Academic Journal of Nawroz University (AJNU), Vol.11, No.3, 2022

https://doi.org/10.25007/ajnu.v11n3a1460

Coverless Image Steganography: Review

Shler Farhad Khorshid[1], Wafaa Mustafa Abduallah[2,3]

[1]Department of Information Technology, Duhok Polytechnic University, Duhok, Iraq
[2]Department of Information Technology Management, Duhok Polytechnic University, Duhok, Iraq
[3]Department of Computer Science, Nawroz University, Duhok, Iraq

ABSTRACT

Due to the digitization of information and the attack on different types of multimedia data, information security has become a key concern. For years, image steganography has been considered one of the best ways to protect sensitive information. In image steganography, a secret message is hidden within a cover image by modifying some pixels, forming a stego-image as a result. In turn, this modification makes it possible for steganalysis algorithms to detect the hidden secret message. To address this issue, the concept of coverless image steganography has emerged. With this approach, instead of modifying the content of the cover images, a mapping relationship is established. This mapping relationship maps the secret message to those cover images that contain its content, without modifying the covers themselves. This paper reviews some of the recent works that have been conducted on the topic of coverless image steganography and provide an important insight into how these techniques are performed.

KEYWORDS: Image steganography, coverless, Stego-image, Security.

1. Introduction

As long as people want to ensure confidentiality of information from recipients who aren't intended, information needs to be protected during transmission. For thousands of years, two techniques have been developed to achieve this goal: first one is an encrypted message is converted into an unreadable data stream, known as ciphertext, by a technique called cryptography (Bruce, 1996), (Bokhari & Shallal, 2016), (Saranya, Mohanapriya, Udhayan, & Research, 2014). The other technique is steganography, in which a secret message is hidden inside another information-rich medium (Stefan & Fabien AP, 2000), (Kour, Verma, & Technology, 2014). Where cryptography ensures the message's security by making the ciphertext difficult to decrypt (Pramanik, Singh, Ghosh, & Science, 2019). On the other hand, the secret message is protected by steganography, which renders the stego image created to appear innocent, i.e., as ordinary as those not carrying any secret message (Maitra, 2011), (Ge, Huang, & Wang, 2011). Secret information is frequently embedded in digital media for secret communication (Shen, Zhang, Feng, Cao, & Huang, 2007), (Lou & Sung, 2004). Information hiding techniques such as steganography and watermarking (Tan et al., 2019) usually select digital images, text, video, audio, etc. to hide (Fridrich, 2009), (Sharda, Budhiraja, & Engineering, 2013) as the carriers (Johnson & Jajodia, 1998). Almost all traditional steganographic techniques embed the payload into the cover image pixels, resulting in a modification of the image (Saha & Sharma, 2012), (Provos, Honeyman, & privacy, 2003), (Verma, 2011). Because any image steganalysis tool can identify the stego-images used in these strategies, security cannot be assured (Petitcolas, Anderson, & Kuhn, 1999), (Chutani, Goyal, & Applications, 2019). A coverless data hiding idea has been presented as a solution to this issue (Tan et al., 2019), which was first proposed in May 2014 (Zhou, Sun, Harit, Chen, & Sun, 2015). Based on an analysis of the carrier's attributes and mapping of those attributes to secret information, the secret information is obscured by coverless image steganography. Therefore, the carrier can expose it directly (Qin, Luo, Xiang, Tan, & Huang, 2019).

The topic of coverless image steganography has grown increasingly popular in recent years. However, there has not been much review research on this topic. By providing such a review, it would be beneficial for those researchers planning to pursue this field to know what advances have been made so far. Accordingly, the purpose of this paper is to summarize some basic frameworks of coverless image steganography and to assess their advantages and disadvantages.

The remainder of the paper is arranged out as follows: general image steganography, coverless image steganography with basic steps and challenges are described in Section two. Related works are presented in Section three. Section four contains a discussion. Recommendations are included in section five. Finally, conclusions are drawn in Section six.

2. BACKGROUND

This section provides an overview of coverless image steganography, steps and key challenges.

2.1 General image steganography

Steganography is a method of hiding private or secret data in images that is undetected. The secret information format might be bits, text or images. The data that is hidden within a carrier image is called a “payload” or 'hidden message', and the resulting image is called a stego-image. An unsecured channel is then used to transmit the stego-image (Kadhim, Premaratne, Vial, & Halloran, 2019) during the embedding process, to increase security, security systems often use an encryption method and optional key. The latter can contain information such as the password, embedding coefficients used to encrypt and so on. Both the sender and the recipient must share it (OMRAN, MAHMOUD, ALI, & Education, 2022).Image steganography terms are (OMRAN et al., 2022):

- **Secret message**: It is the message that must be incorporated into the cover file. Payloads can be images, ciphertext, plaintext or anything else that can be represented as a bit stream.
- **Cover file**: It is the original file that contains the required secret message.
- **Stego-image:** The result of hiding the payload in the carrier image.
- **Stego key**: An optional password that can be used to encrypt the secret information, adding an additional layer of security.

Steganography System Encoder and Decoder steganography is made up of two algorithms as shown in Fig. 1. (OMRAN et al., 2022). An embedded message is concealed within a cover file. Meanwhile, the extraction process, which reverses the embedding process by exposing the hidden message at the end, is typically much simpler.

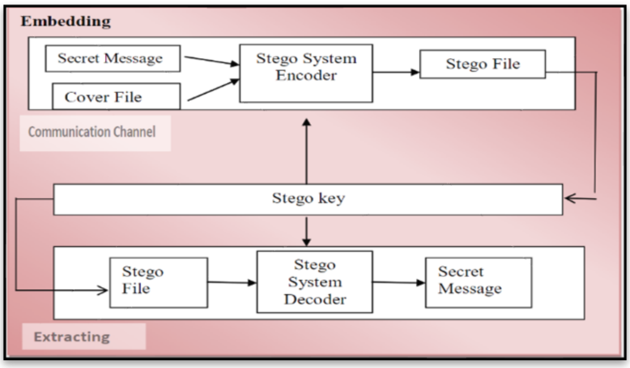

Fig. 1. General model of Steganography (OMRAN et al., 2022).

