ISSN 0315-3681 Volume 122, 2025

A high-capacity Coverless Image Steganography based on the Local Binary Pattern feature and WGAN model

Vijaysinh K. Jadeja[1*], Dr. Harsha Padheriya[2], Bharat Harilal Nagpara[3], Mayank P. Devani[4]

[*]Research Scholar, Department of Computer Engineering, Faculty of Engineering &Technology, Monark University, Ahmedabad.
[2] Associate Professor, Department of Computer Engineering, Monark University, Ahmedabad,
[3] Assistant Professor, Government Engineering College, Rajkot.
[4] Assistant Professor, Department of CE/IT, SAL College of Engineering Ahmedabad,

***ABSTRACT*: -**

By concealing a hidden message inside a cover image without changing it, the idea of coverless image steganography increases the image's resistance to image steganalysis tools. This strategy outperforms conventional high-capacity techniques that use several cover images as stego images, making them unsuitable for real-time applications. The study explores the effectiveness of coverless information concealing by using Wasserstein Generative adversarial networks and the Local Binary Pattern (LBP) feature to transmit sensitive data using a single cover image.In order to generate a sufficient number of distinct hash codes, the embedding process requires overlapping image blocks. To do this, an image must be divided into blocks, the hash code must be determined, and the secret message must be linked to image blocks that have the same hash code. To speed up the embedding process, a lookup table is created. A meaningful, uncorrelated image is created by feeding the generated stego image into the Generative Adversarial Networks model. This image is then transmitted to the recipient, where it is processed by the Wasserstein Generative Adversarial Networks model to reconstruct the stego image. Research indicates that in order to produce a sufficient number of unique hash codes, overlapping image blocks are required.A single image would not be sufficient to finish the embedding process without this overlap. Sending a meaning-normal image that is unrelated to the stego image can accomplish the same goal as sending the stego image. Compared to existing covert information hiding strategies, this suggested method offers a larger capacity for information concealing and is more resilient to attacks during image processing. Additionally, this technique works quickly and provides better defense against detection tools.

***Index Terms*:** Coverless information hiding, Wasserstein Generative adversarial networks (WGAN), Image steganography.

1. Introduction

The Internet transmits a large volume of multimedia content, including military intelligence, private trade information, personal privacy, and other sensitive information. Ensuring the security of data transmission across public channels, such as the internet, has become a key problem due to the rise in cyberattacks and criminal activity. Malicious actors pose a major threat to both national and individual interests if they intercept and use such private information for illegal purposes. Because of this, the

problem of information security has grown more pressing and needs to be resolved right away [1].

A variety of tactics and procedures are used in information security to protect the availability, confidentiality, and integrity of data. Cryptography is the study and use of secure communication techniques when adversaries are present. It includes a variety of methods for data encryption and decryption, guaranteeing the information's integrity, authenticity, and confidentiality [2]. Cryptography makes it possible to turn private information into a form that cannot be read, making it visible but incomprehensible.

By hiding or embedding data inside another file or medium, data hiding—also referred to as information hiding—offers a way to overcome this difficulty and render it invisible to the untrained eye. Sensitive information can be transmitted securely using this technique without drawing undue attention. Steganography is an information-hiding technique that makes unseen communication possible.

Conventional picture steganography entails concealing information in digital media, including text, audio, video, and photographs. The digital cover media can be used to classify different types of steganography. Text steganography, image steganography, and audio/video steganography are the three main types of steganography. Since images are essential to the transmission of multimedia, image steganography is especially significant in this industry. The cover picture is altered during the embedding process, leaving behind evidence of these changes. Consequently, a number of steganalysis techniques are able to identify these traces and possibly reveal the concealed data [4]. Steganalysis is a method used to identify secret information in carriers by analyzing signs of alteration. Although it may be difficult for humans to detect such information, detection methods can utilize these traces of modifications to determine the presence of hidden data.

The fact that there is no cover in the picture does not mean that the carrier is not being used; rather, it is simply left in its original state. To encode the sensitive data, the carrier's intrinsic qualities—such as pixel brightness value, color, texture, edge, contour, and high-level semantics—are used. This method embeds the secret information directly into the carrier, avoiding the traditional steganography process of altering it. By examining the carrier's properties and linking them to the hidden data according to predetermined guidelines, coverless image steganography works. Therefore, to circumvent all current steganalysis techniques and improve security measures, coverless information concealing is implemented [1].

Cover images with features that represent hidden information are selected as stego-images using coverless information procedures, which are made to withstand steganalysis approaches. By creating hash sequences based on the image, a strong hashing algorithm can create relationships between portions of private messages and image properties. However, there are four limitations with existing coverless methods [25].

1. The number of stego-images utilized to send the secret information increases in tandem with the length of the secret message.
2. The capacity for embedding offered by current coverless techniques is limited.
3. Both the sender and the recipient must have large image databases.
4. Incorrect secret retrieval may result from network issues affecting the sequence of received stego pictures.

This study offers a novel method for information concealment without changing the cover image in order to overcome the aforementioned issues. The hash sequences of the cover picture are calculated by utilizing the Local Binary Patterns (LBP) feature, which increases their resilience to image processing attacks. Furthermore, the same goal as the stego image transmission can be accomplished by transmitting a meaning-normal image that has no connection to the stego image. The paper's subsequent sections start with Section 2, which offers a variety of studies centered on coverless picture steganography methods relevant to the paper's general structure. A thorough explanation of the principles of this method is given in Section 3. The suggested coverless steganographic technique for digital photographs is described in full in Section 4. The experimental data and their interpretation are presented in Section 5, and closing remarks are provided in Section 6.

2 Related works

A new coverless information hiding technique based on the Most Significant Bit of the cover image was presented by Yang and Lina [6]. The secret information is encoded in binary form using the pieces of the cover image. The mapping sequence Km determines the mapping between the binary secret information and the most significant bit (MSB) of the image fragments, producing a mapping flag Kf. The recipient can decrypt the stego image's secret information by using Kf and Km. Compared to other approaches, this one has a greater capability for information concealment and is resistant to steganalysis attacks.

