Delving into the Methods of Coverless Image Steganography

Koi Yee Ng[†], Simying Ong[†], and KokSheik Wong[‡]

[†]Faculty of Computer Science and Information Technology, University of Malaya, Malaysia.
[‡]School of Information Technology, Monash University, Malaysia.
wva190003@siswa.um.edu.my, simying.ong@um.edu.my, wong.koksheik@monash.edu

***Abstract*—Conventional cover-based image steganography methods embed secret information by modifying the original state of a cover image. This type of algorithm leaves a trace of changes on output stego image and eventually leads to successful detection by common steganalysis tools. As a solution, a coverless image steganographic method is proposed, where no cover image is required for embedding secret information. In this paper, the conventional coverless image steganography methods are first reviewed and categorized into constructive and non-constructive-based methods. Next, these methods are summarized and analyzed, followed by a discussion about their advantages and drawbacks. Finally, the performances of the proposed methods are discussed using the common steganography evaluation metrics, including resistance to attack, embedding capacity, and perceptual image quality.**

***Index Terms*—Carrier-less, stego image, constructive, image synthesis**

I. Introduction

With today's ubiquitous internet service, digital images can be conveniently downloaded and shared through social networking services (SNS) such as Facebook, Snapchat, Twitter, etc. Therefore, there are vital needs to provide some mechanisms to manage – originally was 'protection' the vast number of originals images [1, 2]. Information hiding (i.e., data embedding) is the process of inserting external information (e.g., ownership information and secret message) into a medium. It is one of the possible solutions to serve the aforementioned needs. Fig. 1 illustrates the general framework during the data embedding process. Data is inserted into the cover image with a secret key to produce an output image with embedded data, while aiming to achieve high perceptual image quality, large embedding capacity, and strong resistance to attacks.

In the image domain, the application of information hiding can be coarsely categorized as watermarking and steganography [3]. Watermarking is the practice of visibly or invisibly embedding information into images to render the ownership [4]. It can be retrieved for the purposes of claiming ownership during a dispute or to detect tampering of content for integrity checking purpose. On the other hand, steganography is the art and science of concealing the existence of the secret communication via a cover such as image, video, audio, text, etc. [5]. The embedded information should be unnoticeable, or in specific, perceptually undetectable by humans.

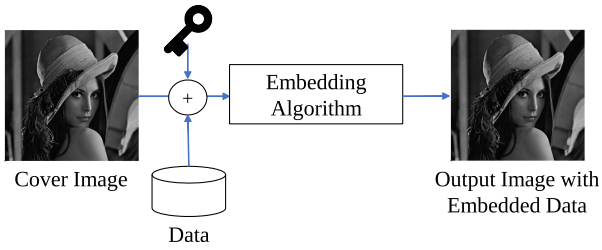

Fig. 1. General framework of information hiding.

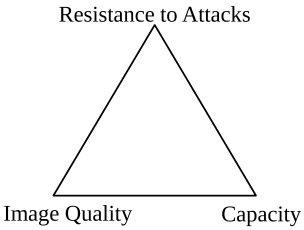

Fig. 2. The "Magic" Triangle: Contradictory requirements of steganography.

There are three important evaluation aspects in steganography, including resistance to attacks, capacity and image quality. Resistance to attacks concerns with the ability to enclose the alteration or hiding of data from unauthorized viewing. Embedding capacity indicates the maximum amount of data which can be hidden into the cover. While the image quality refers to the quality of the image after being utilized for secret embedding. Fig. 2 shows the interrelationship among all three aspects. The main aims of steganography are to increase the embedding capacity and enhance the imperceptibility while maintaining the robustness [6]. However, there is always a contradictory effect on each other. For instance, improving the capacity will decrease the image quality, while improving the output image quality will decrease the capacity, and vice versa. These aspects are important to be measured in steganography to evaluate the performance of the proposed methods and their targeted purposes.

There are a few different types of conventional steganography techniques, which are widely utilized in the current literature, including bit plane replacement, histogram shifting, and pixel expansion. Bit plane replacement (i.e., least significant bit) manipulates the rightmost bit of a pixel during the

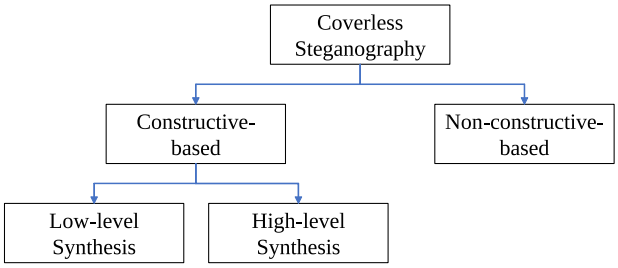

Fig. 3. Classification of coverless steganography.

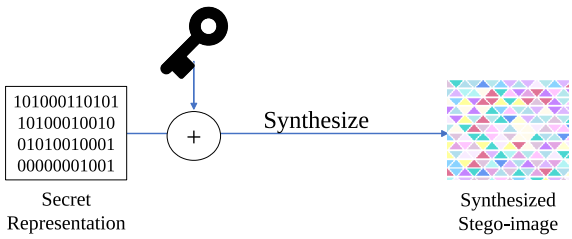

Fig. 4. The framework of constructive-based coverless steganography method [20]

Fig. 5. Example of synthesized texture image with embedded data [21]

embedding of secret. The idea of LSB embedding in image is then generalized by Wang et al. [7] and Chan et al. [8]. This technique can be easily applied to different domains, including image [9, 10], audio [11, 12] and video [13, 14] domains. This method is popular due to its simplicity and insignificant effect on the image perceptual quality since only LSB will be modified. On the other hand, histogram shifting [15] is a simple way to achieve reversibility data hiding. It exploits the zero and peak bins of the pixel histogram to embed the information. The bins next to the peak bin will be shifting one to right or left to prepare an empty bin for secret embedding purpose. For the same purpose of reversibility, Tian [16] proposed to use Difference Expansion (DE). Specifically, the difference between 2 adjacent pixels are converted into binary representations. The secret (i.e., '0' or '1') is then appended to the binary representation after the LSB.