2.2 Coverless Image Steganography (CIS)

Image steganography has received a lot of attention in the field of information security, but the CIS framework outperforms previous steganography methods in terms of robustness to popular attacks including brightness alteration, rescaling, JPEG compression, and contrast enhancement (OMRAN et al., 2022). Because of the fact that it can't be read and is invisible.

The CIS has a lot of potential for development (Wang, Zhang, & Zhang, 2009). Traditional steganography embeds secret information in the carrier, so "coverless" refers to a way of communicating secret information without having to alter the carrier. The process of hiding actually consists of creating a mapping relationship between another image or text and the secret data (Q. Liu, X. Xiang, J. Qin, Y. Tan, Y. J. E. J. o. I. Qiu, et al., 2020). Additionally, coverless techniques for hiding information have recently emerged. Steganalysis tools cannot detect the secret information with these techniques since they do not alter the carrier image, greatly improving the security of information hiding (Chen, Sun, Tobe, Zhou, & Sun, 2015). In summary, the following the characteristics of CIS are:

- Without changing the stego-image, covert communication can be achieved.
- Stegoanalysis tools cannot identify secret information because the stego-image has not been altered.

2.3 Steps of coverless image steganography

The purpose of this section is to go over some steps of coverless image steganography (Qin et al., 2019).

2.3.1 Pre-processing

Pre-processing is necessary to transmit secret information more quickly and accurately. As CIS approaches have evolved in recent years, they have frequently built their own image set of data by processing many images in the same manner and segmenting secret information in advance (Qin et al., 2019). For example, in (Zhou, Mu, & Wu, 2019), (Luo et al., 2020) pre-processing is utilized. As a consequence, many of natural images were collected, standardized and split into the same proportions as shown in Fig. 2. to produce sequence codes. Finally, rather than using the raw data set, the index is used to match them with the necessary images (Zhou et al., 2019), (Luo et al., 2020), (Duan & Song, 2018). Due to the importance of pre-processing, it is essential step (Qin et al., 2019).

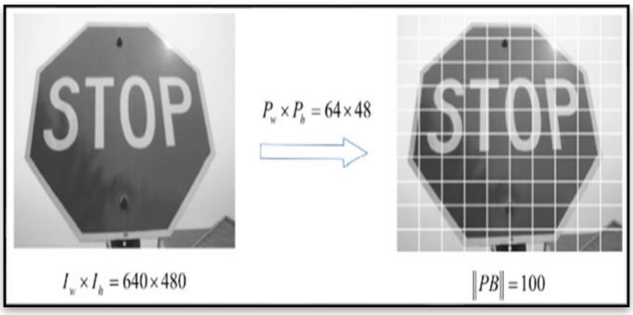
STOP
$P_w \times P_h = 64\times48$
STOP
$I_w \times I_h = 640\times480$
$\|PB\| = 100$

Fig. 2. The way the image is divided (Zhou et al., 2019).

2.3.2 Feature extraction

The image is divided into 16 small blocks, as shown in Fig. 3., so that each block has its own features that are recorded as $\{fk^1, fk^2, \dots , fk^{16}\}h$. As a final characteristic of the image, it is recorded as FK= $\{fk^1, fk^2, ..., fk^{16}\}$ (Zhou et al., 2019). The gray histogram captures the gray-level information in images. In (Zhou et al., 2015), the average gray value is used. The image edges and the places where the brightness dramatically changes with SIFT features are noticeably more stable than with other features (Lowe, 2004). In (Q. Liu, X. Xiang, J. Qin, Y. Tan, Y. J. E. J. o. I. Qiu, et al., 2020), (Luo et al., 2020) and (Q. Liu, X. Xiang, J. Qin, Y. Tan, J. Tan, et al., 2020) feature extraction is done with Deep Learning's DenseNet network model.

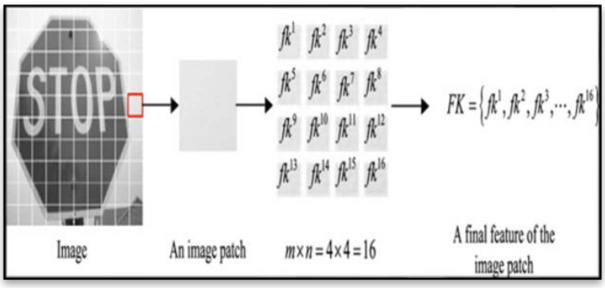
STOP
fk^1 fk^2 fk^3 fk^4
fk^5 fk^6 fk^7 fk^8
fk^9 fk^{10} fk^{11} fk^{12}
fk^{13} fk^{14} fk^{15} fk^{16}
$FK = \{fk^1, fk^2, fk^3, \cdots, fk^{16}\}$
Image
An image patch
$m\times n = 4\times4 = 16$
A final feature of the image patch

Fig. 3. Extracting the final feature from an image patch (Zhou et al., 2019).

2.3.3 Generation of hash sequence

A simple hash algorithm was introduced by (Zhou et al., 2015) as shown in Fig 4. First, the authors transformed a given image to a gray-level image, then divided it into 3x3 blocks denoted by {b11, b12,…, bij ,b33}. The average intensity of each block is then computed, yielding 9 intensity values $\{I\ (b_{11}), I\ (b_{12}), \dots, I(b_{ij}), I(b_{33})\}$. Concatenating the values in a zig-zag pattern gives us the vector

$\{I_1, I_2, \ldots, I_9\}$, and every intensity value Ii is matched to its adjacent I_{i+1} by Eq. (1) to produce the hash sequence of the image $\{h_1, h_2, \ldots, h_8\}$.

$$\begin{cases} h_i = 1 & , \text{ if } \quad I_i \geq I_{i+1} \\ h_i = 0, & \quad \textit{otherwise} \end{cases}, \text{ where } i \leq i \leq 8 \qquad (1)$$