It has a limitless peak signal-to-noise ratio (PSNR) and can conceal up to 2601 bits of secret data per carrier. This technique also successfully protects against JPEG compression attacks, low-pass filtering, salt and pepper noise, and steganalysis tools like AGWN.

A sophisticated method for hiding data in photos without changing their appearance has been developed by Anggriani and Kurnia [7]. This technique uses predetermined keys to link the secret data to the most significant bit of the lowest and highest pixels in each image fragment. Experiments have shown that this strategy not only provides a higher hiding capacity but also outperforms other comparable techniques in terms of security.

To improve the concealment capability of the CIHMSB approach, Shu-Fen Chiou [8] suggested two coverless information concealment approaches, E-CIHMSB and CBCIHMSB. While CBCIHMSB uses combination theory to attain greater average values, E-CIHMSB uses image segmentation to calculate averages. The number of average values strengthens the method's hiding ability. In order to demonstrate the method's resistance to steganalysis attacks, the study explores its resilience against AWGN, Salt & Pepper

noise, low-pass filtering, and JPEG compression attacks. The experiments' results show that the approach outperforms CIHMSB.

WYSAWIS is a new method for high-capacity coverless image steganography that was introduced by Fotso [9]. This technique creates a series of hash sequences for a specific block of a 4x4 image by first creating a 15-bit hash sequence for each block. The 15-bit portions of the secret message are mapped to the hash sequence of the appropriate block. A distributed data hiding approach is used to convey these positions, also known as location information, within a single cloud. This method efficiently overcomes the difficulties of transferring multiple stego images and building big image data sets. As cloud services become more widely used, location data transfer becomes both possible and undetectable.

To address these issues, Zhang [10] created a brand-new information-driven generative adversarial network (IDGAN). GAN, attention processes, and picture interpolation approaches are all combined in this IDGAN. The IDGAN replaces transposed convolution procedures with image interpolation to improve the quality of dense images and increases image accuracy by introducing an attention mechanism. In contrast to traditional techniques, the IDGAN may produce photographs that include private information without the use of cover photos. It has better anti-detection capabilities because it embeds information using GANs.

The model uses an image interpolation approach to maximize the steganography impact and an attention mechanism to improve image clarity and details. With an embedding rate of 0.17 bpp, experimental results show that the IDGAN obtains remarkable accuracy rates of 99.4%, 95.4%, 93.2%, and 100% on the MNIST, Intel Image Classification, Flowers, and Face datasets, respectively.

A new method for coverless information concealment is presented by Liu, Hailun, Chunyu Zhang, and Zhaojie Wang [11], which allows several messages to be sent within a single cover image. One party can generate a binary coding matrix that corresponds to the cover image by utilizing the bag-of-words concept to create a visual dictionary. After then, the cover image and secret messages are encrypted and converted into a series of coordinates before being delivered to a different party. The efficiency of the strategy in terms of resistance, capability, and concealment is confirmed by experimental data. Unlike current approaches, this technology can communicate more messages with a single image and does not require a large image collection. This approach broadens the scope of coverless information research and shows promise for a number of applications.

By using unsupervised learning to build a thorough grouping base, Lu, JianFeng, J. Ni, Li Li, Ting Luo, and C. Chang [12] provide a unique method for coverless information concealing. While texture estimation is used to determine image properties, the original image is used as a reference for encoding the concealed information. A link between the image features and the hidden message is created by training the entire grouping base. Steganographic images are created for data hiding by processing the secret message and

method together. Comparing this strategy to other covert information concealment methods, experimental results show its efficacy and feasibility.

A safe steganography system based on a generative mathematical model based on semi Quick Response (QR) coding and labyrinth game image production has been proposed by Seddik, Al-Hussien, Mohammed Salah, and Gamal Behery [13]. The encryption process and the concealing process are the two primary parts of this technology. Bits of the secret message are encrypted inside a semi-QR code image during the encryption process. The pregenerated code is then hidden inside the generated maze game graphic using the concealing process. The semi-QR code is extracted from the maze game image and the original secret message is recovered by the extraction and decryption operations. This technique has proven to be strong against prospective attackers, operate exceptionally well, and have a large hiding capacity when compared to other approaches.

Using OMR and RBML, Al Hussien, S. Saad, and Mohamed S. [14] presented a reliable and secure coverless picture steganography method. This technique uses a mapping function to represent binary fragments on a bubble sheet after the secret information has been encoded as a binary string. Following that, the recipient receives the bubble sheet with the encoded data on it. This method makes use of optical mark recognition (OMR) and rule-based machine learning (RBML) algorithms. The RBML system recognizes and marks circles according to right responses, simulating a student's actions during a bubble-sheet T/F exam.

The OMR algorithm is designed as a cost-effective substitute for pricey scanners. The secret message encoded during the mapping process is revealed by extracting the right responses from the mapped bubble sheet by combining the OMR and RBML algorithms during the mapping phase.

3 Preliminaries

3.1 LBP

Rotation and gray invariance are two advantages of the picture texture descriptor known as LBP, or local binary pattern. In a 3x3 frame, it entails comparing the gray values of the central pixel with those of the eight neighboring pixels [27]. A surrounding pixel is given a value of 1 if its value is greater than the value of the central pixel; if not, it is given a value of 0. Figure 1 illustrates how this procedure produces an 8-bit binary number that records texture details.