All of the conventional steganography techniques modify the cover image to embed secret. Consequently, they lead to potential issues, since the existing steganalysis methods can detect the secret by analyzing the modification traces caused by secret embedding. Furthermore, existing cover-based steganography methods have limited embedded capacity, i.e., bounded by cover image [17]. Due to all the aforementioned issues, researchers have start to investigate coverless steganography methods, which do not modify the cover to embed secret. In this paper, we study the relevant coverless image steganographic methods. This paper identifies the problems of these methods and analyzes how each technique affects the steganography evaluation aspects, including embedding capacity, perceptual image quality and resistance to attacks.

II. The Rise of Coverless Steganography

In general, coverless image steganography can be categorized into two main types: constructive-based and non-constructive-based as shown in Fig. 3. In constructive-based coverless steganography, the stego images are directly synthesized using secret messages in either Low-Level Synthesis (LLS) or High-Level Synthesis (HLS) manner. For LLS, the decision activity such as labeling of secret is required from human. While for HLS, the framework itself can act autonomously, with the help of supervised learning to synthesize an unnoticeable stego image, as in the methods proposed in [18, 19]. On the other hand, in non-constructive-based steganography, the contents of an image such as the pixel values and color intensities are exploited to represent the secret information.

A. *Constructive-based Coverless Steganography Method*

In constructive-based coverless steganography, stego images are synthesized based on the input of secret message. The framework of this method is illustrated in Fig. 4. The secret is synthesized into a unique stego image without using any cover. To date, various LLS-based coverless steganography are proposed, including the use of texture image [21, 22, 23, 24, 25, 26], pattern image [20] and fingerprint image [27].

1) Low-Level Synthesis (LLS): The concept of texture synthesis steganography is first proposed by Otori and Kuriyama [21, 22] in 2007 and 2009, to create an attractive textual stego image. In this method, the secret is encoded into colored Local Binary Pattern (LBP) dots and painted in Hilbert Curve sequence onto the blank region. The unpainted regions are identified based on the dissimilarity with neighboring pixels and coated using pixel-based texture synthesis method, camouflaging the existence of dotted patterns. Re-coating of pixels is then performed to improve the image quality and finally to synthesize embedded stego images, as shown in Fig. 5. However, this method has a small extraction error and it requires error-correcting codes in recovering the secret. Besides, this method can only perform well in random texture images, and difficult to work in general or structured texture images.

In 2014, Wu and Wang [23] proposed a message-oriented patch-based texture synthesis to conceal the secret messages by resampling small texture images to construct a new stego synthetic texture image. In this method, the image-quilting algorithm [24] is implemented to reduce the visual artifact on the overlapped area of adjacent source patches. However, the transmissions of the images are lossy if the images are compressed. In addition, the image size will increase with

the increase of secret size, generating big output stego image. Also, it suffers from various attacks [28].

In 2017, Qian et al. [25] proposed to use a small texture pattern to construct a message-oriented texture image. A source texture pattern is first divided into overlapped candidate tiles and mapped to their respective categories based on the computed texture complexities using standard deviation. With key, the candidate tile is selected from the represented category and painted onto the canvas by using the proposed texture synthesis algorithm. The receiver will need to extract the candidate tiles using the valid key. Due to the use of small texture patterns for secret representation, the stego image have good capability in withstanding JPEG compression attack.

In 2018, Wei et al. [26] proposed a steganography scheme based on super-pixel structure and Support Vector Machine (SVM) as the solution for the information loss after image compression. Their work is similar to that of Qian et al. [25]. However, in their method, they use Simple Linear Iterative Clustering (SLIC) based super-pixel partitioning and the trained SVM classifier to classify the categories. The steganographic schemes proposed in this paper have better results in withstanding compression and it is more robustness than [25].

In the same year, a novel coverless steganography method to synthesize pattern image is proposed by Lee et al. [20]. In their method, they proposed to use three properties, namely, color, size and position to represent different secret messages. For instance, 16 different colors are used to represent different 4-bit secret messages in their experiment. Therefore, an image with different colors will be synthesized based on the secret message during the embedding process. This method can synthesize the secret into visual plausible image; however, it suffers from low resistance to brute force attack.

Seeing the existing method may arouse suspicion, Li and Zhang [27] proposed to synthesize fingerprint images from the construction of the composite phase of the fingerprint using secret in 2019. The secret message is mapped to a polynomial and encoded into a set of two-dimensional points with different polarities to mimic the fingerprint minutiae, to construct the spiral phase and continuous phase of the fingerprint. They then combined the spiral phase and continuous phase to form the hologram phase, based on the constructed composite phases, including the binary fingerprint image, the thinned fingerprint image, and the grayscale fingerprint image.

2) High-Level Synthesis (HLS): Since 2018, generative adversarial network (GAN) has been applied in HLS steganography method, and referred as generative steganography. The idea of GAN is proposed by Goodfellow [29], where the generator will produce realistic-looking fake image samples based on the training image dataset from noise. On the other hand, the discriminator will identify the fake image, aiming to improve the generated image to become more realistic. This concept is implemented in steganography to synthesize unnoticeable natural stego image using the input secret.