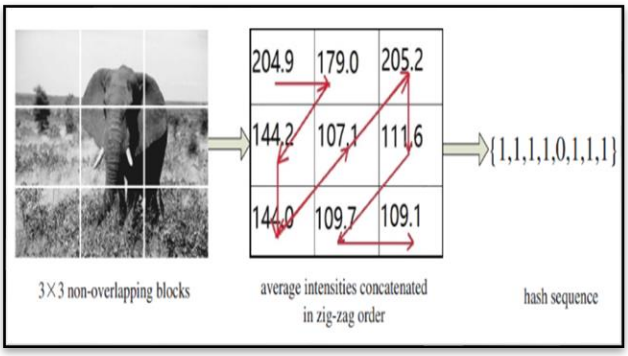
204.9
179.0
205.2
144.2
107.1
111.6
144.0
109.7
109.1
{1,1,1,1,0,1,1,1}
3×3 non-overlapping blocks
average intensities concatenated in zig-zag order
hash sequence

Fig. 4. The robust hashing algorithm's method to create hash sequences (Zhou et al., 2015).

In addition, another algorithm generates the hash sequence, as shown in fig. 4. (Q. Liu, X. Xiang, J. Qin, Y. Tan, Y. J. E. J. o. I. Qiu, et al., 2020). To begin, they features extracted from a data set using a pre-trained DenseNet network.

$$F_{ic} = DenseNet(pi_{ic}) \qquad (2)$$

The blocks B_{ib} are then obtained by partitioning F_{ic} into D blocks

$$B_{ib} = \{B_1, B_2, \ldots, B_D\}, 0 < ib \leq D < w \qquad (3)$$

Feature coefficient Me_{ib} is calculated for each block

$$\mathrm{B_{ib}} Me_{ib} = \begin{cases} \frac{D}{W} \sum_{w(ib-1)/D}^{w.ib/D} f_{iw,} \ \ if\ 0<ib\leq D-1 \\ \frac{D}{W} \sum_{w(ib-1)/D}^{w} f_{iw,if}\ ib = D \end{cases}, 0 < iw < w$$

(4)

In essence, Me_{ib} is the average of each feature block Bib. They use the "arithmetic scan" technique to scan feature coefficients *Me* after calculating all attribute coefficients; the schematic diagram in Fig. 5.

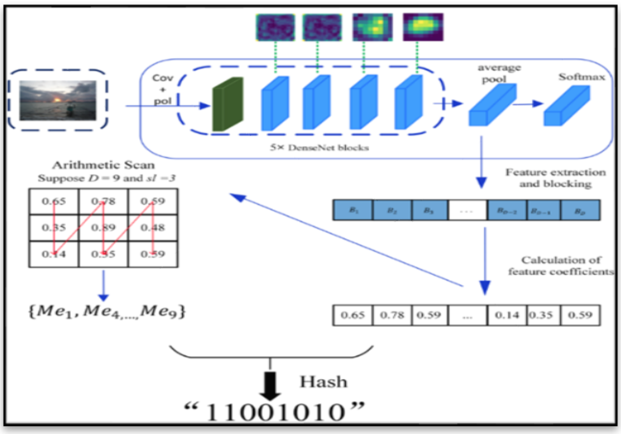

Fig. 5. The process generating hashing sequence (Q. Liu, X. Xiang, J. Qin, Y. Tan, Y. J. E. J. o. I. Qiu, et al., 2020).

Finally, they compare every attribute coefficient Me of an adjacent block to eq. (5) to obtain the hash sequence, so each bit of the hash sequence f_{ic} is

$$f_{ic} = \begin{cases} 1, & if\ Me_{is} > Me_{is+1} \\ 0, & \quad otherwise \end{cases}, 0 < is < D \qquad (5)$$

In communication, different types of attacks could be used to manipulate "stego" images, including luminance changes, rescaling, contrast enhancement, and noise addition. As a result, the hashing must be resistant to the most of of these attacks in order to avoid modification to the image hash sequences during transmission. As a result, the secret information can be communicated accurate with minimal losses and variation (Zhou et al., 2015).

2.3.4 Mapping relationships

Since coverless steganography uses natural images for its carriers, it has become so popular due to its ability to bypass the process of modifying images. Consequently, it is vital for mapping the relationship between natural images and secret information. For coverless image steganography, hash sequences and secret information are the most common mapping relationships (Qin et al., 2019). For example, in (Zhou et al., 2015), A set of images are chosen from the ImageNet dataset relying on matching sections of hash sequences with secret information. Because of the mapping between feature sequences and secret information segments, the image can be represented as a feature sequence. They established an inverted index with entries for all possible eight - bit hash sequences to allow faster the matching of images with secret information (Zhou et al., 2015), every entry, which is shown in Fig. 6., indicates to a list that includes the IDs of images with same hash sequence as entry.

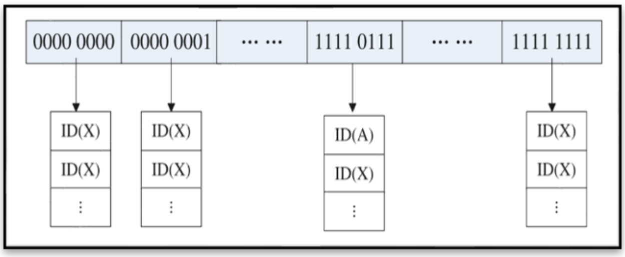

Fig. 6. Structure of inverted indexes (Zhou et al., 2015).

By utilizing the inverted index structure, to find a set of images that already contain the information. The secret message is initially split into multiple segments. Following that, each segment can be utilized as a query to recover images with the similar hash sequence. Finally, inverted indexes are used to locate the images. Stego images can be considered since they already include the secret data (Zhou et al., 2015).