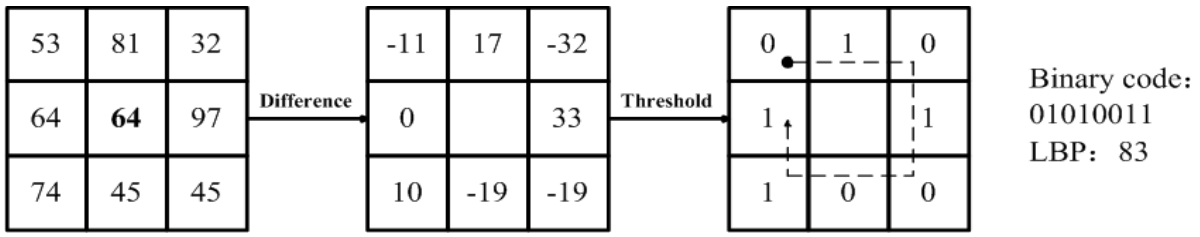

Figure 1: The generation of LBP value

3.2 RSA encryption technique

The RSA cryptosystem is a fundamental and popular encryption technique that was created by Ron Rivest, Adi Shamir, and Len Adleman. The creation of key pairs and encryption-decryption algorithms are highlighted.
A public key and a private key make up the RSA key pair, which is used for encryption. By selecting two large prime integers (p and q) and calculating n=p*q, the RSA modulus (n) is created. Usually 512 bits, n should be a big number to provide strong encryption. With no common factors other than 1, the resultant number (e) must be more than 1 and less than (p - 1) (q - 1). The RSA public key, which is made public, is made up of the values (n, e).

The difficulty of determining the two primes needed to obtain n in an acceptable amount of time is what gives RSA its security. Using p, q, and e, the private key (d) is calculated. Since d is the inverse of e modulo (p - 1)(q - 1), it must be less than (p - 1)(q - 1) when multiplied by e.

Once a key pair is established, RSA encryption and decryption become straightforward and computationally efficient. It requires plaintext to be expressed as a series of numbers less than n and works with numbers modulo n rather than bit strings as symmetric key encryption does. Data exchanged between the sender and the recipient will be encrypted using this technique. The locations of the image blocks used to insert the concealed message are stored in a different file; the x and y coordinates of each image determine its location. The location data file is encrypted with RSA before being sent to the recipient.

3.3 Wasserstein Generative Adversarial Network

An enhancement of the generative adversarial network, the Wasserstein Generative Adversarial Network (also known as the Wasserstein GAN) offers a loss function that is directly related to the quality of the generated images and improves stability during model training. Random noise z is commonly utilized as input when using the WGAN model to generate handwritten text. The model can still produce an independent image IMG' that is unrelated to the stego image being utilized, even if this random noise z is substituted with a stego image.
It is now possible to generate an independent image that is unrelated to the stego image by feeding in the stego image and using WGAN to train the generative model database [26]. The created image is then used as input for the generative model database to produce another image that visually resembles the stego image after this independent image has been given to the recipient. Figures 2 and 3 contain the flow charts that show the complete experiment.

Figure 2: the flow chart of WGAN

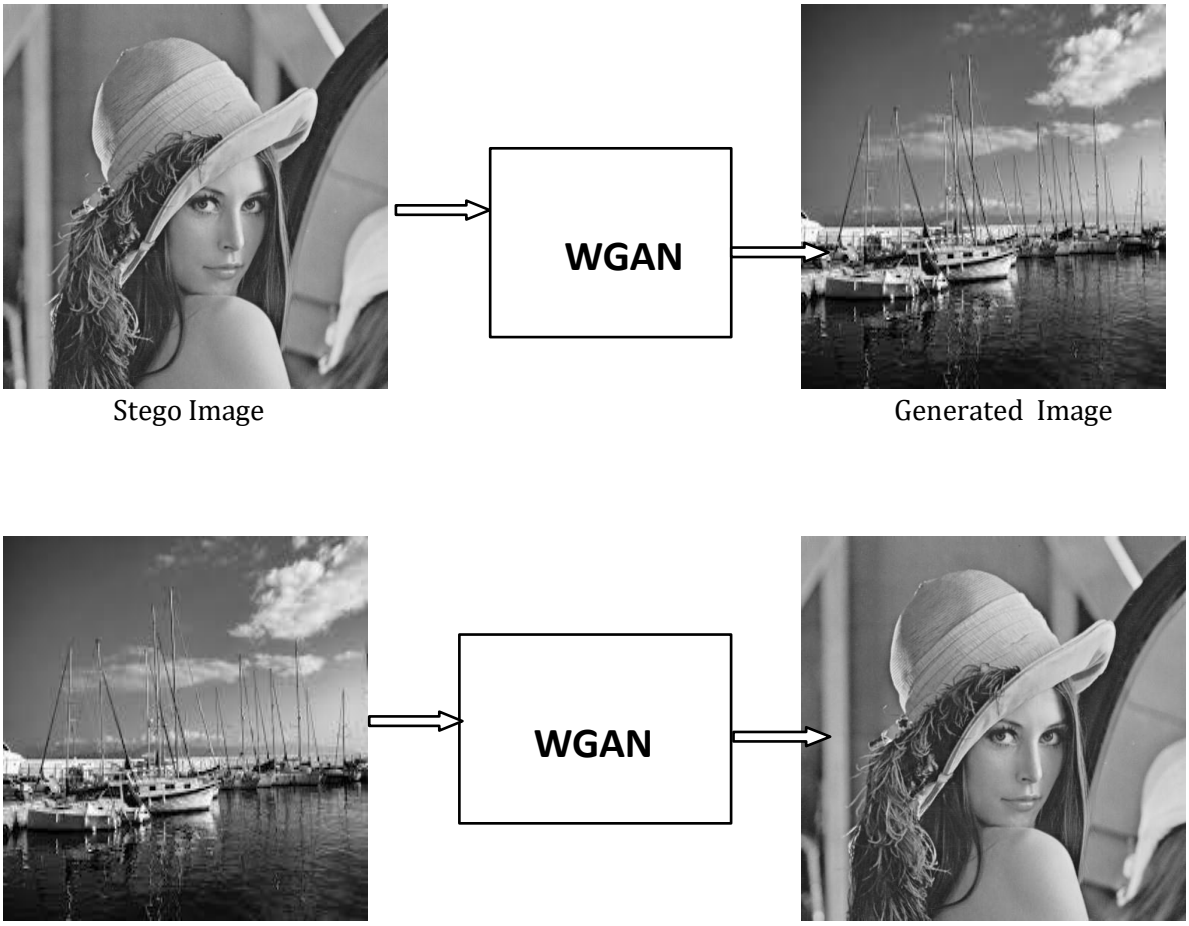

Figure 3:
The flow chart of generative model

D and G engage in a two-player minimax game within the WGAN framework, utilizing the value function V (G; D).