In 2018, Liu et al. [18] proposed to use Binary Controllable Generative Adversarial Network (BCGAN) to directly generate higher-quality images from the secret. The text information to-be-hidden is first encoded in binary code based on the dictionary, combined with the encoded secret information and the noise to generate the image samples using BCGAN. To avoid incorrect orders of images received due to network delays and attacks, the senders need to mark a serial number in each head (start) of secret. The receiver then utilizes an auxiliary classifier and a series of conversion functions to extract the secret from the secret images in sequence respectively, using the serial number.

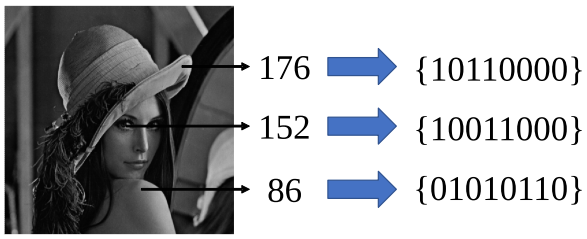

Fig. 6. The use of contents (i.e., intensity values) in an image to represent secret information.

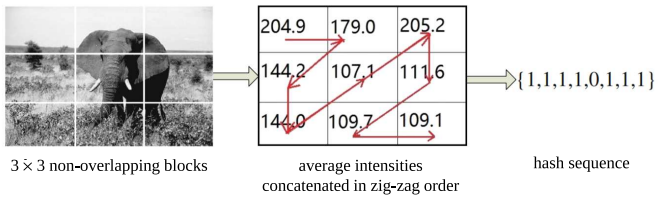

Fig. 7. The novel non-constructive-based framework proposed by Zhou et al. [30].

In the same year, Hu et al. [19] proposed to use Deep Convolutional Generative Adversarial Networks (DCGANs) to generate stego images. In this method, the secret information is first divided into segments and mapped to the interval of noise level to generate a stego image using DCGAN. An extractor is trained using the same setting as the encoder but in a reverse manner to retrieve the secret data from stego images. However, there will be an increase in error rate as the secret size increases.

B. Non-constructive-based Coverless Steganography Method

As shown in Fig. 6, the non-constructive-based method utilizes the contents of a selected image to represent the secret information. In 2015, Zhou et al. [30] first proposed to represent the secret using the intensity values of a selected image. Several images are first collected to construct a stego image database. As shown in Fig. 7, each stego image is divided into nine non-overlapping blocks to compute their average intensity values within each block. By using robust hash sequence, an 8-bit secret represented in each stego image is then generated based on the intensity values of the next block. The senders will segment the secret into 8-bit length, and the stego images which have the same hash sequence as the segment will be retrieved from the database using an

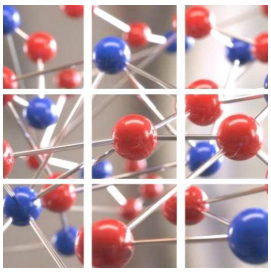

Fig. 8. The molecular structure images of material (MSIM). [32]

inverted index structure search, and sent to the receivers in sequence. During extraction, the receivers need to concatenate all the represented hash sequence of the received stego images (following the correct sequence) to retrieve the secret. However, the receivers might retrieve the secret incorrectly if the stego images are not received in sequence due to network delays or attacks.

In 2017, Zheng et al. [31] further enhanced the capacity of [30] by hashing the direction of the Scale Invariant Feature Transform (SIFT) instead of the intensity values of each stego image. The local extreme point of each layer of the image difference pyramid in each image block will be first calculated. For each stable point extracted from the image blocks, an appropriate window size is selected around the point to form a circular area. The gradient directions of all the sampling points in the window are accumulated to form a histogram. The values within the histogram will be compared to obtain the max value and represented by one of the four directions in the hash map, where each direction will represent 2-bit. By dividing the stego image into nine blocks, each block can represent 2-bit to obtain a total of 18-bit binary sequences in each stego image. However, this method requires an additional image as the side information for the receiver. If the attackers analyze the additional image, they can easily obtain useful information to extract the hidden secret.

In 2018, Cao et al. [32] utilizes the molecular structure images of material (MSIM), where the image consists of atoms with various colors (as shown in Fig. 8) to obtain distinct average image pixel values. The pixel values (i.e., 0 to 255) are divided into 8 intervals, and each interval represents a 4-bit binary secret. At the same time, the stego images are divided into 9 blocks to compute the average pixel values and mapped to the corresponding 4-bit binary sequence. To improve the search efficiency of the matching stego image, multilevel inverted index structure is utilized to first calculate the peak values of the frequency histogram, followed by corresponding visual word's ID, labels, the average pixel values intervals, and finally the satisfied stego image.

In the same year, Zou et al. [33] implemented a similar method on the secret embedding of Chinese sentences. The author first built a dictionary which is composed of 4 parts, including the subjects, predicate, object, and preposition. Each Chinese word will be placed on the designated position in a dictionary based on their parts. Meanwhile, each stego image is divided into 80 blocks (i.e., 8 rows and 10 columns) to obtain the hash sequence of 80 bits. The hash sequence will be divided into 4 segments and labeled according to the decimal of 20-bit hash. The corresponding 20-bit sequence will be obtained based on the position of the word in the dictionary. Finally, an image where each block matches all 4 20-bit sequence will be used to represent the secret.

Wu et al. [34] proposed to calculate the grayscale gradient co-occurrence matrix (GGCM) of an image and establish an image database based on GGCM. The represented secret is then mapped to the library and coded by Turbo encoding to protect the secret. Their experimental results show that the proposed method is able to resist various attacks.