2.4 Key challenges

CIS heads three challenges, as shown in the following subtitle (Qin et al., 2019):

2.4.1 High capacity

Despite the fact that the image already contains a lot of data, like pixel brightness values, colors, textures, edges, contours, and high-level semantics. By definition, coverless steganography has a limited capacity due to the length of the sequences used to map relationships between nature images and secret information. Due to this, coverless steganography's capacity is much smaller than traditional image steganography's (Qin et al., 2019). A common way to measure capacity is bits for each pixel, or the average number of bits hidden in every pixel of the cover image (Subramanian, Elharrouss, Al-Maadeed, & Bouridane, 2021). The Hiding capacity should be as large as possible (Lin, Lin, Wang, & Interfaces, 2009).

2.4.2 High accuracy

In order for the entire image steganography process to work efficiently and effectively, it must be able to transmit complete and accurate information. Through natural images, CIS can transmit data that is hidden in secret images. To send messages precisely, many of natural images from a range of sources are usually required. Due to deviations in natural image choice or incorrect creation of inverted index frame, information is relayed incorrectly or incompletely. The accuracy of the image will also be affected if the image is compromised during transmission (Qin et al., 2019).

2.4.3 Security

Steganography's security is based on two factors: its resistance to steganography tools and its protection against attackers. As everybody knows, the most of tools of steganography work on alteration traces, and the optimum image steganography technique is highly resistant to all kinds of steganography tools (Hussain, Wahab, Idris, Ho, & Jung, 2018). The second factor is that if these mapping and image data sets are found by attackers, they will be able to quickly obtain the information We want to protect the information secret, and even if it is incorrect, it will be easily removed as a result, defending against attackers is critical (Swanson, Kobayashi, & Tewfik, 1998), (Kadhim et al., 2019).

3. LITERATURE REVIEW

Methods of CIS can be divided into two groups; CIS methods without using machine learning and CIS methods on the basis of machine learning.

3.1 CIS methods without using Machine Learning

The image mapping-based CIS technique follows the same transfer flow, the secret information is first encoded into a hash sequence, and then the optimal image is chosen that has the same hash sequence. In 2015, Zhou et al. (Zhou et al., 2015) were the first who used steganography without embedding structure, based on image database with images indexed according to their hash sequence generated by a robust hashing algorithm. The binary secret data is then split into many parts. The database will be used to get an image of every segment with a hash value matching the segment value. For every original image only eight bits of data can be hidden as shown in Fig. 7. In order to increase the capacity that is hidden, Zheng et al. (Zheng, Wang, Ling, & Hu, 2017) improved the hash algorithm that has been proposed by (Zhou et al., 2015) as well as lengthening of the secret information. For fast retrieval, the hash values of 5000 images are computed and stored in a quadtree index structure. The secret information is split into 18-bit segments to match the quadtree. Based on the leaf node's information, the corresponding image is chosen as a carrier of the current 18-bit secret data. As a result, the secret information images are actually a series of images. The receiver accepted these images in turn and uses the shared hash algorithm to extract secret information from them. In July of 2018, Zou et al. (Zou et al., 2019) presented a new CIS technique relying on the average pixel values of sub images, which generated hash sequences as a cover for secret information. At the same year, to transmit the hidden image, Zhou et al. (Zhou et al., 2019), a group of similar blocks of a given secret image were used. After splitting each database image into a number of patches and indexing those images depending on the attributes extracted from these patches, they search for partial duplicates of the secret data to generate the stego images, each of which reveals one or more similarity patches with the secret image. They can nearly restore the image from these partial duplicates at the receiver end. The secret information, on the other hand, cannot be fully extracted. And the image's visual quality is extremely bad. In January of 2019, Chen et al. (Chen et al., 2019) proposed a high-capacity CIS technology. They have divided the cover image into several image blocks, and every image block represents one bit of secret information, thereby greatly improving capacity. To send the secret information, the sender compares the secret information sequence one by one with the hashes of the original image. If the value of the relevant position is the same, a block of images remains unchanged. They must use the secret information sequence to retrieve the image block from the database and flip the hash value in order to produce the original block of image. Depending on the secret information, the blocks of image are retrieved from the image block database and synthesized into Stego images. They've also built a two-level index structure to enhance retrieval performance. Furthermore, the approach is resistant to steganography. This article, however, only covers one type of feature. Yang et al. (Yang, Deng, & Dang, 2020), presented CIS technique based on the Most Significant Bit (MSB) of cover image (CIHMSB). The cover image is initially segmented into several fragments. Secret information is first preprocessed, then converted to binary form. A mapping (denoted as Km) between the MSB of the image fragment and the secret information is established then, according to the mapping sequence determined by the sender and receiver in advance. As a result, a mapping flag (denoted as Kf) is produced, which is sent along with the stego image. Experiments indicate that this method hides more information than (Zhou et al., 2019). A CIS scheme based on DCT transform is proposed by Zhang et al. (Zhang, Peng, & Long, 2018). To begin with, the image database is classified using Latent Dirichlet Allocation (LDA) topic models. Secondly, images from a single topic are selected and subjected to an 8x8 block DCT transform. The relationship among both Direct Current coefficients in adjacent blocks is then utilized to create a robust feature sequence. Finally, an inverted index is used to store the dc, location coordinates, feature sequence, and image path. The receiver calculates the feature sequence using DC coefficients, and all feature sequences are combined to obtain the secret information. This algorithm proved resistant to the majority of image processing and geometric attacks. Govindasamy et al. proposed CIS using Haar Integer Wavelet Transform. They split a 256x256 image into

1024 submatrices. Thereafter, the coefficients in each submatrix are generated using integer wavelet transforms. The arrays are then generated from the submatrices. The coefficients of each sub-matrix are then transformed to binary bits by determining whether the next value in the array is larger or smaller than the current one, yielding a 1064*63 array. In the process, a location map is generated, which can be used by the receiver to find the secret message (Govindasamy, Sharma, & Thanikaiselvan, 2020).