min max V(D,G)= Ex~pdataxlogDx+Ez~pz(z)log(1-DGZ) (1)

The likelihood that x, rather than pg, originated from the data is shown by the formula D(x). The objective is to improve D's training in order to increase the precision of categorizing G's samples and training examples. In parallel, G is trained to minimize [log (1-D(G(Z))]. A gradient ascending step on D and a gradient descent step on G start the training process. Below is a summary of the update guidelines.

Maintain the constant value of G while adjusting the model D by $\theta D \leftarrow \theta D + \gamma D \nabla DL$ with

$$\nabla DL = \partial\partial\theta D\{Ex\sim pdataxlogDx,\theta D + Ez\sim Pnoise(z)log(1-DGZ,\theta D,\theta D)\} \quad (2)$$

Maintain the constant value of D while adjusting the model G by $\theta G \leftarrow \theta G + \gamma G \nabla GL$ where

$$\nabla GL = \partial\partial\theta G\{Ez\sim pdatazlog(1-DGZ,\theta G,\theta D) \quad (3)$$

The Wasserstein distance is alternatively known as the Earth-Mover (EM) distance.

$$W(Pr,Pg)=\gamma\sim\Pi(Pr,Pg)infEx,y\sim\gamma[\|x-y\|]$$

γ(x, y) is a subset of all joint distributions denoted by γ(Pr, Pg), where Pr and Pg are the corresponding marginal distributions. In essence, γ(x, y) represents the amount of "mass" that needs to be transferred from x to y in order to convert the distributions Pr into Pg. As a result, the EM distance represents the cost associated with the most effective transportation configuration.

4. The proposed information hiding approach

Lookup table generation, information extraction, information embedding, WGAN, and hash code construction are the five main components of the suggested methodology. Establishing a link between hash codes generated from a cover image and secret message characters is the basic idea underlying this method. This method computes hash codes from picture blocks using the LBP Feature, introducing a coverless information concealing strategy. This work communicates a hidden message utilizing a single stego-image, in contrast to current covert information concealing approaches. This is done by extracting several different hash codes from the cover image. As a result, the recommended technique is used to divide the cover image into portions that partially overlap.

Although this might affect picture processing resistance, it has a number of benefits, including a greater concealing capacity, less bandwidth needed to send the secret message, the removal of laborious image searching and indexing tasks, and the lack of a need for a sizable imagedatabase.

A fixed-length binary hash algorithm is used to convert each block of the cover image into the corresponding ASCII code in order to encode a hidden message in the image. At the same time, the secret message's characters are changed to ASCII code. During the embedding process, each character in the secret message is compared to the hash code that was generated from the image block based on its ASCII value.

The locations of the matched blocks are then noted in a file. A generative model processes the stego image to produce a semantically normal independent image from a database before sending it to the recipient. The receiver then receives the resultant image via transmission. It is crucial to remember that no information pertaining to the secret data is included in the transmitted image. To guarantee secure communication, the location data file is encrypted and acts as a shared secret key between the sender and the recipient.

After the sender sends a standard solo image, the recipient uses a generative model to create a stego image from the received image. The recipient then uses the created stego image in conjunction with the location file to decrypt the location information file and compute the hash code. The hidden message is then revealed by converting the hash codes into their matching ASCII codes. Figure 4 elaborates on the sequential procedure of the proposed method.