In summary, the conventional non-constructive-based coverless steganography mainly utilizes the intensity values to compute the average pixel value in each block and represent the secret by selecting satisfied stego images. It can retain the quality of the image by not performing any modification on the stego image, eventually resisting detection by steganalysis. However, all of them have a lower capacity compared to conventional steganography methods. They cannot efficiently embed a long secret message within an image, but require the multiples images transmitted to the receivers for secret representation. However, network problems may affect the orders of received stego images, resulting in wrong retrieval of secret. Also, the senders are required to set up a huge image database for secret representation.

On the other hand, in constructive-based steganography method, stego images can be synthesized in LLS and HLS manner based on the input secret and can retain high embedding capacity. However, it might cause the increase of stego image size when secret size is large. Also, for certain methods, it is hard to retain the robustness of stego images after they are compressed for transmission purposes, causing wrong retrieval of secret at the receiver side.

Fig. 9 summarizes the first use of each constructive and non-constructive-based coverless steganography methods. In general, cover-based steganography methods are widely used to embed secret messages for transmission. However, the proposed steganography methods are not secure after various steganalysis tools are developed to extract the secret message by analyzing the modification traces of the cover images. Soon, the first coverless steganography method, texture synthesis [21] is proposed in 2007 to synthesize the texture stego image from secret information without using any cover. In 2015, mapping of secret representations to the image contents using image hashing [30] is then proposed. It uses the information within an image such as the pixel intensity to represent the secret. Pattern synthesis [20] is then proposed under the constructive-based steganography in 2018. In the same year, researchers started to integrate the steganography with deep learning, GAN to synthesize images. In 2019, fingerprint synthesis [27] is also proposed in the constructive-based steganography method. Both low and high-level constructive-based methods are able to achieve high embedding capacity, since the embedding capacity of the stego

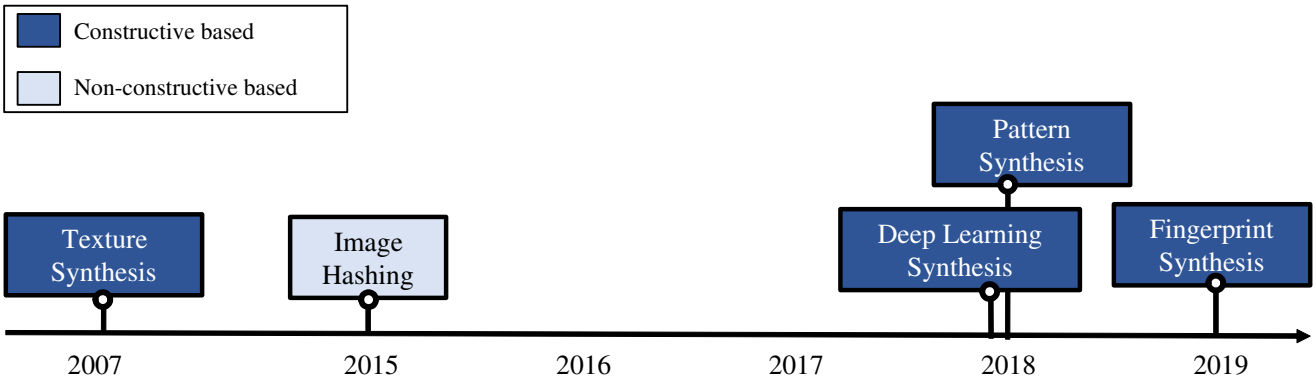

Fig. 9. First use of each coverless image steganography method.

image is proportional to the secret size. Also, they have high resistance to the steganalysis because no cover has been used in their methods.

III. Analysis and Discussion

In this section, the performances of each proposed method are analyzed using three main evaluation parameters, including resistance to attacks, embedding capacity, and perceptual image quality. The following results are all datasets from the discussed paper. Performance comparisons have been done for all the proposed methods and the results are summarized in the following subsections.

A. Resistance to Attacks

Table I summarizes attacks where each paper utilizes to evaluate their proposed methods. The attack methods are categorized into 5 groups, which are common image processing operations, noises, filters, special attack, and miscellaneous attack.

1) Common Image Processing Operation: Rescaling of the stego image is performed in paper [30, 31, 34, 27]. Both methods utilized in [30, 31] are able to achieve 100% success extraction rate after rescaling has been applied onto the stego image since there is no significant change in the intensity correlation between image blocks. For [34], the stego images were rescaled from the ratio of 0.3 to 3.0, and it achieved a small error rate (bit error rate) of less than 0.098. For [27], it is not stable in resisting rescaling attack because it achieved distinct error rates between 0.9% and 61.7% when tested with different sizes of binarized, thinned, and grayscaled fingerprint stego images rescaled at the ratio of 0.995.

Besides, luminance change and contrast enhancement have been tested in paper [30, 31, 33] and there is no significant effect on the results after both attacks have been carried out since all pixels in the stego images will be added or multiplied by a constant. Therefore, the hash sequence of the stego image will remain unchanged when the correlation between image blocks is not affected.

JPEG compression has also been tested in [30, 31, 34, 25, 26, 27]. Zhou et al.'s method [30] can achieve a 0.03% error rate after being compressed using the StirMark attack with default attack parameters. Zheng et al.'s method [31] achieved the error rate from 0.034 to 0.125 after being compressed at the quality factor from 60 to 95. Wu [34] achieved an error rate of as low as 0.007 at the quality factor of 50. As for the method used in [25], it achieved the error rate of as low as 7.7% at the quality factor of 50. The method proposed by Wei et al. [26] achieved an average error rate of 0.04 at the quality factor of 1. For [27], it achieved an error rate from 0% to 21.1% at the quality factor of 5, and a 0% error rate for the quality factor of 25 and above. Among all these methods, the method proposed by Wei et al. [26] has outperformed the others when super-pixel structure was implemented, and consistently achieved the lowest error rate after jpeg compression with a quality factor of 1 was used.