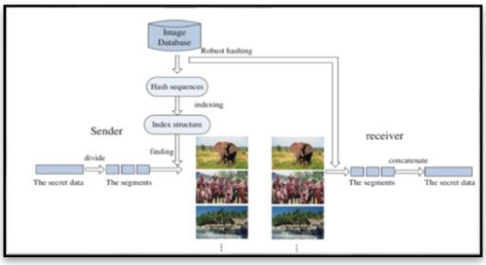

Fig. 7. The proposed CIS framework (Zhou et al., 2015)

3.2 CIS methods based on Machine Learning

One of the Machine Learning research fields is Deep Learning (Luo et al., 2020). A hierarchical artificial neural network can perform both supervised and unsupervised learning end to end. The authors utilized DenseNet to retrieve each block's repeated high-level semantic features. Convolution, pooling, and other operations produce high-level semantic features, that are extracted by a convolutional neural network (CNN). Using Generative Adversarial Networks, the CIS method machine learning based generates a stego image based on the secret information. In 2018, Duan and Song proposed a generative model. This is the first time a generative model-based information hiding technique that can successfully resist steganalysis tools has been proposed (Duan & Song, 2018). They continue to train the generative model database using Wasserstein Generative Adversarial Networks until it is able to create a meaning-normal and independent image that is unrelated to the secret image. They only need to transfer a meaning-normal and independent image to the receiver, and the receiver simply needs to feed the transmitted image into the generative model database, that will generate an image that exactly like the secret one. However, this model is not universal and every secret image needs to create a new model. Due to the lack of correlation between the secret image and cover image in Duan et al. 's method, reconstructed secret images don't have enough detail information. Li et al.'s proposed content-consistency coverless information hiding method based on generative models (Li, Wang, Wang, & Shi, 2021) to solve the existing problems. Through the integration of deep learning in coverless information hiding, they propose to achieve this, VGG16 Nets can be trained to extract the content information of a secret image and encode it into the generated image in order to solve the issue of poor reconstruction of secret information. Because of the consistent feature maps obtained from the layers in VGG16 during training, the stage of secret image reconstruction can be naturally performed without incurring any additional costs of transmitting the secret image. Two generative models are used to transmit and reconstruct the secret image, and no extra cover image is needed. In 2020, Liu et al. (X. Liu et al., 2020) proposed Camouflage Generative Adversarial Network (Cam-GAN), For hiding full images in one image, a two-stage coverless method is employed. A full-size secret image can be concealed inside a cover image using this technique, having complete hiding. A cycle made in accordance GAN synthesizes container images to assure full-image hidden capacity. But, it has a limited capacity compared to traditional steganography. Another framework that has been suggested is as follows, Al Hussien et al. (Al Hussien, Mohamed, & Hafez, 2021) suggested method uses optical mark recognition (OMR) and rules-based machine learning (RBML). OMR, with its ability to identify specific markings on bubble sheets, is an electronic way of collecting human-marked data. Labeled bubbles/circles reflect less light than empty bubbles/circles due to their lower reflectivity; this is usually done by using a scanner that scans the sheet's light reflection. RBML algorithms use relational rules to describe data. As opposed to the machine learning (ML) systems, which develop a technique that can be applied to all incoming data. In this study, they developed a novel and highly robust CIS method that is based on OMR and RBML and uses a bubble sheet as a cover to improve security in CIS. In the current rapid development of deep learning, steganography deep learning-based has been presented by of Zhou et al. (Zhou et al., 2019), in September of 2019, Luo et al. presented a novel method for hiding image information in real time using dense convolutional network (DCN) (Luo et al., 2020). This method has improved accuracy and robustness, demonstrating that CNNs can be effectively used for coverless steganography. Which cut and matched image blocks on the network using real-time search. Then, using DenseNet, extract each block's repeated high-level semantic features. This is usually done with a scanner that examines light reflection through the sheet; bubbles/ci are usually marked. In an inverted index structure, they used the discrete cosine transform (DCT) to create a hash sequence based on DC coefficients between image blocks that are adjacent. Blank circles reflect less light than empty ones due to their lower reflectivity. By comparing and splicing image blocks, a secret message is sent. At 800 bits per pixel, Luo's technique has the largest capacity of all coverless steganographies, which is a really small volume when compared with traditional steganography. Based on the references (Luo et al., 2020), Liu et al. (Q. Liu, X. Xiang, J. Qin, Y. Tan, J. Tan, et al., 2020) used DWT to create a robust hash sequence based on DenseNet feature selected images, to enhancing robustness and security. The main idea behind the approach is to use the DWT coefficient to create a mapping relationship between the carrier images and the secret information in order to convert hidden textual data into carrier image selection and retrieval. Firstly, the image datasets features are extracted using the DenseNet CNN model in deep learning. supervised learning is being used to retrieve the image, and the retrieval results is being used as a carrier of information. Second, the chosen images are broken down into sub for block DWT. After block transformation, the DWT coefficient is computed based on the low-frequency components, and the coefficients between blocks are scanned using the Zigzag scan, resulting in robust feature sequences. Finally, the secret data is divided into segments the same length as the feature sequence, and an inverted index is created using the feature sequence, block position, DWT coefficient, and image path. The carriers are chosen by index from images with the same feature sequence as the secret information segment. But remains weak against the geometric attacks. Simultaneously, the spread of deep learning generates new ideas. Liu et al. (Q. Liu, X. Xiang, J. Qin, Y. Tan, Y. J. E. J. o. I. Qiu, et al., 2020) suggested a new hash mapping rule based on the CNN feature, which makes the system more resistant to geometric attacks. The method is divided into three parts, each of which is implemented in 4 steps: hash sequence generation, binary tree hash index construction, CIS, and secret information extraction. In their technique, the pretrained DenseNet model is first used to select features of the image database. Each image's feature is segmented into D blocks, with the feature coefficient Me calculated for every block. The hash sequence is then created by scanning the feature coefficients Me with an arithmetic scan. The secret information is then segmented that are the same length as the hash sequence, and the search cover images are discovered by comparing them to the hash sequence. Lastly, all cover images have been sent to the receiver in order, so the receiver could retrieve secret information by computing received images that use the similar hash algorithm as shown as in Fig. 8. This method outperforms other methods only when color histogram equalization and gamma correction are applied, it doesn't have an absolute advantage against non-geometric attacks, implying that it doesn't have one.