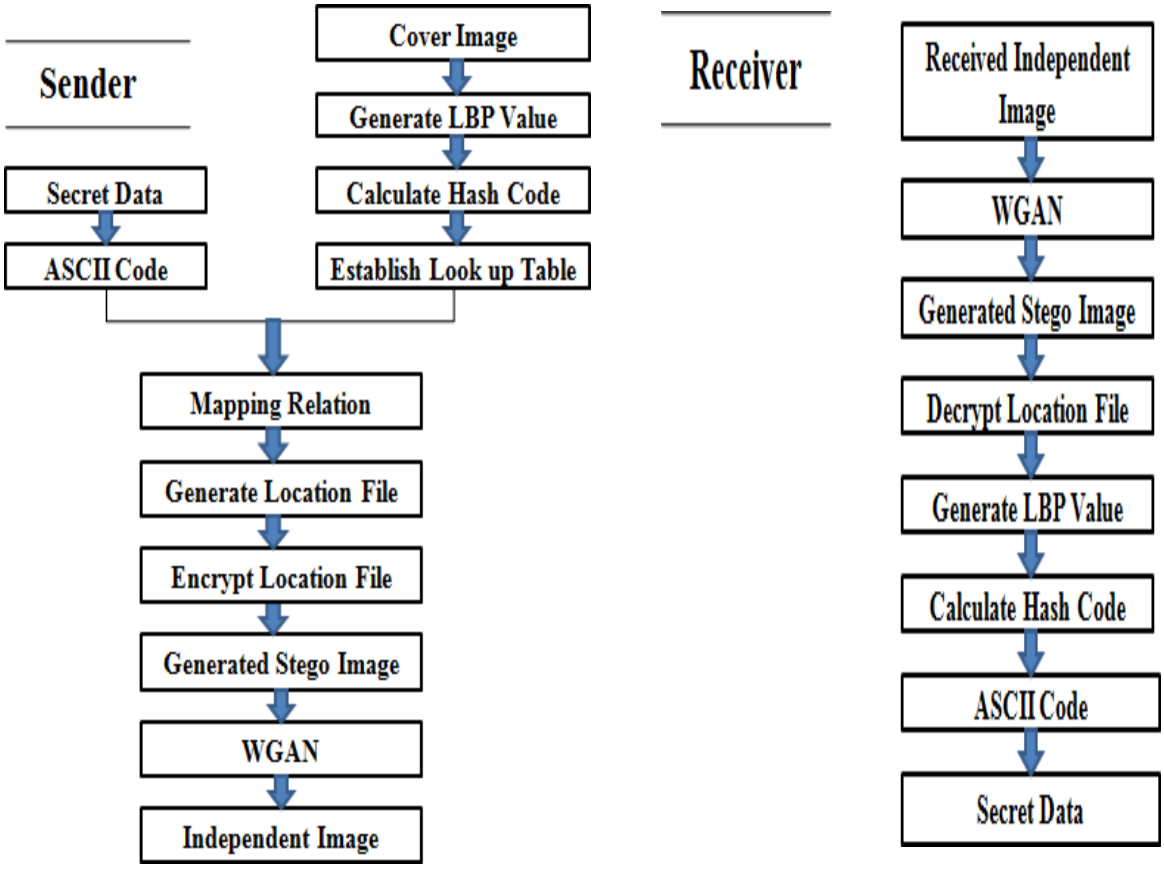

Figure 4: Proposed Method

4.1 Calculation of a binary hash code

The local content of an image block is used to generate the hash code, which is a predefined binary sequence of specified length. A hash code that corresponds to a specific segment of private information can be used to represent each image block. The LBP Feature, an operator used to describe an image's local texture properties, is used in this work to calculate the hash code. Gray invariance and rotation invariance are two noteworthy benefits of LBP. Figure 5 shows the procedure for determining the hash code from each image block; further information is given in the following sections.

Step 1: The cover image is split into blocks with size 3 ×3 as

B1,B2,B3…Bn Where n is the number of blocks.

Step 2: For Each Block, gray value of the adjacent 8 pixels is compared with the center pixel in the Block. If the surrounding pixel value is greater than the central pixel value, the pixel is marked as 1, otherwise 0.

Step 3: Generate 8bits binary string using arrangement which is given in figure.

Step 4: At Last, convert 8-bit binary number to a decimal number which is denoted as a LBP Value.

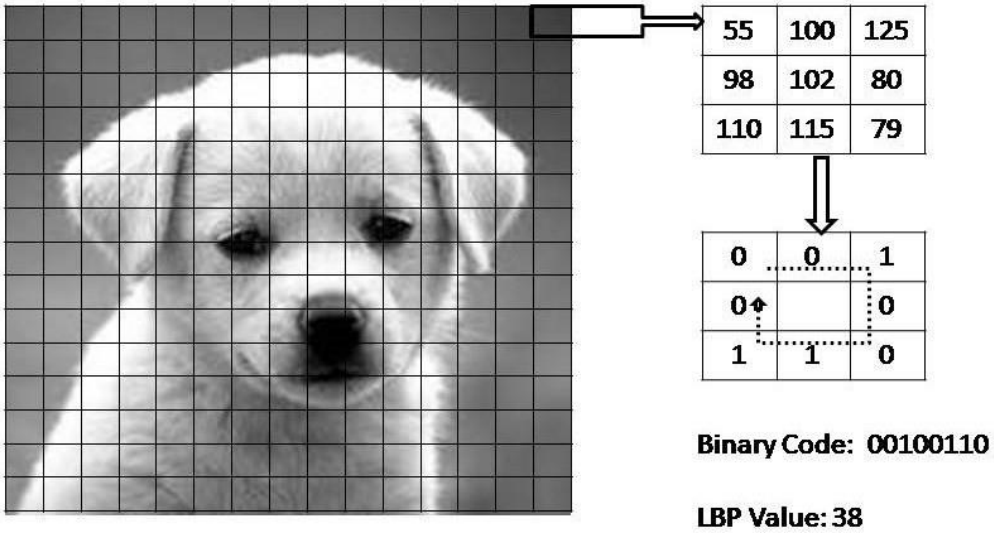

Figure 5: Calculation of a binary hash code

4.2 Establishment of a lookup table

Numerous 8-bit hash codes, each of which corresponds to a distinct image block, can be generated from the provided example. For the purpose of embedding, these hash codes are subsequently transformed into their corresponding ASCII equivalents. Every character in the secret message is converted into its corresponding ASCII code value during the embedding process, allowing it to be linked to one or more image blocks that have the same hash code. A lookup table is made for the cover image to make it easier to find image blocks that match each message character.

Following the conversion of each image block into its ASCII code, the position and hash code of each block are recorded using the lookup table. The block's placement inside the image is determined by the coordinates of the first pixel's upper-left corner. Figure 6 shows how the lookup table is organized.

	Hash Code	Block Coordinate(X,Y)	Mask
1st Block →	95	(1,1)	0
2nd Block →	75	(1,4)	0

3rd Block →	224	(1,7)	1
4th Block →	255	(1,10)	0
→	...	...	...
Nth Block →	221	(n,n)	1

Figure 6: The lookup table structure

4.3 Information Hiding

Sensitive information is protected by using a proper cover image to hide the data before sending it to the intended recipient as a stego-image. This information-embedding method is applied at the sender's end. The sender must use a unique cover image for every new secret message in order to increase the approach's security. The following steps are included in the embedding process:

Step 1: In order to protect from vulnerable to a rescaling attack, the cover image is adjusted to a predetermined size of (M × N).

Step 2: The sender streamlines the embedding process by using picture blocks for hashing and creating a lookup table to hold the generated hash codes and the locations of the relevant blocks.

Step 3: Every character in the secret message is first converted to the appropriate ASCII code during the embedding process so that the correct image block(s) may be matched with the corresponding hash code in the lookup table. After that, a file with the matching block's location data is created. The matching block's mask field in the lookup table is set to 1. If the message character matches many blocks, the method uses the mask field to select the picture block that hasn't been used previously, increasing the embedding's security. Consequently, a character that appears in the message more than once can be matched with a completely different image block each time they appear.

