High Capacity Coverless Information Hiding: A Survey

Vijaysinh K. Jadeja 1st , Dr. Harsha Padheriya 2nd , Archana Patel 3rd Mayank P. Devani4th

1st Department of Inforation Technology ,Sal College of Engineering, Ahmedabad, Gujarat

2nd Department of Computer Engineering,Institution of advance Research, Gandhinagar, Gujarat

3rd Department of Information Technology,Sal College of Engineering,Ahemdabad,Gujarat

4th Department of Information Technology,Sal College of Engineering,Ahemdabad,Gujarat

Abstract — In recent years, the rapid development of computer networks and digital multimedia technologies has contributed in the development of information concealing. Digital content typically contains the concealed information for copyright protection or private communication. Image steganography, whose objective is to employ cover images to hide a little quantity of secret information, is presently one of the most challenging situations and problems in the world of data security. Coverless image steganography, as opposed to traditional image steganography, modifies the image attributes rather than the cover image to deliver a secret message. As a consequence, The image's security is significantly increased, and the likelihood that steganalysis tools will recognise it is greatly decreased. Its fundamental tenet is to evaluate image qualities and link them to important data. This article includes several coverless steganography techniques as well as a summary of fundamental techniques based on hashing techniques, mapping relationships, and feature extraction. In conclusion, current approaches are examined, and potential future employment options are suggested.

Keywords: Image Steganography, coverless image steganography, information hiding, information security, DCT, DWT, DFT, GAN, DGAN.

I. Introduction:

Information security has become a major issue in many fields, including the economics, banking system, military, medical, and many other fields, as a result of the widespread use of the internet. Nowadays, a lot of data, including private information, secret passwords, trade secrets, secret military material, and secret information, is exchanged via the internet [2]. Data transmission security via open networks like the internet is receiving more attention as a result of the rise in cyberattacks and criminality.

Data security is a major concern in many fields, including the economics, banking system, military, healthcare, and other various recorded, due to the widespread use of the internet.

In the period of time, Information security made extensive use of encryption technologies. The most basic principle is to encrypt key data into "unreadable" ciphertext that can only be decoded by the receiver with the correct key [4]. The ciphertext obtained after encryption, on the other hand, is sometimes in the form of 'cryptic code,' which attackers seeking to decrypt it may easily read [8].

As a result, in some applications, such as covert communication, information insertion is favored over encryption since it conceals the communication's trail without generating suspicion from attackers or observers. The information hiding method involves changing the pixels of the cover image to hide hidden information; this implies that the cover image may be altered [9]. Image steganography was quickly found using automated steganography techniques. The changes made by embedding, on the other hand, will be preserved in the cover picture, allowing for effective identification of concealed secret information using technology; this detection step is also known as steganalysis. To solve this problem, the coverless information concealing strategy described by Sun in 2015. Coverless technology provides a direct mapping link between secret information and the hidden carrier based on the hidden carrier's properties. It doesn’t need to change carrier information, thus even if an attacker obtains the original carrier with the secret information, he will be unable to access it. CIH technology offers an anti-steganalysis capacity that is unrivalled.

An image, as we all know, is made up of a variety of feature data, including high-level semantics, pixel brightness value, colour, texture, edge, and contour. Zhou et al. investigated the algorithm that uses this idea. They proposed coverless information hiding using image and text in 2015. For information hidden with a proper feature description, it is possible to create precise connections with features and hiding data. It may communicate the created image, which is independent of the key information, in order to produce the same relevant information as the source images [19]. This method efficiently defends against steganalysis attacks and substantially improves the security of confidential information.

The remaining paper is arranged around the following sections: Section II discusses similar works, such as conventional image steganography, steganalysis, and coverless image steganography, as well as recent developments and significant difficulties. In this, first we show some basic method of the coverless image steganography in Section III. Section IV presents the Performance Evaluation. Section V presents the current key chal-

lenges and in the last, conclusion and further work is presented in Section VI.

II. Background Information and Similar Work

A. Traditional Image Steganography

Steganography is a covert communication technique that is invisible to the naked eye. The three elements of steganography are the carrier, the message, and the password. A message is placed within a carrier, often referred to as a cover-object, which conceals the message's presence. Steganography types can be categorised using digital cover media [4], [14]. The four primary kinds of steganography are (i) text steganography, (ii) image steganography, (iii) audio steganography and (vi) video steganography. Images are the most widely used cover objects in steganography. Only receivers who have the correct decoding key will be able to decode the message from a cover-object, also known as stego-key. The stego image is the cover-object with the covertly inserted message.There are two types of Image steganography methods.

- Spatial-domain Steganography
- Transform domain steganography.

The LSB technique [14] is the most popular and straightforward data concealment strategy. HUGO [5], WOW [6], UNIWARD [22], and other information-hiding algorithms have been built from the fundamental principles of the LSB algorithm. The concealed technique in the DWT, DFT, DCT and IWT are among the numerous transform domain steganography methods suggested. Nonetheless, it's not hard to determine that traditional image steganography changes the image's content to some amount, making it impossible to avoid detection by image steganalysis tools.

B. STEGANALYSIS

There are sure to be some alteration traces left behind when the embedding procedure involves changing pixel values of the cover image. As a result, we're faced with a problem that existing steganalysis tools can detect based on change traces. As a result, secret data would be visible [5]. The statistical anomalies are used to judge whether the information embedded in the carrier data is paramount [12]. The most important approach for steganalysis is to use characteristic extractors [10], such as SPAM [13], SRM [17], and others. SVM, decision trees, ensembles, and other common devices for researching classifiers are

significant for steganalysis. Now a day, neural network is highly used for steganalysis, and the experimental findings suggest that CNN can increase classification accuracy when used instead of traditional classifiers.

