IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 20 September 2023, accepted 8 October 2023, date of publication 12 October 2023, date of current version 18 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3324050

RESEARCH ARTICLE

A Novel Hybrid Image Synthesis-Mapping Framework for Steganography Without Embedding

RONG HUANG[1], CHUNYAN LIAN[1], ZHEN DAI[1], ZHAOYING LI[2], AND ZIPING MA[3]

[1]School of Software, Hunan Vocational College of Science and Technology, Changsha 410118, China
[2]Chenzhou Comprehensive Vocational Secondary School, Chenzhou 423000, China
[3]School of Computer Science and Engineering, Central South University, Changsha 410083, China

Corresponding authors: Chunyan Lian (chunyanlian@gmail.com) and Zhaoying Li (m13142250796@163.com)

This work was supported in part by the Natural Science Foundation of Hunan Province under Grant 2020JJ7042, in part by the Hunan Provincial Education Science Planning Project under Grant XJK21BZJ011.

ABSTRACT Steganography without embedding (SWE) methods, which avoid modifying container images and are thus theoretically immune to steganalysis tools, have drawn great attention. However, current SWE techniques, including synthesis-based and mapping-based methods, still present challenges that need to be solved. Specifically, the former ones can hardly recover secret messages completely, whereas the latter ones face the problems of low payload capacity and a large number of required container images. In this paper, a hybrid synthesis-mapping framework is designed for SWE to address the aforementioned issues. Specifically, an image synthesis module is designed using a disentanglement auto-encoder to hide the principal component of the secret message into a synthesis image. Another image mapping module is designed to hide the compressed extraction error from the synthesis module by mapping additional container images based on block statics hash matching. Since the length of the compressed error is significantly shorter than the original message, only a few images are required. To the best of our knowledge, this is the first time to fuse synthesis-based and mapping-based modules to harness their complementary strengths. Extensive experimental results have demonstrated our method significantly outperforms state-of-the-art SWE methods.

INDEX TERMS Steganography without embedding, image synthesis, image feature mapping, disentanglement auto-encoder, block statistical hash.

I. INTRODUCTION

Image steganography aims to hide secret messages into container image without arousing suspicion for the conceal communication. It is widely used in military intelligence, confidential data transfer, digital watermarking, and various other fields where the security of transmitted information is important. Traditional Image steganography methods embed the secret information by modifying the pixels of the texture-rich regions of a carrier image, which are selected by either handcraft-designed strategies [1], [2], [3], [4], [5] or deep learning (DL)-based mechanisms [6], [7], [8], [9], [10], to enhance the undetectability. However, it is difficult for them to fundamentally avoid the detection risks of the existence of secret message by using advanced steganalysis tools since they still cause distortions on carrier images.

Recently, an emerging technique namely steganography without embedding (SWE) is proposed by selecting or generating container images for conceal communication. This technique avoids directly modifying the container image, and thus is theoretically immune to typical steganalysis tools [11].

Current SWE methods can be classified into two main categories: synthesis-based [12], [13], [14] and mapping-based techniques [15], [16], [17]. The former utilizes deep synthesis methods, such as generative adversarial networks

The associate editor coordinating the review of this manuscript and approving it for publication was Joewono Widjaja.

(GANs) [18], [19], [20], to synthesize images and hide secret message in their latent space. While the latter selects suitable images from an existing image set as carriers by matching the secret message and image hashes. The key weakness of the synthesis-based technique is that the secret message can hardly be recovered completely at the receiver side even without attack. While mapping-based techniques pose the challenge of a low payload capacity, which is limited by the size of the image set for container selection. In addition, the required number of candidate images increases exponentially with a increase in the length of secret messages. In this manner, the number of images required for conceal communication for even a short secret message is quite large, which will also increase the suspicion risks owing to the unusual behavior of sending extensive images.