Step 4: The location information file is encrypted using the RSA public-key encryption method once every message character has been matched to its corresponding image block.

Step 5: Then a stego-image is fed into the WGAN model; a unique and independent image is produced.

Step 6: The sender sends a generated independent image to the receiver, along with an encrypted file that contains a shared secret key between them.

4.4 Information Retrieval

To extract the concealed message characters from the stego image, the recipient must complete the following data gathering procedure.

Step 1: The recipient receives an independent image first.
Step 2: Next, a stego picture is created by feeding an independent image that was received into the WGAN model.

Step 3: The location information file is decrypted in order to identify the locations of the target picture blocks within the stego-image.
Step 4: Use the hash technique to determine the Block LBP value based on the decrypted location file.
Step 5: To determine the character of the secret message, the block's binary hash code is translated to its matching ASCII code.

5. Experimental Results and Analysis

Improving the capacity, security, imperceptibility, and robustness of coverless image steganography is the primary goal of this research. The effectiveness and efficiency of the suggested method were evaluated experimentally, and the results were used to contrast it with alternative coverless picture steganography strategies. The evaluation on 100 randomly selected photographs shows that our approach significantly increases the information hiding capability and successfully counters common harmful attacks.

(A) Lenna

(B)Baboon

(C) Boats

(D) Cameraman (E) Dog (F) House

Figure 6: Sample Image

5.1 Analysis of the number of unique hash codes

The embedding procedure heavily relies on the hash codes that are extracted from a cover image. The possibility of effectively embedding a secret message with a variety of characters in a single image rises when the hash codes are variable and span a large range of values. A maximum of 256 distinct hash codes can be produced as each block's hash code is 8 bits long. Overlapping blocks can be used to create enough unique hash codes to successfully insert a secret message in a single image. To compare the variations in the quantity of distinct hash codes between overlapping and non-overlapping blocks, an experiment was carried out. Both overlapping blocks with a two-third block width and non-overlapping blocks were used to compute the hash codes. Table 1 presents the results, which show that for the two images, overlapping blocks provide more unique hash codes than non-overlapping blocks. Thus, the proper implementation of the embedding process using single images requires the use of overlapping blocks.

Table 1: The number of unique hash codes

Image	**With overlapping blocks**	**With non-overlapping blocks**
Lenna	256	248
Baboon	256	234
Cameraman	256	230
Houses	256	240
Boats	256	229
Cameraman	256	241

In every trial, it is discovered that the blocks of the image partially overlap from the upper left corner to the lower right corner by two-thirds of a block width. The amount of distinct hash codes required to embed a single message in an image can be produced in this way.

5.2 Embedding Capacity

Eight bits of information can be stored in each image block using the suggested method. Thus, the hiding capacity of the suggested method can be determined by the number of picture blocks and the degree of overlap between blocks in the cover images. Generally speaking, the hiding capacity rises with the overlap. The overlap in the suggested method is two-thirds of the block width, and the sub-block size is H × H = 3 × 3. It is possible to compute the hiding capacity (C) as

$$C=MH\text{-}2X\ MH\text{-}2\ \text{For overlapping blocks}MHX\ MH\ \text{For Non-overlapping blocks} \quad (4)$$

Table 2 computes the hiding capacity of the suggested method for a 512 by 512 grayscale image. The ability of several ways to conceal information is seen in this table. Even when non-overlapping blocks are utilized for embedding, it can be shown that our method has a larger hiding capacity than other methods in the literature.

Theoretically, an image's maximal embedding capacity is unlimited. In actuality, the only constraint on this capability is the amount of time required to conceal and recover the location data. The hiding capacity of the various methods is displayed in Table 2. Even if we take into account the minimum capacity, it is clear that the suggested method offers a better capacity than the current approaches.

.

Table 2: The number of unique hash codes

Approach	**Capacity (bits/image)**
Zheng's method [15]	18
Faster-RCNN [18]	20 and 25
MSIM [23]	36
Zou et al. [24]	80
Abdulsattar's method [16]	6272

Proposed method	491520 - ∞

5.3 Undetectability analysis

In order to prevent third parties from discovering any hidden information, the cover image must be extremely similar to the original image in order to be considered undetectable. Our approach preserves the original image during the hiding process, in contrast to traditional methods that alter the cover image to encode secret data. Steganalysis methods are successfully thwarted by this method, guaranteeing the confidentiality of the encoded data.

Additionally, using WGAN is essential for improving the suggested algorithm's undetectability. In real-world applications, this method makes it possible to create an independent, meaningful image that has nothing to do with the stego image that is meant to be transmitted. Since this capacity successfully satisfies the majority of requirements, we hypothesize that sending a meaningful and independent image to the recipient is sufficient when conveying a stego image. Instead of sending the stego image directly, the recipient can use the communicated image to create a visually equivalent image to the secret one by entering it into the generative model database.

Furthermore, there are no visual clues for possible attackers in the transmitted image, which makes image steganography analysis useless because it does not include any information from the stego image. As a result, this approach effectively avoids detection by any steganalysis instrument now in use, strengthening the image's security.

