit Replacement Algorithm in Spatial Domain of Steganography Using Character Sequence Optimization	J.R. JAYAPANDIAN et al. [22]	Enhanced Least Significant Bit Algorithm	Enable high capacity embedding rate, additional security and enhanced cover image quality. Better PSNR,MSE and RMSE values.	Finding more such algorithm in spatial domain and contribute to better image quality after embedding.
Enhancing LSB Using Binary Message Size Encoding for High Capacity, Transparent and Secure Audio Steganography—An Innovative Approach	M.M. MAHMOUD et al. [23]	Novel Least Significant Bit Algorithm and Huffman Coding for Compression and BMSE.	Increase in image quality and superior to existing methods. Resistent against resampling attack.	Work can be done to increase the embedding capacity without compromising on quality.
Spread Spectrum Image Steganography	L.M. MARVEL et al. [24]	Spread spectrum Image Steganography	Increased Security and Embedded signal power is insignificant.	Improving embedded signal estimation process and complex error correction to be implemented
Spread Spectrum Based Encrypted Audio Steganographic System with Improved Security	A.A. KRISHNAN et al. [25]	Direct sequence Spread Spectrum Steganography.	Robust and Secure with reduced noise for optimal SF and CR values.	Use of Improved encryption algorithm.Optimization of various parameters used in embedding and extraction stages.
Hiding Data Using Efficient Combination of RSA Cryptography, and Compression	O.F.A. WAHAB et al. [26]	Discrete Wavelet Transform, RSA and LSB.	Increased video quality and storage capacity and highly secure.	To increase the security using improved algorithm.

Steganography Techniques				
Directional Pixogram: A New Approach for Video Steganography	M. BEZIYAD et al. [27]	Discrete Cosine Transform and Directional Pixogram.	Improved Quality and storage capacity.	Improving Directional Pixogram to make iot adapt various motions.
Video steganography: recent advances and challenges	J. KUNHOTH et al. [28]	Discrete Cosine Transform and Discrete Wavelet Transform with LSB.	Discussed different Steganography methodologies.	Designing Efficient data hiding methods.
Data Encryption & Decryption Using Steganography	N.MANOHAR et al. [29]	Convolutional Neural Network,Fuzzy Logic.	More Security, Quality of output and accuracy.	Use new algorithm, in use of more quantization and security.
Design and implementation of video steganography using Modified CNN algorithm	E.VENUGOPAL et al. [30]	Convolutional Neural Network.	Provide great proficiency and security, robust and unpredictable detectibility.	Use new methods to increase accuracy and security.
Audio Steganography Based on Iterative Adversarial Attacks against Convolutional Neural Networks	J.WU et al. [31]	Convolutional Neural Network, Adversarial Network.	Effective embedding cost, better compared to adaptive steganography.	Inherent patterns investigation for improving security, gradient amplitude.
A New Convolutional Neural Network-Based Steganalysis Method for Content-Adaptive Image Steganography in the Spatial Domain	Z.XIANG et al. [32]	Convolutional Neural Network, Content-adaptive image steganography.	Better performance that CNN based steganalysis methods.	Exploring new techniques for enhancing performance of the model.
CNN-Based Adversarial Embedding for Image Steganography	W.TANG et al. [33]	Adversarial-machine learning, CNN.	Enhanced security, accuracy.	Introducing new Adversarial-embedding methods to enhance the performance.
Image-into-Image Steganography Using Deep Convolutional Network	P.WU et al. [34]	Convolutional Neural Network.	Enhanced Robustness.	Reducing the generated noise and enhancing the quality.
A Novel Grayscale Image Steganography Scheme Based on	Q.LI et al. [35]	Generative Adversarial Network	Enhanced security, ease in decryption and retrieval.	Increasing quality of generated images.