Wu et al. [34] and Li et al. [27] had also tested on rotation. The method proposed in [34] has higher resistance than [27] when it achieves a zero error rate with different angles of rotation applied during the experiment. Whereas, the method proposed in [27] achieved 0% to 36.8% and 1.3% to 72.8% error rate when the stego images were rotated at the angle of 0.25° and 0.5°, respectively. The method proposed by Wu et al. in [34] also outperformed Li et al.'s methods [27] in the testing of resistance to rotation since the rotation does not give any significant effect.

Also, Li et al. [27] tested on different common image processing operation attacks such as sharpening, shearing, linear transform, line removal, and cropping. The error rate results from the experiment range from 1.1% to 100%, indicates the instability of the proposed method in resisting the attacks.

2) Noise: Li et al. [27] tested on random noise and the results show error rates between 0% to 100% when the proposed method is tested with different noise intensities. Li et al. [27] and Wu et al. [34] also tested on salt & pepper noise attack. The method proposed by Wu et al. in [34] has outperformed Li et al.'s methods [27] in the testing of

TABLE I
EXPERIMENTS ON VARIOUS ATTACKS PERFORMED IN EACH PAPER.

ATTACKS	PAPER										
	[30]	[31]	[33]	[34]	[23]	[25]	[26]	[20]	[27]	[18]	[19]
Common Image Processing Operation											
Rescaling	✓	✓		✓					✓		
Luminance Change	✓	✓	✓								
Contrast Enhancement	✓	✓	✓								
JPEG Compression	✓	✓		✓		✓	✓		✓		
Rotation				✓					✓		
Sharpening									✓		
Shearing									✓		
Linear Transform									✓		
Line Removal									✓		
Cropping									✓		
Noise											
Random Noise									✓		
Salt & pepper				✓					✓		
Gaussian Noise Adding	✓	✓		✓							
RS Detection [35]					✓						
Filter											
Median Filter									✓		
Mean Filter				✓							
Gaussian Filter				✓					✓		
CMFF [36]											✓
Special Attack											
Spiral Alteration									✓		
Fingerprint Binarization									✓		
Fingerprint Thinning									✓		
SCNN [37]										✓	
CRM [38]											✓
CNN based steganalyzer [39]											✓
Miscellaneous Attack											
Statistical Attack								✓			
Comparison Attack								✓			

resistance to salt & pepper attack with the results of 0.0005 error rate at the noise point of 0.04.

Gaussian noise addition was tested in paper space[30, 31] with varying degrees of Gaussian noise ranging from 0.005 to 0.01. Zhou [30] achieve a low error rate of 0.02, while Zheng [31] achieved an error rate between 1.2% to 11.7%. In [34], it shows an increase in error rate with the increase of noise variance.

3) Filter: Li et al. [27] also tested on 3×3 window median filter. From the results, it shows an unstable outcome of error rate from 9.6% to 100% when the proposed method is tested. Then, Wu et al. [34] also tested on mean filter. The experiment shows an increase error rate with the increase of mean filter size. For [19], Hu et al. proposed the use of CMFF [36], which is a CNN-based forensics algorithm with image median filtering, to detect the stego images. As a result, there is a 0% probability of stego images being identified. Lastly, Wu et al. [34] and Li et al. [27] had also tested on Gaussian filter. The method proposed by Wu et al. in [34] also outperformed Li et al.'s methods [27] in the testing of resistance to Gaussian filter attacks.

4) Special Attack: Besides all the aformentioned attacks, Wu et al. [23] had also tested on the RS detection attack [35]. The difference value computed between regular group R_M and R_{-M} is similar to the difference value computed for pure synthetic texture, indicating the proposed methods can resist the RS detection attack.

Li et al. [27] also tested on different attacks spiral alteration, fingerprint binarization and fingerprint thinning. From the results, it shows an unstable outcome which has a wide range of error rate (i.e., from 0% to 39%) when the proposed method is tested with different attacks.

In [18], an experiment is carried out to test the test set which consists of generated stego images and original images using Shallow Convolutional Neural Network (SCNN) [37]. The result showed that there was a 50% probability of the synthesized images being identified by the steganalysis tool. For [19], the authors proposed to use CRM [38] and CNN based steganalyzer [39] to detect the stego images. As a result, there is a 0.8% and 47% probability of stego images being identified using the respective tools.

5) Miscellaneous Attack: Lee et al. [20] claimed their proposed method is able to resist statistical and comparison attacks. The statistical attack analyzes the image statistical properties to identify modification traces caused by secret embedding while comparison attack detects suspicious images and extract the secret by using side-by-side comparison with the original image. This is because the proposed method did

TABLE II
COMPARISONS OF PERFORMANCES BETWEEN DIFFERENT COVERLESS STEGANOGRAPHY METHOD.

METHOD	CAPACITY
Constructive-based method	
[22]	low
[23]	scalable
[25]	scalable
[26]	scalable
[20]	scalable
[27]	high
[18]	high
[19]	high
Non-constructive-based method	
[30]	low
[31]	low
[32]	low
[33]	low
[34]	low

not modify any cover to embed the secret message, leaving no modification traces. However, the aforementioned attacks were only briefly discussed in [20], but there is no detailed experiment done in proving their claims.