5.4 Image Quality Assessment Parameters Analysis

To evaluate the image quality, we used a number of measures, such as peak signal-to-noise ratio (PSNR) and structural similarity (SSIM). The pixel errors between the original and stego image are calculated using PSNR. A higher quality stego image is indicated by a higher PSNR score. The peak value of PSNR, which is expressed in decibels (dB), represents the highest value found in the picture data. The maximum value for an 8-bit unsigned integer data type is 255.

$$PSNR=10\log_{10}\frac{2552}{MSE} \quad (5)$$

The mean square error (MSE) is utilized to quantify the resemblance between the cover image and stego image. It can be calculated using the equation 6.

$$MSE=\frac{1}{M\,X\,M}\sum_{i=1}^{M}\sum_{j=1}^{M}\left(L_{ij}-L'_{ij}\right)^2 \quad (6)$$

The similarity between the stego image and the cover image is measured using the SSIM index. The range of its scale is -1 to +1. The SSIM equals 1, which is the optimum value,

when the cover picture and the stego image match. Equation 7 provides a mathematical representation of this.

$$SSIM=2\ p\ \ q\ +c1(2\ \sigma xy+c2)(p)2+(q)2+c1(\sigma x2+\sigma y2+c2) \quad (7)$$

Let p and q stand for the cover image's and the stego image's respective mean pixel values. The covariance between the cover picture and stego image is indicated by σxy, while the standard deviation of the two images is represented by σx2 and σy2. The suggested method conceals confidential information without changing the stego picture. This indicates that the stego image and the cover image are the same.

Table 3: Image Quality Assessment Parameters Analysis

Methods	**PSNR**	**SSIM**	**QI**
Sahu's Method[17]	51.30	0.9988	0.9965
Muhuri et al. [9]	51.668	0.998	0.997
Sahu and Swain [12]	48.200	0.997	0.997
Proposed Method	∞	1	1

Sahu's technique [12], Muhuri et al. [9], Sahu's method [17], and the proposed method are compared in Table 3 with respect to hiding capacity, PSNR, SSIM, and Qi. Table 3 shows that, in terms of concealing ability, our method outperforms other ways in terms of PSNR, SSIM, Qi, and information-hiding capability.

5.5 Robustness

The use of grayscale photographs to hide information is examined in this research. An independent image is susceptible to a variety of interference types, including internal noise and flaws in communication components, when it is produced and sent via traditional methods. These elements have the potential to distort the image, which will impact the quality of the hidden information extraction.

Bit Error Rate (BER)

The performance of the method is evaluated based on the Bit Error Rate (BER) criterion, which serves as a measure of its robustness.

BER= NmNnX 100%(8) Where, Nm denotes the count of erroneous bits while extracting concealed information from the stego image, whereas Nn signifies the overall number of bits of secret information to be concealed.

In the event that the BER is 0, no mistakes have been found. The successful and precise recovery of the secret bits shows that the method is totally impervious to this attack. On the other hand, if the BER is higher than zero, then indicates that some secret bits were altered or compromised during the assault. This implies that the method is not entirely impervious to this specific assault.

Correlation Coefficient (CC).

CC utilizes an equation to determine the level of similarity between the cover image and stego image.

$$CC=Xi\text{-}Xm(Yi\text{-}Ym)(Xi\text{-}Xm)2(Yi\text{-}Ym)2 \quad (9)$$

Let Xi and Xm stand for the intensity of the ith pixel and the cover image's mean intensity, respectively. In the same way, Yi denotes the Stego image's ith pixel's intensity, whereas Ym denotes the image's mean intensity.

When two images are absolutely identical, the correlation coefficient is 1, when they are completely uncorrelated, and when they are completely anti-correlated, it is -1.

Not all types of content damage during communication can be totally eliminated, including image noise, JPEG compression, rescaling, brightness change, contrast adjustment, and related issues. Any stego image chosen from the database to hide the secret data segment can be the target of these kinds of attacks. Consequently, it is essential that these variables be resilient to the information that is taken from the image. The following attacks are considered in the experiments.

(a) Gaussian noise with variance (v) = 0.001 to 0.005.

Attack type	variance	CC	BER
Gaussian noise	0.001	1	1
	0.002	1	1
	0.004	1	1
	0.005	1	1

(b) JPEG compression attacks with Quality factors (Q)=10,30,40,50

Quality factors (Q)	CC	BER
10	1	1
30	1	1
40	1	1

50	1	1

(c) Salt-pepper noise with rate (r) = 1% to 5%.

Attack type	**% Density of noise**	**CC**	**BER**
Salt and pepper	1%	1	1
	2%	1	1
	4%	1	1
	5%	1	1

(d) Median filtering with window size (w) of 3 × 3 and 5 × 5.

Attack type	**Size**	**CC**	**BER**
Median filter	3 × 3	1	1
	5 × 5	1	1

(e) Mean filtering with window size (w) of 3 × 3 and 5 × 5.

Attack type	**Size**	**CC**	**BER**
Mean filter	3 × 3	1	1
	5 × 5	1	1

(f) Gaussian low-pass filtering with window size (w) of 3 × 3 and 5 × 5.

Attack type	**Size**	**CC**	**BER**
Gaussian filter	3 × 3	1	1
	5 × 5	1	1

6. Conclusions

The effectiveness of using Wasserstein Generative Adversarial Networks (GANs) in conjunction with the Local Binary Pattern (LBP) feature for coverless information concealment is examined in this paper. Unlike other approaches in this domain, the proposed method embeds a secret message in a single cover image by dividing the image into blocks that partially overlap. Overlapping picture blocks are necessary for the embedding process to provide a wide enough range of distinct hash codes. In order to do this, an image must be divided into blocks, the hash code must be extracted, and the secret message must be connected to image blocks that have the same hash code. The embedding procedure is streamlined by creating a lookup table. A coherent, uncorrelated image is then produced by feeding the stego image into the Generative Adversarial Networks model. This image is then transmitted to the recipient, where it is processed by the Wasserstein GAN model to reconstruct the stego image. Studies show that overlapping picture blocks are necessary to get a significant number of distinct hash codes; without this overlap, one image would not be sufficient for the embedding. A meaningful, unrelated image can be sent in place of the stego image to accomplish the same objective. Compared to current covert information-hiding strategies, the suggested approach improves the ability to conceal information and provides better defense against attacks during picture processing.

7. References

[1] Kanzariya Nitin, Dhaval Jadhav, Gaurang Lakhani, Uttam Chauchan, and Lokesh Gagani. "Coverless Information Hiding: A Review." In Proceedings of International Conference on Computational Intelligence: ICCI 2021, pp. 109-135. Singapore: Springer Nature Singapore, 2022.