Chaos Encryption and Generative Adversarial Networks		(GAN) and CNN.		
A Generative Method for Steganography by Cover Synthesis with Auxiliary Semantics	Z.ZHANG et al. [36]	GAN and Steganography by cover synthesis.	Enhanced security,capacity and robustness.	Enhance quality of generated image and improve capacity.
GAN Tunnel: Network Traffic Steganography by Using GANs to Counter Internet Traffic Classifiers	S.F. KAZEROONI et al. [37]	GAN and WGAN.	Protection of identity of source application.	Work to enhance capacity.
Learning to Generate Steganographic Cover for Audio Steganography Using GAN	L.CHEN et al. [38]	GAN and Deep learning based steganalysis.	High quality, undetectable and large embedding rate.	Enhancing the capacity and make it more secure.
Recent Advances of Image Steganography With Generative Adversarial Networks	J. LIU et al. [39]	Generative Adversarial Network.	Proposed recent advances I GAN-based steganography.	More safe and efficient method to be studied.

Table 1: Overview Of Referred Papers.

IV. Material And Methods

There is only one dataset, BossBase, used specifically for steganography, and other testing is done on other available datasets which are generally used for other purposes.

4.1 BOSSBASE:

In P. Bas et al. [40], it is the first scientific challenge to take steganography from research to practical implementation. The main aim is to develop a better steganalysis method capable of breaking steganographic images to detect secret information. The dataset contains train and test sets and is used to create stego-images. The training data contain 10,000 grayscale images, and testing contains 1,000 grayscale images.

4.2 CELEBA:

In Z. Liu et al. [41], the Large-scale CelebFaces dataset, a vast dataset with more than 200K images used for face recognition, face detection, face localization, and other operations is proposed. The dataset contains images from different sources, locations, backgrounds, poses, and is best suitable for steganography. The probability of using a photo or image as a cover is very high. Also, with images, it contains annotations like with/without glasses, emotions, and hairstyles.

4.3 IMAGENET:

In J. Deng et al. [42], the ImageNet dataset is also one of the large datasets containing images from WordNet, with each node containing more than 500 to 1000 images. In addition, it does not have any copyrights on images and contains links or thumbnails to the original image. The dataset contains varying sizes. The images can be selected based on requirements, belonging to different classes, backgrounds, and sizes.

4.4 MNIST HANDWRITTEN DIGITS:

The Modified National Institute of Standard and Technology database, MNIST, is another database that can be used for various computer vision and image processing applications. The dataset contains training and testing sets with images of handwritten digits 0 to 9. Images in this dataset are normalized, black and white with dimensions 28x28 pixels. The training dataset contains 60,000, and the testing dataset contains 10,000 images.

V. Conclusion

Steganography is a technique to hide information in plain sight. The traditional methods are most widely used along with some new Deep learning-based methods and used for research as well. The review of various techniques of steganography and all related work led to categorization in three categories: spatial domain, transform domain, and Deep learning methods. LSB is the most widely used spatial domain method for steganography along with some other methods. The transform domain methods are also not been part of work and research as well. The capacity of traditional methods is less, resulting in burdening the cover image and exploitation of pixels, resulting in distortion after embedding. The modern CNN-based methods are most prevailing; also, deep learning-based GAN architecture recently gained popularity and has the ability to deal with image reconstruction tasks. GAN-based methods proved better performance in security, hiding capacity, and are extensively used and most preferred nowadays over traditional methods, because of the security issue of traditional methods.

In Future Work, the use of popular networks U-Net, cycle-GAN, and DCT and DWT have been considered for exploration and other customized architecture. The most methods use text or gray images as secret information, and there is a need for more research on it. The result of the combination of traditional and Deep Learning methods should be studied. The performance and security from different attacks should be studied to enhance the performance.

References

[1]. H. -J. Ko, C. -T. Huang, H. -W. Tseng and S. -J. Wang, "Efficient Cost-Reduced With High-Quality Image of Imperceptible Steganography Using Modulo and Magic Cube," in IEEE Access, vol. 10, pp. 67686-67693, 2022, doi: 10.1109/ACCESS.2022.3185120.