C. COVERLESS INFORMATION HIDING

Coverless information hiding is presented as a way of transmitting secrets without altering the cover image. The term "coverless" does not indicate that there is no need for a cover [2]. Coverless information hiding, unlike traditional image steganography, does not need changing the cover image; rather, it focuses on the image's basic characteristics to directly communicate concealed information. A proper feature description can be used to find links between feature information and hidden information.
Coverless steganography will be divided into two categories as show in fig. 1: Mapping Coverless steganography and Full structured Coverless steganography.
For structured steganography, according to particular criteria, the stego will be produced straight from the key data [10]. The researchers proposed a number of coverless structural steganography approaches based on this foundation. A completely structured algorithm provides low capacity. However, attacks on samples and the extraction of secret information, both of which need sophisticated computer help, will be difficult to counter.

In contrast to structured steganography, the presence of a mapping relationship is provided by mapping technique, in which establishing a meaningful link between the carrier and the secret information is how key information is expressed [15]. The number of image sample required rises exponentially with the increase in capacity in mapping approaches due to the limits of the mapping process [7]. The basic idea is to look at image features and map them to important information using a set of criteria based on the characteristics of image attribute. In this manner, the carrier may instantly communicate the necessary information. As a result, it significantly enhances image security by avoiding steganography recognition.

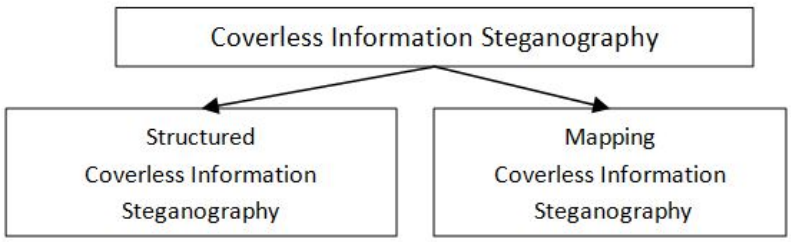

Fig. 1 Types of Coverless Information Steganography

Following are the main contributions made by Coverless Information Hiding:

1. No modifications will be made to the stego-image in order to execute covert communication.
2. Currently available steganalysis tools cannot detect secret information since the stego-image was not modified.

D. PROGRESS IN THE PAST FIVE YEARS

Zhou et al. [16] suggested that make an image database by downloading a collection of images from the internet. A robust technique creates a hash value for each image in the next phase. Using generated image hashes, images are then indexed in an inverted index structure in accordance with mutual sharing of image hashes between sender and receiver. Following that, the key message is sent as follows: The sender begins by converting it into a tiny quantity stream. Second, divide it into equal-length halves. Third, look for pictures with hash sequences that are appropriate for the key message parts. Finally, generated stego image send to the receiver. Zheng et al. presented a resilient hash method that creates an 18-bit binary hash sequence for each image using a Scale Invariant Feature Transform (SIFT) [1]. As a first stage, a local database (image database) will be generated on the fly, including images and hashes relating to each picture. However, the writers uncovered a flaw: the database included 218 images, each with its own hash, making it impossible to represent all 18-bit possibilities. To achieve the desired database capacity, authors represented every image with such a unique code of 18-bit hashes. Finally, secret message is divided into 18-bit segments large enough to accommodate the image hash code size, and a stego-image with a hash equal to the secret message segment is selected as the carrier to send to the receiver.

Wu et al. [14] support the "Grayscale Gradient Co-occurrence Matrix" technique, which performs as follows: the message is initially represented as a binary stream. After that, the binary streams are divided into eight-bit equal chunks. A turbo encoder is used to convert each 8-bit segment to 16 bits due to the rapid information flow. Finally, seek for an image that fits the 16 bit segment length, as specified by the mapping function.

Using Faster-RCNN, ZHILI ZHOU presented a strategy that supported the coverless information concealing approach in the Cloud Environment [6]. Throughout this process, the initial images with characteristics that might transmit essential information are used as stego-images. It's difficult to achieve desired protection against picture attacks with today's coverless information concealing methods, which

rely on precise image characteristics to hide information. Furthermore, their ability to hide is limited. To overcome these issues, we developed a unique robust image coverless information hiding technique based on Faster-RCNN. Faster-RCNN recognizes and locates objects in images, then uses their labels to deduce hidden information. The suggested approach may successfully withstand steganalysis and cannot arouse attackers' suspicion since the initial images with no alteration are utilized as stego-images. In terms of durability and capacity, the suggested system improves traditional coverless information concealing techniques.

III. FUNDAMENTAL FRAMEWORK

The coverless strategy is considered the foundation for securing secret data, and it is crucial to plan an efficient fundamental framework. Fig. 2 shows steadily improved coverless image steganography solutions. The feature extraction method and the mapping methods are significant discussed in this article. This paper presents the basic structure of coverless image steganography, as shown in Fig.2.

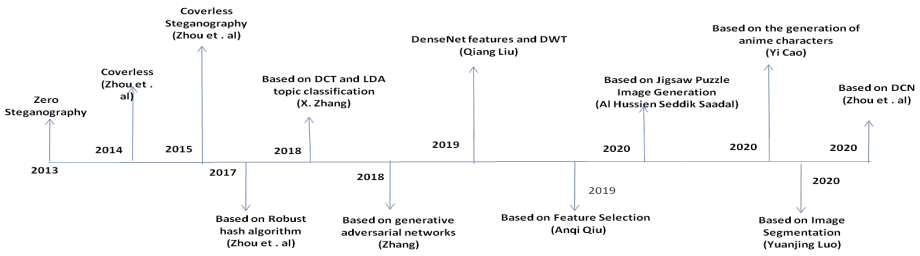

Fig. 2 Current Methods of Coverless image steganography.

A. Coverless image steganography based on DenseNet feature mapping [13].

The suggested CIS technique uses DenseNet feature mapping. To extract high-dimensional CNN features that are mapped into hash sequences, deep learning is used. To speed up the index speed of searching for hidden information and the DenseNet hash sequence for the sender, a binary tree hash index is constructed, and all matching images are then provided. Calculating the cover image's DenseNet hash sequence enables the recipient to successfully retrieve the secret information. The cover photos are unaltered during the whole steganography process.

The three elements of this approach are as follows:

1. Generation of hash sequence

The generation process for the hash sequence, which is based on mapping rules, is essential to the CIS since it determines how resilient the steganography system is against assaults. The method of creating a hash sequence is depicted in Figure 3, and the specific phases are listed below.