In short, based on the experimental results, non-constructive methods might have higher resistance to attacks compare to constructive-based methods. As we can see from the results, the attacks give minimal impact on [30, 31, 32, 34]. There are not many attacks applicable on those stego methods, since the stego images contents are used to represent the secret. On the other hand, the experiment results of constructive-based steganography method show various attacks can work effectively on the synthesized stego images and having lower resistance to non-constructive-based steganography method.

B. Capacity

Table II summarizes the capacity performance of each proposed method. In the construction-based approach, the stego image is directly generated based on the input of the secret message. [21, 22] first proposed to conceal the secret during texture synthesis, and this method is able to embed 25 to 100 bytes. In [23, 25, 26], the capacity of an embedded secret can be flexibly adjusted based on the sizes of the stego images. Larger stego image is able to embed more secret bits. In [25], 1600 bits is able to be embedded in a stego image sized 653. Based on our understanding, [26] inherits a similar amount of capacity as of [25] because of the close resemblance of both methods. On the other hand, [20] proposed to embed secret using pattern image, which the secrets are represented by image attributes such as shape, size, and color. The experiment utilized 16 different colors to represents 4 bits secret. This method is able to embed 4480 bits in a synthesized image. By combining multiple attributes in an image or enlarging the stego image, it is able to embed more. For fingerprint, capacity depends on the resolution of the constructed fingerprint image. In the high-level constructive-based method [18, 19], the stego images are synthesized solely based on the secret size. Therefore, this method is able to synthesize a stego image with high embedding capacity.

On the other hand, the hashing method is mainly utilized in non-construction-based approach, and the embedding capacity of each image is calculated based on the number of the segmented blocks. The total embedding capacity of non-construction-based approach is as shown below:

$$TC = \text{BPB} \times EP \tag{1}$$

where TC indicates the total embedding capacity, BPB indicates bit per block and EP indicates the number of embeddable blocks. In [30], the stego image is divided into nine blocks, where each block represents 1-bit to embed a total of 8-bit in a stego image. [31] further enhanced the capacity of [30] using SIFT and each block represents 2 bits to achieve a total embedding bits of 18 in each stego image. [32] categorized the intensity values into 8 intervals, each represents 4 binary bits. By dividing the images into 9 blocks, the stego images managed to hide 36 bits. [33] then divided the stego images into more blocks (i.e., 8 columns and 10 rows) to embed 80 bits in a stego image. From the analysis of the papers, the embedding capacity are enhanced from time to time. Also, by dividing the image into more blocks, it is able to embed more secret messages. However, all these proposed methods still has a lower embedding capacity compared to conventional steganography methods. The capacity is still not sufficient enough to embed a longer message. Therefore, multiple images are required to represent more secret.

In short, the methods proposed in constructive-based steganography have higher capacity than the non-constructive-based methods. In non-constructive-based methods, multiple images are required to represent longer secret messages due to the limitation of the images. On the other hand, constructive-based methods utilize mainly the secret to synthesize a stego image. Therefore, the capacity is based on the input of secret size, which is usually scalable or high.

C. Image Quality

For constructive-based methods, the naturality of the synthesized image is important to avoid arousing suspicion. Since there is no cover image involved in coverless methods, existing objective evaluations such as the computation of PSNR or SSIM utilized in conventional image steganography methods cannot be used in evaluating the image quality of the synthesized image. Therefore, in most existing papers, only subjective evaluation are performed on the synthesized stego images.

Nevertheless, certain papers mentioned the measurement of image quality in evaluating the synthesized image. In [23], mean squared error of the overlapped area (MSEO) is computed to determine the similarity between the synthetic patch and the candidate patch areas. When more secrets are conveyed in each patch, the MSEO value increases. Besides, Pearson Product Moment Correlation (PPMC) is used to measure how well the two variables are related. As a result, the proposed method can preserve a high PPMC values, which eventually preserve a visual plausible image. In [25], no experiment has

been conducted to test the image quality. However, the authors claimed that the stego textures can preserve a good visual appearance using their proposed method. Same goes to Wei et al. [26] and Qian et al. [25]'s method. In [20], the authors carefully selected the colors during the synthesis of the color pattern images to generate a visual plausible image. For [27], they proposed to use fingerprint images as the stego images. The synthesized image was natural enough when the average awareness of the spiral alteration by the attackers is less than 50%. On the other hand, in high-level synthesis method, [18, 19] synthesized human face using GAN. However, based on our observation, the output synthesized images of human faces are not natural and might arouse suspicion.

For non-constructive-based methods, the selected images will be used to represent the secret information without the need to perform any modification on the them. Therefore, the quality of the images can be preserved same as the original images.

In short, at present, there is no existing benchmark in evaluating the image quality of the synthesized images. Most authors performed subjective evaluations on the stego images to ensure they are not arousing suspicion. Only certain papers compared the secret embedded patches with their neighbor patches. In non-constructive-based methods, images are selected to represent the secret without modifying them; therefore preserving the image quality.

IV. Recommendation and Future Research Direction

Coverless steganography has started to raise the attention of researchers today since it can embed secret data without using any cover. However, there is no available detailed and specific evaluation benchmark for each coverless steganography method. Most of the papers do not provide the experiments to prove the performance of the proposed method for each important property of information hiding, namely resistance to attack, embedding capacity, and perceptual image quality.