[2]. Y. -Q. Zhang, K. Zhong and X. -Y. Wang, "High-Capacity Image Steganography Based on Discrete Hadamard Transform," in IEEE Access, vol. 10, pp. 65141-65155, 2022, doi: 10.1109/ACCESS.2022.3181179.

[3]. S. Dhawan, C. Chakraborty, J. Frnda, R. Gupta, A. K. Rana and S. K. Pani, "SSII: Secured and High-Quality Steganography Using Intelligent Hybrid Optimization Algorithms for Ior," in IEEE Access, vol. 9, pp. 87563-87578, 2021, doi: 10.1109/ACCESS.2021.3089357.

[4]. C. Zhang, W. He, X. Liu, X. Peng and Q. Tang, "High Capacity Steganography via Optical Phase-Encoding and Transport of Intensity Equation," in IEEE Photonics Journal, vol. 13, no. 1, pp. 1-8, Feb. 2021, Art no. 7800408, doi: 10.1109/JPHOR.2021.3052802.

[5]. M. Anwar, M. Sarosa and E. Rohadi, "Audio Steganography Using Lifting Wavelet Transform and Dynamic Key," 2019 International Conference of Artificial Intelligence and Information Technology (ICAIIT), Yogyakarta, Indonesia, 2019, pp. 133-137, doi: 10.1109/ICAIIT.2019.8834579.

[6]. Abdulrazzaq, S.T., Siddeq, M.M. & Rodrigues, M.A. A Novel Steganography Approach for Audio Files. SN COMPUT. SCI. 1, 97 (2020).

[7]. P. Yadav and M. Dutta, "3-Level security based spread spectrum image steganography with enhanced peak signal to noise ratio," 2017 Fourth International Conference on Image Information Processing (ICIIP), Shimla, India, 2017, pp. 1-5, doi: 10.1109/ICIIP.2017.8313696.

[8]. F. Shadmand, I. Medvedev and N. Gonçalves, "CodeFace: A Deep Learning Printer-Proof Steganography for Face Portraits," in IEEE Access, vol. 9, pp. 167282-167291, 2021, doi: 10.1109/ACCESS.2021.3132581.

[9]. R. Wazirali, W. Alasmary, M. M. E. A. Mahmoud and A. Alhindi, "An Optimized Steganography Hiding Capacity and Imperceptibly Using Genetic Algorithms," in IEEE Access, vol. 7, pp. 133496-133508, 2019, doi: 10.1109/ACCESS.2019.2941440.

[10]. J. Wang, X. Jia, X. Kang and Y. -Q. Shi, "A Cover Selection HEVC Video Steganography Based on Intra Prediction Mode," in IEEE Access, vol. 7, pp. 119393-119402, 2019, doi: 10.1109/ACCESS.2019.2936614.

[11]. Q. P. Huu, T. H. Dinh, N. N. Tran, T. P. Van and T. T. Minh, "Deep Neural Networks based Invisible Steganography for Audio-into-Image Algorithm," 2019 IEEE 8th Global Conference on Consumer Electronics (GCCE), Osaka, Japan, 2019, pp. 423-427, doi: 10.1109/GCCE46687.2019.9015498.

[12]. G. Xie, J. Ren, S. Marshall, H. Zhao and H. Li, "A New Cost Function for Spatial Image Steganography Based on 2D-SSA and WMF," in IEEE Access, vol. 9, pp. 30604-30614, 2021, doi: 10.1109/ACCESS.2021.3059690.

[13]. R. Thabit, N. I. Udzir, S. M. Yasin, A. Asmawi and A. A. -A. Gutub, "CSNTSteg: Color Spacing Normalization Text Steganography Model to Improve Capacity and Invisibility of Hidden Data," in IEEE Access, vol. 10, pp. 65439-65458, 2022, doi: 10.1109/ACCESS.2022.3182712.