1. First, to extract features from a picture database, we utilize the pre-trained DenseNet121 network, which is described as

$$F_{ic} = DenseNet(P_{iic})$$

2. After that, Fic is divided into D blocks, and Bib is derived from the blocks.

$$B_{ib} = \{B_1, B_2, \ldots, B_D\}, 0 < ib \leq D < w$$

3. The feature coefficient Meib for each block Bib is determined by

Put eqution

2. Construction of binary tree hash index
3. Coverless image steganography
4. Extraction of secret information

C. Coverless Image Steganography Based on Image Segmentation [2]

In this paper, Image segmentation was supported by a coverless image steganography approach in this research. We utilize ResNet to extract semantic features and Mask RCNN to conceal information from an image. The ethical structural integrity of these selected object regions, which do appear to be in the image's visual centre, reduces intentional attack knowledge loss. Experiment outcomes demonstrated that our technique is more resistant to geometric attack than existing coverless image steganography methods.

1. The proposed steganography scheme

Mask RCNN is used to segment a large number of object regions in this framework. The required object regions are then chosen. To construct item area sequences and establish an index for feature matching, we use strong hash techniques. As a consequence, the recipient's stego-images are matched and delivered. Image segmentation, the development of an inverted index and the steganography technique make up the majority of this method's components.

2.1 Image segmentation

Semantic segmentation identifies all pixels in an image without regard for the enclosing box. Detecting items from a specific category are present in a picture and locating the objects are the two issues that object detection addresses. Semantic segmentation is coupled with object detection in instance segmentation. It could segment the recognized objects and forecast their position and category within a picture. Panoptic segmentation detects and segments the backdrop as well as identifying and segmenting all objects inside an image. For this type of task, Mask

RCNN is the recommended network; Fig. 7 shows how Mask RCNN may be used to perform object identification, instance segmentation, and panoptic segmentation.

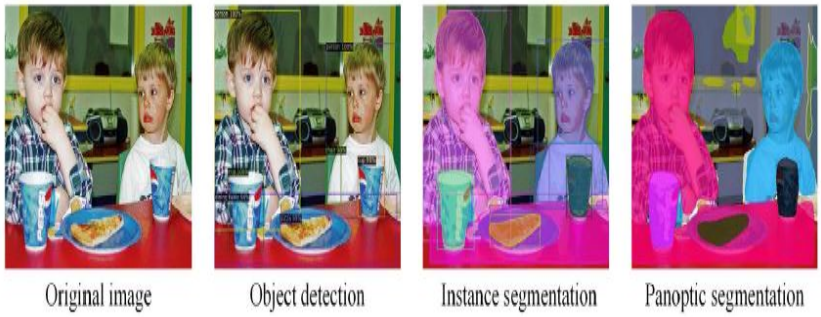

Fig.7. Visual examples of object detection and image segmentation [2]

2.2 Selection of object areas

Mask RCNN is used to partition all of the object regions in many images and calculate the number of different-sized object areas. The ratio is depicted in Figure 8. Small regions whose size is 0 to 5 KB are very easily lost and could not cover enough data. While large regions whose size is greater than 50KB are limited, areas of 5-25kKB are very suited to being chosen.

2.3 Construction of inverted index

To speed up the comparison of secret info and object areas, an index must be constructed. The inverted index structure, as shown in Fig. 9, includes entries for all possible 8-bit hash sequences. A collection of object regions including the related stego-images, as well as points that will be utilized to identify the item areas may be found under each entry. It's worth noting that each sequence code entry should include at least one picture to ensure that the image is found inside the index structure.

2.4 Steganography process based on image segmentation

As seen in Fig. 10, the sender divides the secret data into segments, matches it to object region, and extracts the stego-image and feature points that go with it. To ensure security, these image features will be encoded in reverse order. These photos are then emailed to the recipient. Mask RCNN is used by the receiver to extract the item regions from stego-images per feature point. Following that, the hash method is used to produce the item area sequences, which are then progressively concatenated to get secret information.

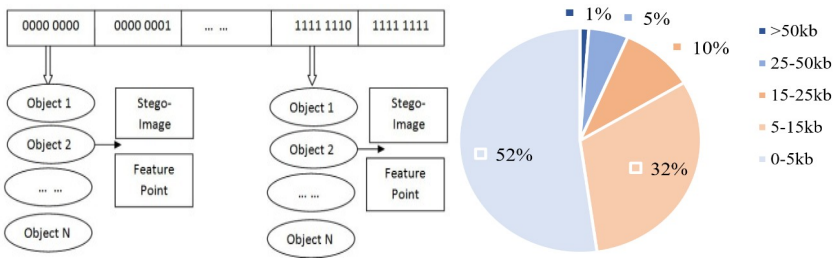

Fig.9. The inverted index [2]

Fig.8. Object areas with size [2]

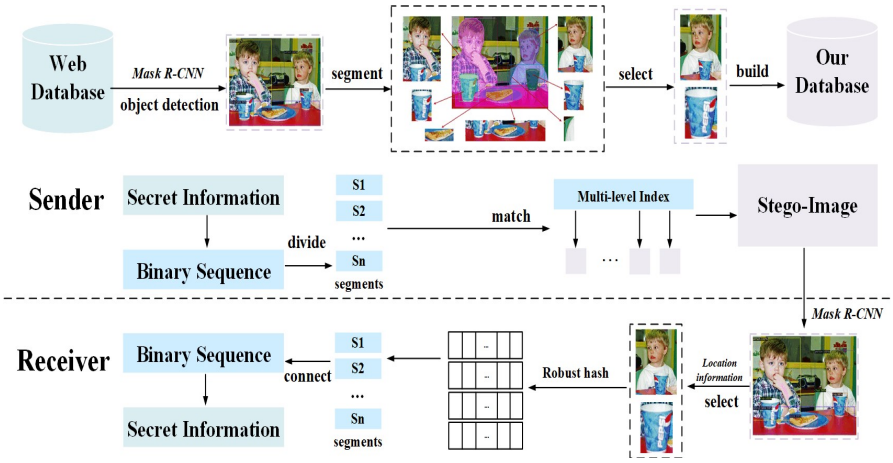

Fig.10. Flowchart of the proposed method[2]

D. Coverless information hiding based on the generation of anime characters [3].

In this approach, they offer a coverless information concealing approach for the creation of anime characters. It includes converting secret data into an anime character attribute label set, which is subsequently utilized as a driver for creating anime characters with GANs. The results show that, as compared to current approaches, the proposed method enhances hiding capacity by roughly 60 times and also performs well in terms of picture quality and durability.