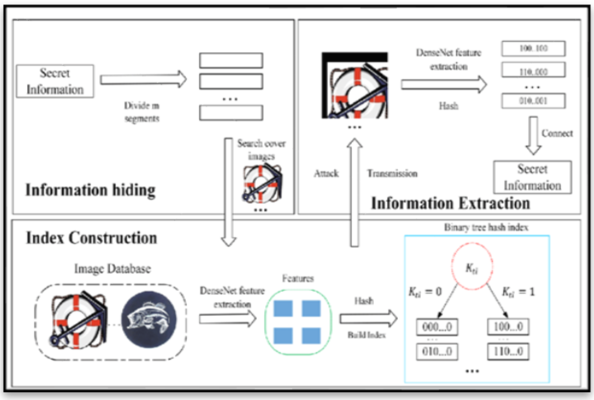

Fig. 8. The proposed CIS (Q. Liu, X. Xiang, J. Qin, Y. Tan, Y. J. E. J. o. I. Qiu, et al., 2020).

Additionally, Qiu et al. (Qiu et al., 2019) proposed a CIS method that uses three kinds of features, namely Local Binary Pattern (LBP), variance value of pixels, and mean value of pixels. Thus, they realize that secret information is being transmitted. According to the description of the feature, first they obtain the hash sequence of the cover image, then they match the sequence of the secret information with the hash sequence of the original cover image. In case the values do not match, the image blocks in the original cover image are replaced in accordance with the secret information. Because stego images derived from natural images are the most similar to actual images, the visual quality of stego images can be improved by utilizing appropriate features. When they choose the image block to be replaced, they must compare every picture block in the index to the cover image block to locate the most comparable image block, which will take a long time. In (Pan et al., 2020) used natural video as carrier, conducted semantic segmentation on it, and created a statistical histogram of semantic segmentation. A histogram is used to map the hash sequence to the hidden bit sequence. By computing the semantic information, the receiver can recover secret information from carrier videos. The carrier videos were not changed at any point during the private information delivery process. As a result, the technique can successfully resist steganalysis, making it difficult to identify by attackers, while video as a communication carrier has the benefit of having a high capacity. A summary of some previous literature reviews is represented in Table 1

4. DISCUSSION

From table 1, the robustness of the CIS without embedding algorithm can be observed (Zhou et al., 2015). However, each original image can only hide 8-bit data. The capacity in CIS using partial-duplicate image retrieval algorithm (Zhou et al., 2019) is better than CIS based on robust image hashing (Zheng et al., 2017), CIS based on the average pixel value of sub-images (Zou et al., 2019) and CIS based on DCT and LDA Topic Classification (Zhang et al., 2018). However, in (Zhou et al., 2019) the visual quality of the recovered secret image is not the best. In (Chen et al., 2019) the authors enhanced the visual quality of secret message but in this work only one sort of features are utilized to describe the cover image and the similarity between cover image block and replacement image block to obtain stego images. On the other hand, CIS based on machine learning, have the highest security (Al Hussien et al., 2021) because it used bubble sheets. While, in (Duan & Song, 2018) the absolute capacity of CIS is more than 37,5 bits per pixel. This method embeds information directly into the generated image based on generational adversarial networks. Image texture complexity is guaranteed, but not image quality and integrity. Additionally, Deep learning networks are often trained in advance by using steganography methods based on CNN to ensure accuracy. Also, the robustness in (Q. Liu, X. Xiang, J. Qin, Y. Tan, J. Tan, et al., 2020) is strong against most image attacks because, the DWT coefficients generated from the sequences of the features which eventually

Table1. The main coverless image steganography

Ref.	Method Name	Key points	Advantages	Disadvantages	Capacity (bits per carrier)
(Zhou et al., 2015)	CIS without embedding	A robust hashing algorithm can generate hash sequences that can represent 8 bits of information, and all hash sequences are built with an inverted index structure.	Have a desirable level of resistance to common attacks like rescaling, luminance change, and noise addition	capacity is limited	8 bits
(Zheng et al., 2017)	Coverless information hiding based on robust image hashing	Using this technique, 18-bit binary values are extracted from every image as a hash value. In this method, the hash value is stored as a quadtree.	Enhanced the hash of algorithm (Zhou et al., 2015) and increased the length of the secret information.	volume of the image database	18 bits
(Zou et al., 2019)	Coverless information hiding technique based on the average pixel value of the sub-images	Using a dictionary, every segment of the secret information can be determined using its position in a Chinese sentence. In order to transfer information, each part of the hash array is labeled.	The capacity is greater than (Zheng et al., 2017)	-	80bits
(Zhang et al., 2018)	CIS depend on DCT and LDA Topic Classification	The image database is classified using the LDA topic model. These images are then subjected to a DCT transformation. After that, a robust feature sequence is created, and an inverted index is created to enhance image search efficiency.	It is resistant to geometric attacks to some extent. It has great potential application in secure communication of big data environment.	It has a limited capacity compared to traditional steganography.	1-15 bits
(Duan & Song, 2018)	Coverless information hiding based on Generative Model	The secret image is loaded into a Generative Adversarial Networks to create meaningful and normal image, then the secret image is extracted from the generated image at the receiving end.	Has high capacity, safety and reliability.	When a large amount of secret information needs to be transmitted, multiple generate models must be trained.	37.5
(Zhou et al., 2019)	CIS using partial-duplicate image retrieval	Steganography employs a number of appropriate partial duplicates of a given secret image from a natural image database as stego-images.	This method not only has a high level of steganalysis resistance, but it also has a high level of security and concealment.	Visual quality of the image is bad	384 bits