[2] Gagnani, Lokesh P. "Multi Objective Association Rule Mining with Soft Computing Approach." In 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), pp. 968-971. IEEE, 2020.

[3] Gagnani, Lokesh, and Kalpesh Wandra. "Data Mining Task Optimization with Soft Computing Approach." In Proceedings of the Third International Conference on Computational Intelligence and Informatics: ICCII 2018, pp. 567-577. Springer Singapore, 2020.

[4] K Kanzariya Nitin, V Nimavat Ashish –"Comparison of various images steganography techniques" In 2013, International Journal of Computer Science

[5] Kanzariya, Nitin, Ashish Nimavat, and Hardik Patel. "Security of digital images using steganography techniques based on LSB, DCT and Huffman encoding." In Proceeding of international conference on advances in signal processing and communication-elsevier. 2013.

[6] Yang, Lina, Haiyu Deng, and Xiaocui Dang. "A novel coverless information hiding method based on the most significant bit of the cover image." IEEE Access 8 (2020): 108579-108591.

[7] Anggriani, Kurnia, Shu-Fen Chiou, Nan-I. Wu, and Min-Shiang Hwang. "A high-capacity coverless information hiding based on the lowest and highest image fragments." Electronics 12, no. 2 (2023): 395.

[8] Anggriani, Kurnia, Shu-Fen Chiou, Nan-I. Wu, and Min-Shiang Hwang. "A Robust and High-Capacity Coverless Information Hiding Based on Combination Theory." Informatica 34, no. 3 (2023): 449-464.

[9] Muhuri PK, Ashraf Z, Goel S (2020) A novel image steganographic method based on integer wavelet transformation and particle swarm optimization. Appl Soft Comput 92:1–26

[10] Zhang, Chunying, Xinkai Gao, Xiaoxiao Liu, Wei Hou, Guanghui Yang, Tao Xue, Liya Wang, and Lu Liu. "IDGAN: Information-Driven Generative Adversarial Network of Coverless Image Steganography." Electronics 12, no. 13 (2023): 2881.

[11] Liu, Hailun, Chunyu Zhang, Zhaojie Wang, Chenfei Guo, Peidong Gou, Liying Shan, and Zewei Lu. "To deliver more information in coverless information hiding." Multimedia Tools and Applications 83, no. 3 (2024): 7215-7229.

[12] Sahu AK, Swain G (2020) Reversible image steganography using dual-layer lsb matching. Sensing and Imaging 21(1):1–21

[13] Seddik, Al-Hussien, Mohammed Salah, Gamal Behery, Ahmed El-harby, Ahmed Ismail Ebada, Sokea Teng, Yunyoung Nam, and Mohamed Abouhawwash. "A New Generative Mathematical Model for Coverless Steganography System Based on Image Generation." Computers, Materials & Continua 74, no. 3 (2023).

[14] Al Hussien, S. Saad, Mohamed S. Mohamed, and Eslam H. Hafez. "Coverless image steganography based on optical mark recognition and machine learning." IEEE Access 9 (2021): 16522-16531.

[15] Zheng, S., Wang, L., Ling, B., Hu, D. (2017). Coverless information hiding based on robust image hashing. In Intelligent Computing Methodologies: 13th International Conference, ICIC 2017, Liverpool, UK, August 7-10, 2017, Proceedings, Part III 13 (pp. 536-547). Springer International Publishing.

[16] Abdulsattar, F. S. (2021). Towards a high capacity coverless information hiding approach. Multimedia Tools and Applications, 80(12), 18821-18837.

[17] Sahu AK, Swain G (2019) A novel n-rightmost bit replacement image steganography technique. 3D Research 10(2):1–18

[18] Zhou, Z., Cao, Y., Wang, M., Fan, E., & Wu, Q. J. (2019). Faster-RCNN based robust coverless information hiding
system in cloud environment. IEEE Access, 7, 179891- 179897.

[19] Xintao Duan1, *, Haoxian Song1, Chuan Qin2 and Muhammad Khurram Khan3 ”Coverless Image Information Hiding Based On Generative Model”,Tech Science Press 2018.

[20] Zhou, Z.; Su, Y.; Zhang, Y.; Xia, Z.; Du, S.; Gupta, B.B.; Qi, L. Coverless Information Hiding Based on Probability Graph Learning for Secure Communication in IoT Environment. IEEE Internet Things J. 2021.

[21] Sahu, A.K.; Swain, G. Reversible image steganography using dual-layer LSB matching. Sens. Imaging 2020, 21, 1–21.

[22] Zhou, Z.; Wu, Q.J.; Yang, C.N.; Sun, X.; Pan, Z. Coverless image steganography using histograms of oriented gradients-based hashing algorithm. J. Internet Technol. 2017, 18, 1177–1184.

[23] Cao, Y., Zhou, Z., Sun, X., & Gao, C. (2018). Coverless information hiding based on the molecular structure images of material. Computers, Materials & Continua, 54(2), 197- 207.

[24] Zou, L., Sun, J., Gao, M., Wan, W., & Gupta, B. B. (2019). A novel coverless information hiding method based on the average pixel value of the sub-images. Multimedia tools and applications, 78, 7965-7980.

[25] Kanzariya Nitin, Dhaval Jadhav, Lokesh Gagnani, Nilesh Maltare, and Kamakshi Kaul. "A high-capacity Coverless Image Steganography Based on OMR and Mapping Rules." Journal of Electrical Systems 20, no. 3 (2024): 1999-2006.

[26] Duan, Xintao, Haoxian Song, Chuan Qin, and Muhammad Khurram Khan. "Coverless Steganography for Digital Images Based on a Generative Model." Computers, Materials & Continua 55, no. 3 (2018).

[27] Qiu, A., Chen, X., Sun, X., Wang, S. and Guo, W., 2019. Coverless image steganography method based on feature selection. Journal of Information Hiding and Privacy Protection, 1(2), p.49.