It will be split into three modules based on the majority of functions.

- Create a label collection from sensitive information.
- index module for Location information
- Image creation module.

1. Create a label collection from sensitive information.

This study uses anime character attribute labels to represent secret information, as seen in Fig. 11. In this study, we'll look at 5 haircuts, 13 hair colours, 10 eye colours, and a range of other traits including blush, grin, open lips, and ribbon that have a high chance of appearing. In this piece, the secret information and labels set are converted using a long memory network (LSTM) as seen in Fig. 13[3]. For each anime character, the labels set format suggested in this work may be represented as hairstyle (2 bits), hair colour (3 bits), eye colour (3 bits), other characteristics 1 (2 bits), other attributes 2 (2 bits),..., other attributes n. (2bit).

2. Position index

10

Fig.13 shows how to figure out which of the anime characters' places indicated hidden information. In the position matrix, 0 indicates that the anime character in this position does not convey secret data and 1 indicates that the anime character in this position does convey secret data.

Fig.11.Secret information representation[3]

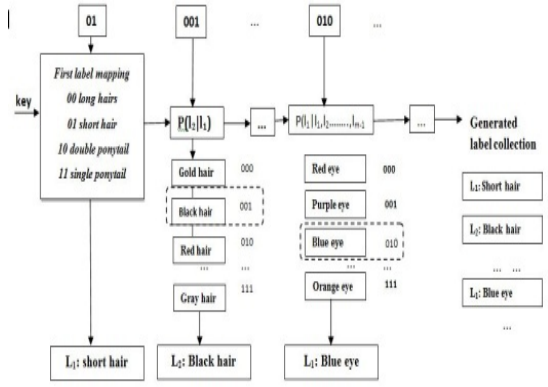

Fig. 12 Long memory network conversion example[3]

0	1	13	17	0	0	26	0
10	0	9	0	0	0	14	0
25	0	0	4	0	0	7	19
0	2	22	0	0	16	21	0
24	0	0	3	27	5	0	0
0	0	0	0	0	0	15	8
0	0	23	0	0	0	6	20
11	0	12	28	18	0	0	0

Fig.13 An example of an index[3]

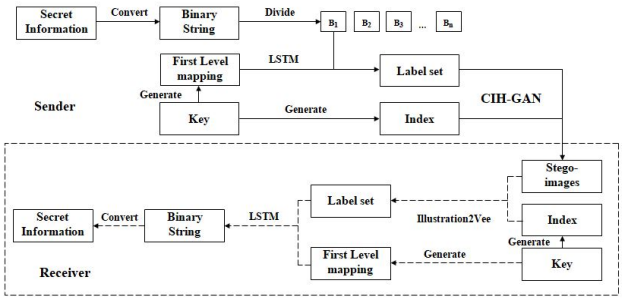

Fig.14 The framework of the proposed method[3]

3 Generation of stego-images

The anime character generating network is implemented on the CIH and creates animation images transmitting secret information at the index point, which is primarily restricted by the secret information labels established.

3.1 Information hiding (See Fig.14)

Step 1: The first classified piece of information is Convert the secure data series S = s1, s2, s3,... st to a binary string and segment it based on the label structure, then get the primary characteristic M and location index I= l'1, l'2, l'3,..., l't from the Key.

Step 2: Transfer the private data stream into the anime character attributes label sequence I = l1, l2, l3... lt using the LSTM model.

Step 3: Construct the animation character by providing secret information at the index position of the stego-image.

Step 4: Finally, deliver the stego-image created to the recipient.

3.2 Information extraction

As seen in Fig. 14 the extraction process is to extract attribute labels from anime characters. The exact steps are as follows:

Step 1: Using the mapping Key, get the primary attribute mapping M and location index I = l1, l2, l3,..., lt.

Step 2: Extract the L = l1, l2, l3... it attribute label combination.

Step 3: Using the LSTM model, Converting the anime character attribute label series into the secret data series S = s1, s2, s3,..., st.

Step 4: At last we got binary bits series from step 3 and transform binary bits information into secret data.

E: Coverless Image Steganography Based on Jigsaw Puzzle Image Generation [5].

In this work, a novel exciting CIH approach is given, which supports the creation of puzzle images based on a hidden message. The first carrier is divided into rows and columns to produce blocks known as sub images. The shape of a puzzle component will be induced by tabs/blanks in each block, concluding in a properly developed puzzle stego-image in keeping with hidden bits and a suggested mapping function. After then, the completed puzzle image is emailed to the addressee. When compared to existing coverless steganography algorithms, the experimental findings and analyses indicate an honest performance in terms of concealing capacity, security, and resilience.

1. Proposed Method

It has two primary components: embedding, which creates the puzzle image that supports the payload, and extraction, which extracts the crucial message.

The suggested approach is entirely based on the creation of puzzle images and secret message mapping.

1.1 Jigsaw Puzzle

Puzzles are defined as "puzzles composed of little parts and these parts combine together to form an image." See Fig. 15.a. Most puzzle pieces are rectangular or square and Fig. 15.b. shows tabs and blanks. Every bit has a random arrangement of tabs and blanks. The maximum count of tabs and blanks could be equal to 4, as seen in the Fig. 15.b. [22].