[14]. M. Aloraini, M. Sharifzadeh and D. Schonfeld, "Quantized Gaussian JPEG Steganography and Pool Steganalysis," in IEEE Access, vol. 10, pp. 38031-38044, 2022, doi: 10.1109/ACCESS.2022.3165031.

A. S. Ansari, M. S. Mohammadi and M. T. Parvez, "A Multiple-Format Steganography Algorithm for Color Images," in IEEE Access, vol. 8, pp. 83926-83939, 2020, doi: 10.1109/ACCESS.2020.2991130.

[15]. M. Kalita, S. Majumder and T. Tuithung, "A spatial domain steganographic approach using pixel pair differencing and LSB substitution," 2017 4th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 2017, pp. 304-309, doi: 10.1109/SPIN.2017.8049964.

[16]. S. S. M. Than, ‘‘Secure data transmission in video format based on LSB and Huffman coding,’’ Int. J. Image, Graph. Signal Process., vol. 12, no. 1, p. 10, 2020.

[17]. K. Rajalakshmi and K. Mahesh, "Video steganography based on embedding the video using PCF technique," 2017 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, India, 2017, pp. 1-4, doi: 10.1109/ICICES.2017.8070726.

[18]. S. Teoria and P. Srivastava, "Enhancing Audio and Video Steganography Technique Using Hybrid Algorithm," 2018 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2018, pp. 1059-1063, doi: 10.1109/ICCSP.2018.8524182.

[19]. S. P. Rajput, K. P. Adhiya and G. K. Patnaik, "An Efficient Audio Steganography Technique to Hide Text in Audio," 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, 2017, pp. 1-6, doi: 10.1109/ICCUBEA.2017.8463948.

[20]. M. Kalita, S. Majumder and T. Tuithung, "A spatial domain steganographic approach using pixel pair differencing and LSB substitution," 2017 4th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 2017, pp. 304-309, doi: 10.1109/SPIN.2017.8049964.

[21]. J. R. Jayapandiyan, C. Kavitha and K. Sakthivel, "Enhanced Least Significant Bit Replacement Algorithm in Spatial Domain of Steganography Using Character Sequence Optimization," in IEEE Access, vol. 8, pp. 136537-136545, 2020, doi: 10.1109/ACCESS.2020.3009234.

[22]. M. M. Mahmoud and H. T. Elshoush, "Enhancing LSB Using Binary Message Size Encoding for High Capacity, Transparent and Secure Audio Steganography–An Innovative Approach," in IEEE Access, vol. 10, pp. 29954-29971, 2022, doi: 10.1109/ACCESS.2022.3155146.

[23]. L. M. Marvel, C. G. Boncelet and C. T. Retter, "Spread spectrum image steganography," in IEEE Transactions on Image Processing, vol. 8, no. 8, pp. 1075-1083, Aug. 1999, doi: 10.1109/83.777088.

A. A. Krishnan, C. S. Chandran, S. Kamal and M. H. Supriya, "Spread spectrum based encrypted audio steganographic system with improved security," 2017 International Conference on Circuits, Controls, and Communications (CCUBE), Bangalore, India, 2017, pp. 109-114, doi: 10.1109/CCUBE.2017.8394128.

[24]. O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein and H. F. A. Hamed, "Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques," in IEEE Access, vol. 9, pp. 31805-31815, 2021, doi: 10.1109/ACCESS.2021.3060317.

[25]. M. Baziyad, T. Rabie and I. Kamel, "Directional Pixogram: A New Approach for Video Steganography," 2020 Advances in Science and Engineering Technology International Conferences (ASET), Dubai, United Arab Emirates, 2020, pp. 1-5, doi: 10.1109/ASET48392.2020.9118180.

[26]. Kunhorh, J., Subramanian, N., Al-Maadeed, S. et al. Video steganography: recent advances and challenges. Multimed Tools Appl (2023).