(Chen et al., 2019)	CIS based on double-level index and block matching	To build an image block database, they collect a large number of images and divide them into blocks. Then they created a double-level index to speed up retrieval.	Has better visual quality than (Zhou et al., 2019)	Only one type of feature used to describe he cover image	10000 bits
(Luo et al., 2020)	Coverless real-time image information hiding based on image block matching and dense convolutional network	This method sends a set of stego-images to the given secret image that share one or more virtually similar blocks.	-High accuracy - Strong security protection, and robustness.	It has a limited capacity compared to traditional steganography.	800 bits
(Q. Liu, X. Xiang, J. Qin, Y. Tan, J. Tan, et al., 2020)	CIS based on image retrieval of DenseNet features and DWT sequence mapping	The feature sequences are created using the corresponding wavelet function and DWT coefficient between the blocks of the Zigzag scan.	This process enhances the ability to detect subjective visual resistance.	Weak against the geometric attacks	1-15 bits
(Q. Liu, X. Xiang, J. Qin, Y. Tan, Y. J. E. J. o. I. Qiu, et al., 2020)	CIS based on DenseNet feature mapping	The features of cover images are captured through deep learning and then mapped into hash sequences. In order to increase index searching speed, a binary tree hash index is construct for the sender.	When compared to state-of-the-art techniques, it is more resistant to geometric attacks.	weak against non-geometric attacks.	8 bits
(Govindasamy et al., 2020)	CIS using Haar Integer Wavelet Transform	There is only one coverless image utilized, and it contains enough 8-bit sequences to represent all the secret bits	Using only one coverless image, it is very efficient	It has a limited capacity compared to traditional steganography	8 bits
(Yang et al., 2020)	CIS Based on the Most Significant Bit of the Cover Image	According to the mapping sequence Km, the MSB of the image fragments and the binary form secret information are mapped, producing a mapping flag.	It performs well against low-pass filtering, salt & pepper noise, and JPEG compression attacks	It has a limited capacity compared to traditional steganography	1296 bits
(Al Hussien et al., 2021)	Based on Optical Mark Recognition and Machine Learning	In the mapping phase, the generated bubble sheet and secret message are fed into the rule-based machine learning (RBML) algorithm. detection phase works in the same way such the mapping step, but in reverse order.	-No database is required. - No time wasted in searching. - High capacity. - High robustness. - High security.	-	120 bits

could improve robustness. And, capacity in (Q. Liu, X. Xiang, J. Qin, Y. Tan, Y. J. E. J. o. I. Qiu, et al., 2020) is greater than those of other CIS-based methods, but significantly less than that of traditional steganography. According to these findings, CIS based on convolutional neural networks frequently trains deep learning networks fully in advance to ensure the accuracy and stability of CNN features against geometric attacks, which can enhance steganography's robustness. These methods successfully overcome the shortcomings of the existing methods by obtaining the high-level semantic features of cover images using deep learning.

5. RECOMMENDATIONS

Although coverless image steganography has been successful in recent years; however, there is still some challenges that need to be addressed, as follows:

- The capacity should be increased: We should emphasis on ways to do this while ensuring the accuracy and security of the retrieved images.
- Increase attack resistance: there is no such method that resists all types of attacks.

So, it is recommended the aforementioned points to be taken into consideration in the upcoming research.

6. CONCLUSION

Since it was introduced, coverless image steganography has grown exponentially in popularity. It was developed for its ability to resist Steganalysis tools. The purpose of this review was to familiarize the reader with different coverless image steganography techniques and discuss the advantages and disadvantages of each. The previous sections have demonstrated that deep learning-based coverless image steganography can extract high-level semantic features and keep them even when it is being geometrically attacked. Therefore, even if the hash sequence is vulnerable to geometrical attacks, it can still be recovered. It was observed that coverless image steganography based on machine learning could improve accuracy and robustness. Furthermore, it was observed that the papers reviewed in this study have a very low capacity when compared with traditional steganography. As a result, future research should be focused on improving steganography's capacity while ensuring its accuracy and security of retrieval.

7. REFERENCES

1. Al Hussien, S. S., Mohamed, M. S., & Hafez, E. H. J. I. A. (2021). Coverless Image Steganography Based on Optical Mark Recognition and Machine Learning. *9*, 16522-16531.
2. Bokhari, M. U., & Shallal, Q. M. J. I. J. o. C. A. (2016). A review on symmetric key encryption techniques in cryptography. *147*(10).
3. Bruce, S. (1996). Applied cryptography: protocols, algorithms, and source code in C. In: Wiley.
4. Chen, X., Qiu, A., Sun, X., Wang, S., Wei, G. J. M. B., & Engineering. (2019). A high-capacity coverless image steganography method based on double-level index and block matching. *16*(5), 4708-4722.
5. Chen, X., Sun, H., Tobe, Y., Zhou, Z., & Sun, X. (2015). *Coverless information hiding method based on the Chinese mathematical expression.* Paper presented at the International Conference on Cloud Computing and Security.
6. Chutani, S., Goyal, A. J. M. T., & Applications. (2019). A review of forensic approaches to digital image Steganalysis. *78*(13), 18169-18204.
7. Duan, X., & Song, H. J. a. p. a. (2018). Coverless information hiding based on generative model.
8. Fridrich, J. (2009). *Steganography in digital media: principles, algorithms, and applications*: Cambridge University Press.
9. Ge, H., Huang, M., & Wang, Q. (2011). *Steganography and steganalysis based on digital image.* Paper presented at the 2011 4th International Congress on Image and Signal Processing.
10. Govindasamy, V., Sharma, A., & Thanikaiselvan, V. (2020). *Coverless Image Steganography using Haar Integer Wavelet Transform.* Paper presented at the 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC).
11. Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K.-H. J. S. P. I. C. (2018). Image steganography in spatial domain: A survey. *65*, 46-66.
12. Johnson, N. F., & Jajodia, S. J. C. (1998). Exploring steganography: Seeing the unseen. *31*(2), 26-34.
13. Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. J. N. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *335*, 299-326.
14. Kour, J., Verma, D. J. I. J. o. E. R. i. M., & Technology. (2014). Steganography techniques–A review paper. *3*(5), 132-135.
15. Li, Q., Wang, X., Wang, X., & Shi, Y. J. N. P. L. (2021). CCCIH: Content-consistency Coverless Information

Hiding Method Based on Generative Models. *53*(6), 4037-4046.