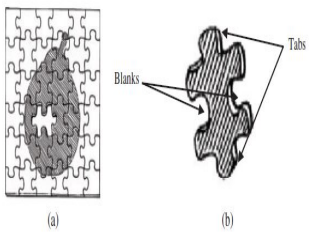

Fig.15: (a) puzzle image.
(b) Structure of Jigsaw puzzle piece [5]

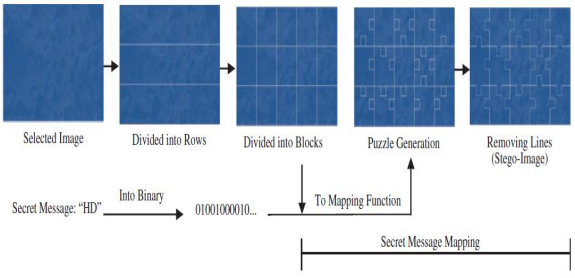

Fig.16 Information hiding framework[5]

1.2 Information Hiding Process

The given image and the secret message are the first two inputs to our method. Then secret message is converted to binary string. Same as specified image will be fragmented into number of parts by adding horizontal lines, as shown in the “Divided into Rows” phase. Next, the picture is divided into equal size blocks and split into columns of comparable width by adding vertical lines, as seen Fig.16. These are the jigsaw pieces that are missing the tabs and blanks described before. Here Key bit is represented by 0 or 1. If the key bit value is 1 and depending on the block location and scanning technique, a tab will be attached to the top, bottom, left, or right side. A blank is inserted to the current block side if the key bit is 0. This procedure will be repeated until all of the hidden bits are indicated by tabs and blanks; for more information, see the "Puzzle Generation" step in Fig.16. After that, the edges seen between blocks and tabs/blanks are erased, leaving a puzzle pattern that may be visualized as a stego image. Finally, the receiver receives this stego picture.

1.3 Retrieval of Secret Information Extraction

In Retrieval of Secret Information, The produced puzzle image is fed into the extraction mechanism via the receiver. To begin, the system monitors each block in the puzzle picture's from left and right sides, row by row. Then, for each block, 1 bit is used to represent a tab and 0 bit is used to represent a blank. Next, to reach the top and bottom sides of each block, the same method will be performed column by column. The key bit stream is then formed by gathering all of the secret bits and concatenating them. Finally, the bit stream is split into 8-bit chunks, translated into characters, and assembled to form the key message.

F: Coverless real time image information hiding based on image block matching and dense convolutional network [7].

In this paper, the high-level semantic characteristics of cover image is extracted by the supervised learning of deep learning Simultaneously, hash sequences of cover image is generated by using the DC coefficient. Matching and splicing the image blocks provides the necessary information. This technique includes three primary steps, as shown in Fig.17:

1) Pre-processing.

The internet is used to search and download a large number of images. Dense Net is used to extract the strong semantic features of every block, and the images are then divided into numerous non-overlapping blocks for feature matching. The inverted index structure is produced by using DCT to create a strong hash code from the DC coefficients between consecutive image units.

3. Sending processing. The index structure matches the picture blocks that are similar, and the key image is split into blocks. For transmission, the most appropriate image block is picked based on Euclidean distance.

4. Receiving processing. Equivalent blocks from the stego-image are obtained using the location information. Because the secret picture has been provided, a similar-sized blank space has been created. Finally, these picture pieces are placed in the empty area to produce a duplicate of the key image.

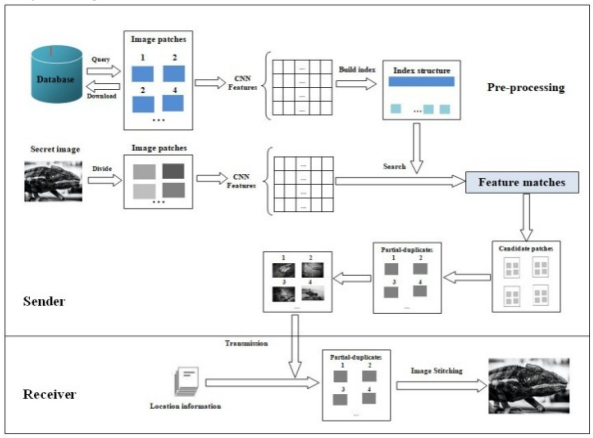

Fig.17 Flowchart of Proposed method [7]

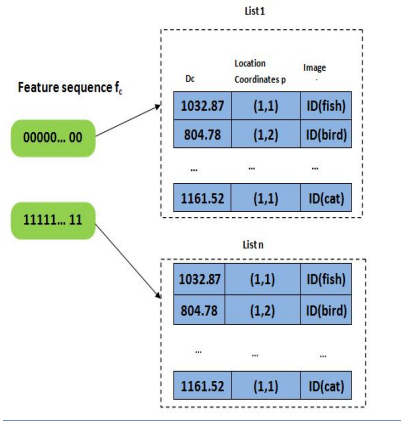

Fig.18 inverted index[10]

G: Coverless Image Steganography Based On Discrete Cosine Transform and Latent Dirichlet Allocation (LDA) Topic Classification [10].

The image database is classified using the LDA topic model. Second, images from a single topic are chosen, and an 8x block DCT transform is applied to them. The strong feature sequence is then generated by the association between coefficients inside nearby blocks. Finally, add the feature sequence, DC, coordinates, and picture link in an inverted index. Converting the key information to binary and segmenting it at the same time, the image also with optimal feature series matching the key information fragment is chosen as the index's cover image. The feature sequence is created at reception using DC coefficients and every feature pattern is concatenated to get the key information as show in Fig.19, which is broken into four sections, shows the exact steps:

1) Image database classification. BOF is a technique for extracting features from all pictures in a database and calculating word frequency. The subject distribution of images is calculated using the LDA topic model. By comparing the image is classed into the subject suggestion with the highest probability, and the procedure is repeated until all images have been classified into the correct manner.

2) Retrieval of Feature sequence. The images are all scaled to the same size and divided into N*N/ l*l blocks. Every block is transformed to YUV colour mode, with each block's Y channel subdivided into 16 sub blocks. Every sub-block receives an 8*8 DCT transformation. The neighboring sub-blocks are used to acquire each small amount of feature sequence

that belongs to each block. To get the feature sets of all sub-blocks for every image, follow the procedures above.