The parameters and suggested evaluations are intended to cater to general coverless methods. More specific evaluations can always be utilized, depending on the application domain or the types of generated stego image. In recent years, most of the researchers are focusing on constructive-based methods due to its flexibility in embedding capacity. However, based on our analysis, there are still many rooms for improvements left in these methods, such as higher perceptual image quality and strong robustness in evaluating the robustness of coverless image steganography methods, attacks from the first three categories, namely common image processing attack (10 attacks), noise (4 attacks) and filter (4 attacks) can be utilized to evaluate the resistance to attacks. Special attacks and miscellaneous attacks are optional. As for special attacks, they are only applicable to be used in their own domains, respectively. For instance, spiral alteration and fingerprint binarization can only be performed on synthetic fingerprint images. From miscellaneous attacks, coverless methods will always resist comparison attacks because there is no original image which can be used for comparison.

As for embedding capacity evaluation, we are still suggesting the utilization of conventional measurement which is bits per pixel for constructive-based methods. It is difficult to compare the capacity performance in the current state-of-the-art methods because all of them are synthesizing stego images of varies sizes. Hence, it is easier to measure and compare if all the coverless methods are standing on the same ground, which is by measuring the embedded bits over the number of synthetic image pixels. For non-constructive-based methods, we should take into consideration the number of selected images in representing secret data and the number of embedded bits to compare the capacity performance with other similar coverless methods.

In terms of perceptual image quality assessment, non-constructive-based methods will always maintain the highest state of quality because images are only selected to represent information. For constructive-based methods, they should be evaluated in two directions, including subjective and objective evaluations. Survey or interview can be performed by inviting human tester in identifying suspicious-looking synthetic stego image against natural image. Besides, specific synthetic images such as fingerprint, subjective evaluation can be tested by inviting the domain experts. For objective evaluation, no-reference image assessment metric, such as Blind/Referenceless Image Spatial Quality Evaluator (BRISQUE) [40] can be utilized in accessing the naturality or imperceptibility of the synthetic stego images.

V. Conclusions

In this paper, we studied and analyzed various types of coverless image steganography methods. In addition, we categorized each method into constructive and non-constructive-based methods depending on the nature of the algorithm in hiding secret data in a coverless manner. For non-constructive methods, the secret is represented by the information, e.g. pixel intensities in the image. On the other hand, constructive-based steganography refers to the synthesis of stego images using the secret information via a low- or high-level manner. The strengths and weaknesses of each method are also highlighted in this paper. Then, the timeline of each first used coverless steganography method is presented. Besides, we also evaluated each of the coverless methods in three important parameters for steganography, namely resistance to attacks, embedding capacity and perceptual image quality. Finally, we provided some recommendations on the evaluation methods. In the future, we aim at exploring the other coverless steganography methods and proposing a standard benchmark on the evaluation of non-constructive-based methods.

Acknowledgment

This work was supported by the Faculty of Computer Science and Information Technology, University of Malaya under RU Geran - Fakulti Program UM.0000628/HRU.OP.RF,

GPF008D-2018 (Project title: Carrierless Image Information Hiding via High-Level Image Synthesis Approach).

REFERENCES

[1] A. K. Singh, B. Kumar, S. K. Singh, S. Ghrera, and A. Mohan, "Multiple watermarking technique for securing online social network contents using back propagation neural network," *Future Generation Computer Systems*, vol. 86, pp. 926–939, 2018.

[2] A. Castiglione, B. D'Alessio, and A. De Santis, "Steganography and secure communication on online social networks and online photo sharing," in *2011 international conference on broadband and wireless computing, communication and applications*. IEEE, 2011, pp. 363–368.

[3] N. F. Johnson, Z. Duric, and S. Jajodia, *Information Hiding: Steganography and Watermarking-Attacks and Countermeasures: Steganography and Watermarking: Attacks and Countermeasures*. Springer Science & Business Media, 2001, vol. 1.

[4] W. P. Fang, J. S. Kuo, V. Ip *et al.*, "Using digital hiding to revitalize traditional chinese proverb," in *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. Springer, 2017, pp. 314–321.

[5] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal processing*, vol. 90, no. 3, pp. 727–752, 2010.

[6] M. K. Ramaiya, N. Hemrajani, and A. K. Saxena, "Improvisation of security aspect in steganography applying des," in *2013 International Conference on Communication Systems and Network Technologies*. IEEE, 2013, pp. 431–436.

[7] R. Z. Wang, C. F. Lin, and J. C. Lin, "Image hiding by optimal lsb substitution and genetic algorithm," *Pattern Recognition*, vol. 34, no. 3, pp. 671 – 683, 2001. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0031320300000157

[8] C. K. Chan and L. M. Cheng, "Hiding data in images by simple lsb substitution," *Pattern recognition*, vol. 37, no. 3, pp. 469–474, 2004.

[9] X. Liao, Q.-y. Wen, and J. Zhang, "A steganographic method for digital images with four-pixel differencing and modified lsb substitution," *Journal of Visual Communication and Image Representation*, vol. 22, no. 1, pp. 1–8, 2011.

[10] A. Singh and H. Singh, "An improved lsb based image steganography technique for rgb images," in *2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*. IEEE, 2015, pp. 1–4.

[11] M. Asad, J. Gilani, and A. Khalid, "An enhanced least significant bit modification technique for audio steganography," in *International Conference on Computer Networks and Information Technology*. IEEE, 2011, pp. 143–147.

[12] S. Divya and M. R. M. Reddy, "Hiding text in audio using multiple lsb steganography and provide security using cryptography," *International journal of scientific & technology research*, vol. 1, no. 6, pp. 68–70, 2012.

[13] M. Ramalingam, "Stego machine–video steganography using modified lsb algorithm," *World Academy of Science, Engineering and Technology*, vol. 74, pp. 502–505, 2011.

[14] P. Yadav, N. Mishra, and S. Sharma, "A secure video steganography with encryption based on lsb technique," in *2013 IEEE International Conference on Computational Intelligence and Computing Research*. IEEE, 2013, pp. 1–5.