16. Lin, I.-C., Lin, Y.-B., Wang, C.-M. J. C. S., & Interfaces. (2009). Hiding data in spatial domain images with distortion tolerance. *31*(2), 458-464.
17. Liu, Q., Xiang, X., Qin, J., Tan, Y., Qiu, Y. J. E. J. o. I., & Processing, V. (2020). Coverless image steganography based on DenseNet feature mapping. *2020*(1), 1-18.
18. Liu, Q., Xiang, X., Qin, J., Tan, Y., Tan, J., & Luo, Y. J. K.-B. S. (2020). Coverless steganography based on image retrieval of DenseNet features and DWT sequence mapping. *192*, 105375.
19. Liu, X., Ma, Z., Guo, X., Hou, J., Schaefer, G., Wang, L., . . . Fang, H. (2020). *Camouflage generative adversarial network: Coverless full-image-to-image hiding.* Paper presented at the 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC).
20. Lou, D.-C., & Sung, C.-H. J. I. T. o. M. (2004). A steganographic scheme for secure communications based on the chaos and Euler theorem. *6*(3), 501-509.
21. Lowe, D. G. J. I. j. o. c. v. (2004). Distinctive image features from scale-invariant keypoints. *60*(2), 91-110.
22. Luo, Y., Qin, J., Xiang, X., Tan, Y., Liu, Q., & Xiang, L. J. J. o. R.-T. I. P. (2020). Coverless real-time image information hiding based on image block matching and dense convolutional network. *17*(1), 125-135.
23. Maitra, I. K. J. J. o. G. R. i. C. S. (2011). Digital steganalysis: Review on recent approaches. *2*(1).
24. OMRAN, N. F., MAHMOUD, N. R., ALI, A. A. J. T. J. o. C., & Education, M. (2022). Securing Messages by Using Coverless Steganography: A Survey. *13*(2), 335-345.
25. Pan, N., Qin, J., Tan, Y., Xiang, X., Hou, G. J. E. J. o. I., & Processing, V. (2020). A video coverless information hiding algorithm based on semantic segmentation. *2020*(1), 1-18.
26. Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. J. P. o. t. I. (1999). Information hiding-a survey. *87*(7), 1062-1078.
27. Pramanik, S., Singh, R., Ghosh, R. J. I. J. o. E. E., & Science, C. (2019). A new encrypted method in image steganography. *14*(3), 1412-1419.
28. Provos, N., Honeyman, P. J. I. s., & privacy. (2003). Hide and seek: An introduction to steganography. *1*(3), 32-44.
29. Qin, J., Luo, Y., Xiang, X., Tan, Y., & Huang, H. J. I. A. (2019). Coverless image steganography: a survey. *7*, 171372-171394.
30. Qiu, A., Chen, X., Sun, X., Wang, S., Guo, W. J. J. o. I. H., & Protection, P. (2019). Coverless image steganography method based on feature selection. *1*(2), 49.
31. Saha, B., & Sharma, S. J. D. S. J. (2012). Steganographic techniques of data hiding using digital images. *62*(1), 11.
32. Saranya, K., Mohanapriya, R., Udhayan, J. J. I. J. o. S., Engineering, & Research, T. (2014). A review on symmetric key encryption techniques in cryptography. *3*(3), 539-544.
33. Sharda, S., Budhiraja, S. J. I. J. o. E. T., & Engineering, A. (2013). Image steganography: A review. *3*(1), 707-710.
34. Shen, C., Zhang, H., Feng, D., Cao, Z., & Huang, J. J. S. i. C. S. F. I. S. (2007). Survey of information security. *50*(3), 273-298.
35. Stefan, K., & Fabien AP, P. (2000). Information hiding techniques for steganography and digital watermarking. In: Artech House.
36. Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. J. I. A. (2021). Image steganography: A review of the recent advances.
37. Swanson, M. D., Kobayashi, M., & Tewfik, A. H. J. P. o. t. I. (1998). Multimedia data-embedding and watermarking technologies. *86*(6), 1064-1087.
38. Tan, Y., Qin, J., Xiang, X., Ma, W., Pan, W., & Xiong, N. N. J. I. A. (2019). A robust watermarking scheme in YCbCr color space based on channel coding. *7*, 25026-25036.
39. Verma, N. (2011). *Review of steganography techniques.* Paper presented at the Proceedings of the international conference & workshop on emerging trends in technology.
40. Wang, S.-Z., Zhang, X.-P., & Zhang, W.-M. J. C. j. o. c. (2009). Recent Advances in Image Based Steganalysis Research [J]. *32*(7), 1247-1263.
41. Yang, L., Deng, H., & Dang, X. J. I. A. (2020). A novel coverless information hiding method based on the most significant bit of the cover image. *8*, 108579-108591.
42. Zhang, X., Peng, F., & Long, M. J. I. T. o. M. (2018). Robust coverless image steganography based on DCT and LDA topic classification. *20*(12), 3223-3238.
43. Zheng, S., Wang, L., Ling, B., & Hu, D. (2017). *Coverless information hiding based on robust image hashing.* Paper presented at the International conference on intelligent computing.
44. Zhou, Z., Mu, Y., & Wu, Q. J. J. S. C. (2019). Coverless image steganography using partial-duplicate image retrieval. *23*(13), 4927-4938.
45. Zhou, Z., Sun, H., Harit, R., Chen, X., & Sun, X. (2015). *Coverless image steganography without embedding.* Paper presented at the International Conference on Cloud Computing and Security.
46. Zou, L., Sun, J., Gao, M., Wan, W., Gupta, B. B. J. M. t., & applications. (2019). A novel coverless information hiding method based on the average pixel value of the sub-images. *78*(7), 7965-7980.