3) The creation of an inverted index.

In inverted indexing, each feature sequence corresponds to a list with three columns as show in Fig. 18. The dc that will be used to decide the order of the received images is computed and saved in the first column. The relevant picture path is stored in the last column. The feature sequence of every block of the images could be determined, and the info of all blocks of the same feature sequence forms a list. For hidden communication, the recipient receives edge information and photos. The sequence of the sub-feature block is calculated down to the tiniest detail. Repeat the steps above to get the feature sequence of each image in order to obtain the necessary information.

4. Hiding and Retrieval of secret information.

First at the sender side, the private data is transformed to M binary pieces. The feature patterns of every sub-block are acquired once the image dataset has been trained. After that, the reverse exponential is generated. For the secret data part, an image with the same feature sequence is produced. Repetition of the preceding method will result in all essential information pictures being erased. The preceding paragraph's number of zeros is tallied and converted into an M-bit binary sequence. Using the previous approach, locate the picture and it should be added to the cover picture. There is no need to save location information if full-size feature sequences are retrieved. The matrix, on the other hand, contains all position coordinates that have been encrypted using the AES encryption method. Using the geometric calibration technique, the image is corrected at the receiver, and the arrangement of the image containing secret information is retrieved using the dc. To acquire the sub-block location coordinates of each picture, decrypt the matrix. To sub-block, an 8*8 DCT transform is used.

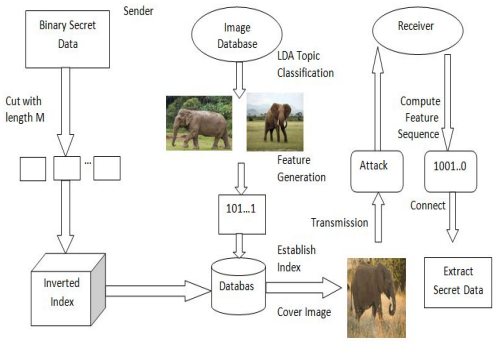

Fig.19 the flow chart of the proposed framework[10]

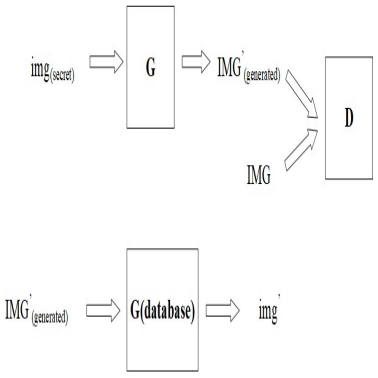

Fig.20 the suggested framework's flow chart[20]

H. Coverless Image Information Hiding Based On Generative Model [20]

This method was the first to use a generative model to enable the way of concealing visual information without a cover. The key image (refer fig. 20) in the generative model database is used to create regular and autonomous pictures with a variety of meanings from the key image. The receiver gets the developed image and enters it into the repository to build a comparable image to the secret image. Both the transmitter and the receiver have the similar data set and, as a result, the similar settings.

1. Training process. WGAN (Wasserstein Generative Adversarial Networks) [7] is an updated version of GAN that ensures more training stability. We'll training the generative model database with the WGAN until it could create a meaningful image that isn't connected to the key image. We give the generative model the key picture, and it generates significance, unrelated IMG which has no relation with the hidden image. If we choose 'Leena' as the secret photo, as illustrated in Fig.21, it may produce an IMG that is aesthetically similar to the 'penguins' we want to send. Meanwhile, we're working with 'penguins' to make the IMG appear to be the same as 'Leena' using the WGAN.' The G1 and G2 models are named "Leena" and "penguins" respectively. To appropriately explore, we capture more image as hidden images, preserve the relevant generative models, and use the same method to put them into practice on the following trial. To create the generative model database, we put the generative models G1, G2, and so on of producing exactly identical to "Leena" "penguins ".

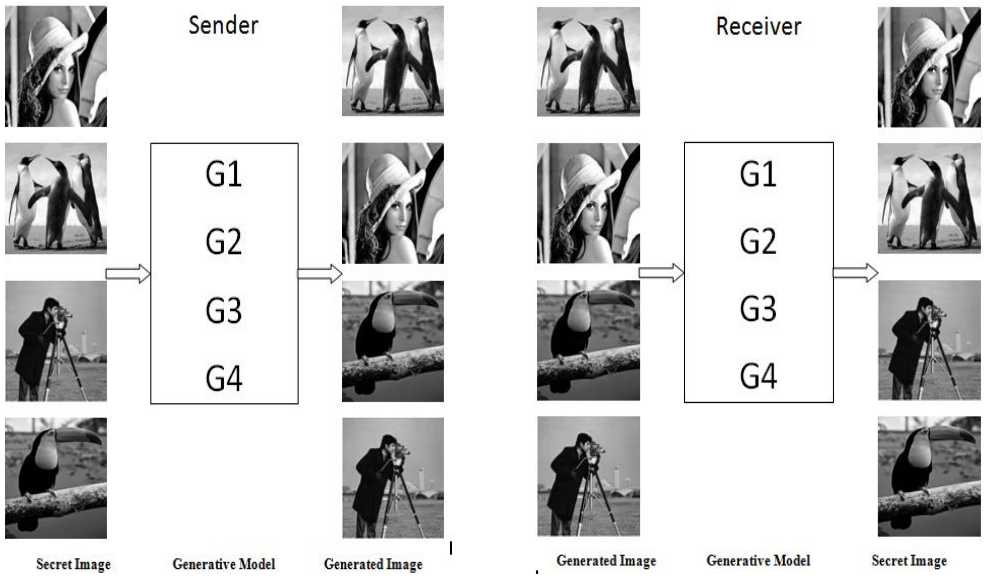

Fig.21. A training process [20].