[15] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," in *Proceedings of the 2003 International Symposium on Circuits and Systems, 2003. ISCAS'03.*, vol. 2. IEEE, 2003, pp. II–II.

[16] J. Tian, "Reversible data embedding using a difference expansion," *IEEE transactions on circuits and systems for video technology*, vol. 13, no. 8, pp. 890–896, 2003.

[17] A. K. Hmood, H. A. Jalab, Z. Kasirun, B. Zaidan, and A. Zaidan, "On the capacity and security of steganography approaches: An overview," *Journal of Applied Sciences(Faisalabad)*, vol. 10, no. 16, pp. 1825–1833, 2010.

[18] M. M. Liu, M. Q. Zhang, J. Liu, and X. Y. Yang, "Generative steganography based on gans," in *International Conference on Cloud Computing and Security*. Springer, 2018, pp. 537–549.

[19] D. Hu, L. Wang, W. Jiang, S. Zheng, and B. Li, "A novel image steganography method via deep convolutional generative adversarial networks," *IEEE Access*, vol. 6, pp. 38 303–38 314, 2018.

[20] W. K. Lee, S. Ong, K. Wong, and K. Tanaka, "A novel coverless information hiding technique using pattern image synthesis," in *2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*. IEEE, 2018, pp. 1122–1127.

[21] H. Otori and S. Kuriyama, "Data-embeddable texture synthesis," in *International Symposium on Smart Graphics*. Springer, 2007, pp. 146–157.

[22] H. Otori and S. Kuriyama, "Texture synthesis for mobile data communications," *IEEE Computer Graphics and Applications*, vol. 29, no. 6, pp. 74–81, Nov 2009.

[23] K.-C. Wu and C.-M. Wang, "Steganography using reversible texture synthesis," *IEEE Transactions on Image Processing*, vol. 24, no. 1, pp. 130–139, 2014.

[24] A. A. Efros and W. T. Freeman, "Image quilting for texture synthesis and transfer," in *Proceedings of the 28th annual conference on Computer graphics and interactive techniques*. ACM, 2001, pp. 341–346.

[25] Z. Qian, H. Zhou, W. Zhang, and X. Zhang, "Robust steganography using texture synthesis," in *Advances in Intelligent Information Hiding and Multimedia Signal Processing*. Springer, 2017, pp. 25–33.

[26] W. Wei, A. Chengfeng, L. Wang, and H. Ma, "A tex-

ture synthesis steganography scheme based on superpixel structure and svm," in *International Conference on Intelligent Information Processing*. Springer, 2018, pp. 375–383.

[27] S. Li and X. Zhang, "Toward construction-based data hiding: from secrets to fingerprint images," *IEEE Transactions on Image Processing*, vol. 28, no. 3, pp. 1482–1497, 2019.

[28] H. Zhou, K. Chen, W. Zhang, and N. Yu, "Comments on "steganography using reversible texture synthesis"," *IEEE Transactions on Image Processing*, vol. 26, no. 4, pp. 1623–1625, 2017.

[29] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial nets," in *Advances in neural information processing systems*, 2014, pp. 2672–2680.

[30] Z. Zhou, H. Sun, R. Harit, X. Chen, and X. Sun, "Coverless image steganography without embedding," in *International Conference on Cloud Computing and Security*. Springer, 2015, pp. 123–132.

[31] S. Zheng, L. Wang, B. Ling, and D. Hu, "Coverless information hiding based on robust image hashing," in *International Conference on Intelligent Computing*. Springer, 2017, pp. 536–547.

[32] Y. Cao, Z. Zhou, X. Sun, and C. Gao, "Coverless information hiding based on the molecular structure images of material," *Computers, Materials & Continua*, vol. 54, no. 2, pp. 197–207, 2018.

[33] L. Zou, J. Sun, M. Gao, W. Wan, and B. B. Gupta, "A novel coverless information hiding method based on the average pixel value of the sub-images," *Multimedia Tools and Applications*, pp. 1–16, 2018.

[34] J. Wu, Y. Liu, Z. Dai, Z. Kang, S. Rahbar, and Y. Jia, "A coverless information hiding algorithm based on grayscale gradient co-occurrence matrix," *IETE Technical Review*, vol. 35, no. sup1, pp. 23–33, 2018.

[35] J. Fridrich, M. Goljan, and R. Du, "Detecting lsb steganography in color, and gray-scale images," *IEEE multimedia*, vol. 8, no. 4, pp. 22–28, 2001.

[36] J. Chen, X. Kang, Y. Liu, and Z. J. Wang, "Median filtering forensics based on convolutional neural networks," *IEEE Signal Processing Letters*, vol. 22, no. 11, pp. 1849–1853, 2015.

[37] M. M. Liu, M. Q. Zhang, J. Liu, and P. X. Gao, "A steganalysis method based on shallow convolution neural network," *Journal of ShanDong University (Natural Science)*, vol. 53, no. 3, pp. 63–70, 2018.

[38] M. Goljan, J. Fridrich, and R. Cogranne, "Rich model for steganalysis of color images," in *2014 IEEE International Workshop on Information Forensics and Security (WIFS)*. IEEE, 2014, pp. 185–190.

[39] J. Ye, J. Ni, and Y. Yi, "Deep learning hierarchical representations for image steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2545–2557, 2017.

[40] A. Mittal, A. K. Moorthy, and A. C. Bovik, "Blind/referenceless image spatial quality evaluator," in *2011 conference record of the forty fifth asilomar conference on signals, systems and computers (ASILOMAR)*. IEEE, 2011, pp. 723–727.