[27]. N. Manohar and P. V. Kumar, "Data Encryption & Decryption Using Steganography," 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2020, pp. 697-702, doi: 10.1109/ICICCS48265.2020.9120935.

[28]. E. Venugopal, S. Ranganathan, V. Velmurugan and T. Hailu, "Design and implementation of video steganography using Modified CNN algorithm," 2020 Third International Conference on Advances in Electronics, Computers and Communications (ICAECC), Bengaluru, India, 2020, pp. 1-6, doi: 10.1109/ICAECC50550.2020.9339531.

[29]. J. Wu, B. Chen, W. Luo and Y. Fang, "Audio Steganography Based on Iterative Adversarial Attacks Against Convolutional Neural Networks," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2282-2294, 2020, doi: 10.1109/TIFS.2019.2963764.

[30]. Z. Xiang, J. Sang, Q. Zhang, B. Cai, X. Xia and W. Wu, "A New Convolutional Neural Network-Based Steganalysis Method for Content-Adaptive Image Steganography in the Spatial Domain," in IEEE Access, vol. 8, pp. 47013-47020, 2020, doi: 10.1109/ACCESS.2020.2978110.

[31]. W. Tang, B. Li, S. Tan, M. Barni and J. Huang, "CNN-Based Adversarial Embedding for Image Steganography," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 8, pp. 2074-2087, Aug. 2019, doi: 10.1109/TIFS.2019.2891237.

[32]. P. Wu, Y. Yang, and X. Li, ‘‘Image-into-image steganography using deep convolutional network,’’ in Proc. Pacific Rim Conf. Multimedia. Cham, Switzerland: Springer, 2018, pp. 792–802.

[33]. Q. Li et al., "A Novel Grayscale Image Steganography Scheme Based on Chaos Encryption and Generative Adversarial Networks," in IEEE Access, vol. 8, pp. 168166-168176, 2020, doi: 10.1109/ACCESS.2020.3021103.

[34]. Z. Zhang, G. Fu, R. Ni, J. Liu and X. Yang, "A generative method for steganography by cover synthesis with auxiliary semantics," in Tsinghua Science and Technology, vol. 25, no. 4, pp. 516-527, Aug. 2020, doi: 10.26599/TST.2019.9010027.

[35]. S. Fathi-Kazerooni and R. Rojas-Cessa, "GAN Tunnel: Network Traffic Steganography by Using GANs to Counter Internet Traffic Classifiers," in IEEE Access, vol. 8, pp. 125345-125359, 2020, doi: 10.1109/ACCESS.2020.3007577.

[36]. L. Chen, R. Wang, D. Yan and J. Wang, "Learning to Generate Steganographic Cover for Audio Steganography Using GAN," in IEEE Access, vol. 9, pp. 88098-88107, 2021, doi: 10.1109/ACCESS.2021.3090445.

[37]. J. Liu et al., "Recent Advances of Image Steganography With Generative Adversarial Networks," in IEEE Access, vol. 8, pp. 60575-60597, 2020, doi: 10.1109/ACCESS.2020.2983175.

[38]. P. Bas, T. Filler, and T. Pevný, ‘‘‘Break our steganographic system’: The ins and outs of organizing BOSS,’’ in Information Hiding, T. Filler, T. Pevný, S. Craver, and A. Ker, Eds. Berlin, Germany: Springer, 2011, pp. 59–70.

[39]. Z. Liu, P. Luo, X. Wang, and X. Tang, ‘‘Deep learning face attributes in the wild,’’ in Proc. IEEE Int. Conf. Comput. Vis. (ICCV), Dec. 2015, pp. 3730–3738.

[40]. J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, and L. Fei-Fei, ‘‘ImageNet: A large-scale hierarchical image database,’’ in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., Jun. 2009, pp. 248–255.

[41]. L. Deng, ‘‘The MNIST database of handwritten digit images for machine learning research [best of the Web],’’ IEEE Signal Process. Mag., vol. 29, no. 6, pp. 141–142, Nov. 2012**.**