16

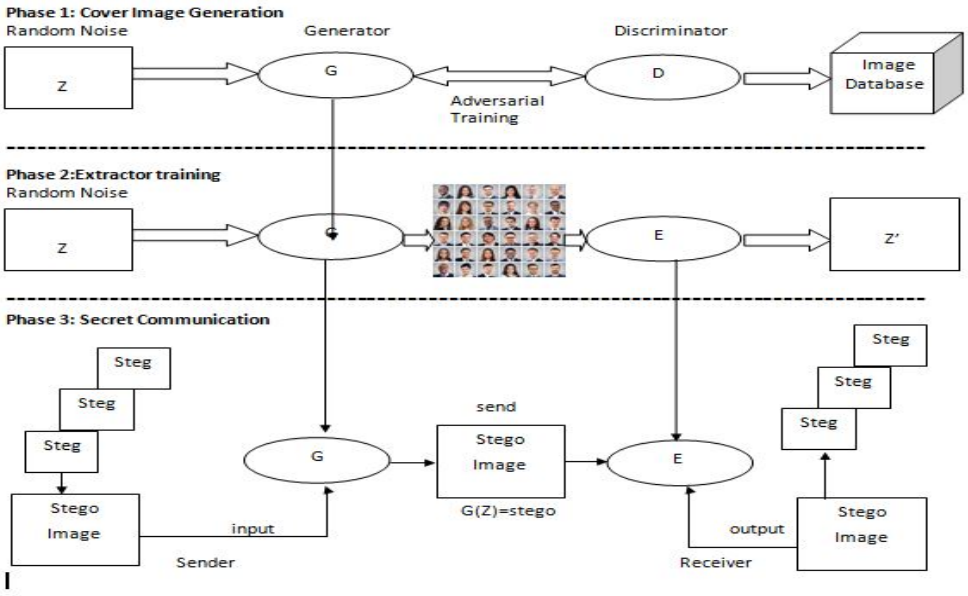

Fig.22 the flow chart of the proposed framework based on DCGANs [12].

2. Information hiding process and extraction process. The transmitter and the recipient share the same dataset and parameters since both the transmitter and receiver have a solid grasp of the generative model database. As illustrated in Fig.21, all we need to do is send the receiver a meaning- a normal picture that isn't connected with the key image, so that the receiver may produce an image that looks exactly like the secret image.

I. Coverless Information Hiding Based On DCGAN [12]

In this method, the generator generates the Stego image, which is backed by pre-processed secret data in DCGANs, as depicted in Fig.22, and it contains no information. DCGANs are used to produce a canopy image that already contains hidden information throughout this approach. At various phases, DCGANs are thoroughly trained, and the guidance is also transformed into a vector of noise [12]. To summaries, the noise vectors from the stego images are extracted using DCGANs. After the mapped noise vectors have been trained into them. The elements of this coverless steganography approach supported by DCGAN are as follows:

1. Development of Stego image. The secret data is split into small parts, each of which is compared to a noise vector of two or three bits. DCGAN is learned on an image dataset generator, and G is acquired once DCGAN has reached its convergence point. The stego images are created by matching the information exchange of the 000 images in the training set to construct a synthetic image using G, which consists of fully connected and 4 convolutional layers. The magnitude of the noise dimension is

related to the depth of the small print inside the generated image.

2. The extractor's training: The extractor E, a CNNs classifier, is trained using the recovered losses from a huge set of random noisy vectors. E has a leak-Relu activation function with batch normalization but no pooling or dropout for each of the 4 convolutional layers. After the final convolutional layer, a fully connected layer is used. The generator creates stego images with 64 * 64 * 3 dimensions in line with these noise vectors as input to the extractor, and the output may be a high - dimensional noise vector.

3. Invisible communication: The network's transmitter and receiver, as well as the G and E parameters after the DCGANs have been trained. Transmitter split the key data into small parts based on the capacity of the steganographic image, then uses G to generate stego images in accordance with noise z. At the last, Receiver receives stego images, reduces noise vectors with E, and then retrieves the relevant data using reverse mapping techniques

IV. PERFORMANCE EVALUATION

First we compared coverless image steganography to regular image steganography in this part, as well as evaluated the performance of current coverless image steganography. The greatest advantage of coverless image steganography is that it can resist the existing steganalysis tools to a great extent. Coverless image steganography is more robust against geometric attack compare to traditional image steganography. The capacity is restricted by the length of the image hash, which is its greatest issue. Longer hash sequences may be constructed to conceal more secret information, but the image database must also be increased.

Second, we analyzed the performance of existing coverless image hiding method based on two attributes. First attributes is embedding capacity which is show in Table 1and second one is Robustness which show in table 2.

Table 1 the embedding capacity of the proposed methods

Methods	Capacity	Robustness
Proposed Method 1[13]	18 bits per carrier	Provide higher Robustness
Proposed Method 2 [1]	2600bits per carrier	Provide Low Robustness
Proposed Method 3[2]	8bits per carrier	Provide Low Robustness
Proposed Method 4 [3]	14 bits per carrier	Provide Low Robustness

18

Proposed Method 5 [5]	760bits per carrier	Provide higher Robustness
Proposed Method 6 [7]	800bits per carrier	Provide higher Robustness
Proposed Method 7 [10]	15bits per carrier	Provide higher Robustness

Table 2: Robustness tests against geometric attack (BER))

Geometric Attack		Method 1[13]	Method 2 [1]	Method 7[10]
	10°	0.7894	0.0937	0.164
Rotational	30°	0.8307	0.1190	0.1116
	50°	0.792	0.1676	0.1288
	0.5	0.7364	0.5892	0
Scaling	0.75	0.5943	0.2354	0
	1.5	0.3928	0.0582	0
	$\sigma(0.001)$	0.8088	0.1548	0.0301
Gaussian noise	$\sigma(0.005)$	0.8165	0.4680	0.0172
	$\sigma(0.1)$	0.8662	0.9638	0.0086
	(3 × 3)	0.6822	0.1813	0
Median filter	(5 × 5)	0.6951	0.3486	0.0086
	(7 × 7)	0.8088	0.4699	0.0172
	(3 × 3)	0.686	0.1743	0
Gaussian filter	(5 × 5)	0.7558	0.3051	0
	(7 × 7)	0.9031	0.4984	0

V. **Current Key Challenges**

Finally, conducting an analysis of existing coverless image steganography and their characteristics, it was found that current approaches had the following drawbacks:

1. Most of propose methods are very sensitive to geometric attack because they capture feature from spatial domain [2, 3, 5, 7].
2. Existing techniques are insecure and insufficiently robust [1, 2, 3].

3. Most of propose methods are also have a limited embedding capacity.
4. To send the secret information, several images are needed [2, 10, 13].
5. It is necessary to have a large image database [15, 16].
6. They scan the database for images that contain hidden message bits, almost like image retrieval.
7. At both the transmitter and the receiver, current techniques produce a hash code for every image or image block in the database, which is wasteful in terms of time and resources [2, 3, 4, 5, 8].

VI. CONCLUSION AND FUTURE WORK

This article explores a comprehensive analysis of coverless image steganography, emphasizing recent advancements, providing an overview of the framework of those techniques, and examining performance for the most representative ways. Despite the significant advancements in coverless image steganography over the previous several years, there is still considerable need for development in future task.

In future work, we will focus on enhance hiding capacity, Extend the image's distinct identifiable details, extend image database and Enhance Robustness. To enhance data hidden capacity, we may split the picture into numerous sub-images or create a longer hash series based on real-world demands. In upcoming progress will require us to enhance our image database in order to enhance the performance of the recovered image and effectively communicate hidden information through natural photographs. At the last also focus on to Enhance Robustness. The system's robustness against rotation and content loss assaults will be improved in future.

REFERENCES

[1] LINA YANG, (Member, IEEE), HAIYU DENG , AND XIAOCUI DANG ," A Novel Coverless Information Hiding Method Based on the Most Significant Bit of the Cover Image ".IEEE, VOLUME 8, 2020 .

[2] Yuanjing Luo1, Jiaohua Qin," Coverless Image Steganography Based on Image Segmentation". *Computers, Materials & Continua* CMC, vol.64, no.2, pp.1281-1295, 2020.

[3] Yi Cao, Zhili Zhou, Q. M. Jonathan Wu, Chengsheng Yuan and Xingming Sun," Coverless information hiding based on the generation of anime characters". EURASIP Journal on Image and Video Processing (2020).

[4] Anqi Qiu, Xianyi Chen,Xingming Sun," Coverless Image Steganography Method Based on Feature Selection ". Tech Science Press JIHPP, vol.1, no.2, pp.49-60, 2019.

[5] Al Hussien Seddik Saad, M. S. Mohamed and E. H. Hafez ," Coverless Image Steganography Based on Jigsaw Puzzle Image Generation ". Tech Science Press 10 December 2020.

[6] ZHILI ZHOU, (Member, IEEE), YI CAO," Faster-RCNN Based Robust Coverless Information Hiding System in Cloud Environment". ".IEEE, December 23, 2019.

[7] Yuanjing Luo · Jiaohua Qin · Xuyu Xiang ," Coverless real-time image information hiding based on image block matching and dense convolution network". Springer, December 2019.

[8] Qiang Liu, Xuyu Xiang ∗, Jiaohua Qin" Coverless steganography based on image retrieval of DenseNet features and DWT sequence mapping" Elsevier December 2019.

[9] M.-M. Liu, M.-Q. Zhang, J. Liu, Y. Zhang, and Y. Ke, ''Coverless information hiding based on generative adversarial networks,'' J. Appl. Sci., vol. 36, pp. 371–382, Mar. 2018.

[10] X. Zhang, F. Peng, and M. Long, ''Robust coverless image steganography based on DCT and LDA topic classification,'' IEEE Trans. Multimedia, vol. 20, no. 12, pp. 3223–3238, Dec. 2018.
[11] Zhou, Z., Sun, H., Harit, R., Chen, X., Sun, X.: Coverless image steganography without embedding. In: Huang, Z., Sun, X., Luo, J., Wang, J. (eds.) ICCCS 2015. LNCS, vol. 9483, pp. 123–132. Springer, Cham (2015).
[12] M Liu, M Zhang, J Liu, Y Zhang," Coverless Information Hiding Based On DCGAN", 2017.
[13] Shuli Zheng1, Liang Wang1, Baohong Ling2, and Donghui Hu1," Coverless Information Hiding Based on Robust Image Hashing Springer , June 2017.
[14] Z.-L. Zhou, Y. Cao, and X.-M. Sun, ''Coverless information hiding based on bag-of-words model of image,'' J. Appl. Sci. Electron. Inf. Eng., vol. 34, no. 5, pp. 527–536, Sep. 2016.
[15] Z. Zhou, Y. Mu, and Q. J. Wu, ''Coverless image steganography using partial-duplicate image retrieval,'' Soft Comput., pp. 1–12, Mar. 2018.
[16] V. Holub, J. Fridrich, and T. Denemark, ''Universal distortion function for steganography in an arbitrary domain,'' EURASIP J. Inf. Secur., vol. 2014, no. 1, pp. 1–13, Dec. 2014.
[17] M. Y. Valandar, M. J. Barani, P. Ayubi, and M. Aghazadeh, ''An integer wavelet transform image steganography method based on 3D sine chaotic map,'' Multimedia Tools Appl., vol. 78, no. 8, pp. 9971–9989, Apr. 2019.
[18] W. Liang, J. Long, A. Cui, and L. Peng, ''A new robust dual intel- lectual property watermarking algorithm based on field programmable gate array,'' J. Comput. Theor. Nanosci., vol. 12, no. 10, pp. 3959–3962, Oct. 2015.
[19] J. A. Hartigan and M. A. Wong, ''A K-means clustering algorithm,'' Appl. Statist., pp. 100–108, Jun. 2013.
[20] Xintao Duan1, *, Haoxian Song1, Chuan Qin2 and Muhammad Khurram Khan3 "Coverless Image Information Hiding Based On Generative Model",Tech Science Press 2018.
[21] Image steganography with LSB, Lokesh Gagnani,International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume –II Issuse –I 2013 pp-228-229
[22] Image Steganography , Lokesh Gagnani,International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume –II Issuse –I 2013 pp-224-227