To address the above mentioned issues of current SWE methods, a novel two stage framework including an image synthesis module and an image mapping module, namely synthesis-mapping hybrid SWE (SMH-SWE), is proposed. In the synthesis module, a auto-encoder(AE) is trained to disentangle the image structural and texture features. And then the principal part of the secret message is hidden into the synthesis image by swapping the structural features. In the mapping module, the extraction error of the synthesis module is compressed losslessly as secret residuals. Container images are then selected by matching their block statistical hashes to the compressed secret residuals. Since the lengths of the compressed secret residuals are significantly shorter than those of the original message, only a few images are required.

The main contributions of our proposed SMH-SWE are highlight as below:

- We propose a two stage SWE framework by fusing an image synthesis module and an image mapping module. Extensive experimental evaluations demonstrate superior performance compared to state-of-the-art (SoTA) methods. To the best of our knowledge, this is the first time to fuse synthesis-based and mapping-based methods to fully utilize their complementary advantages.
- We design an image synthesis module based on a swapping auto-encoder and hide the principal part of the secret message into a synthesis image to enlarge the payload capacity.
- We design an image mapping module based on block statistical hash matching to hide the secret residuals with a few selected container images to ensure the complete recovery of the secret message.

The remainder of this paper is organized as follows. Related work is discussed in Section II. In Section III, we explain our proposed SMH-SWE method in detail. Following it, Section IV presents the experimental results to demonstrate that the proposed SMH-SWE method outperforms the SoTA benchmarks. Finally, conclusions are drawn and future work is suggested in Section IV-E.

II. RELATED WORK

In the field of image steganography, methods can be classified based on their approach of data hiding into the carrier image. Traditional image steganography methods modify the carrier image by embedding data, whereas steganography without embedding methods explore alternative ways to achieve covert communication without directly modifying the carrier image.

A. TRADITIONAL EMBEDDING BASED IMAGE STEGANOGRAPHY METHODS

Traditional image steganography methods predominantly rely on the modification of pixels residing in texture-rich regions of the carrier images. These methods employ either handcrafted strategies [1], [2], [4], [5] or deep learning (DL)-based mechanisms [6], [7], [8], [9], [10] to enhance the undetectability of secret message embedding. Most of these methods are based on the spatial domain [1], [2], [3] or frequency domain [4], [5], and secret messages are embedded into the image.

1) HANDCRAFTED BASED METHODS

Van Schyndel et al. [21] design a method by replacing the least significant bits (LSBs) of pixel values in images with secret message bits. Wu and Tsai [2] divide gray-valued cover images into non-overlapping blocks and utilizing range-based difference values. Their embedding process achieves imperceptibility through sub-stream substitution for enhanced steganography. Luo et al. [3] expand the LSB matching revisited image steganography and propose an edge adaptive scheme to enhance the security. To achieve better resistance against steganalysis, Pevny et al. [22] minimize the weighted difference of feature vectors by designing high-dimensional models for data hiding, named HUGO. Atawneh et al. [5] propose a diamond encoding (DE)-based digital image wavelet-domain embedding scheme, which efficiently embeds a 5-bit numerical sequence into the carrier image while minimizing image distortion. Holub and Fridrich [23] select the texture-rich and noisy regions of images to embed messages, named S-UNIWARD, and then extend this strategy to arbitrary domains [24], named UNIWARD. Li et al. [25] use a high-pass filter with two low-pass filters to focus the embedding modification on the texture-rich area. Zhou et al. [26] design a distortion function to concentrate the embedding process towards the locations with significant distortion differences among different steganography methods, named controversial pixels prior. Qin et al. [27] models the image residuals obtained through high-pass filtering kernel processing as independent variables subject to multivariate Gaussian distribution, to further enhance the imperceptibility.

2) DEEP LEARNING BASED METHODS

Recently, deep learning-based image information hiding methods have been proposed to achieve acceptable

imperceptibility and minimal secret message extraction errors. Baluja [6] employ a full-size color image placed on another image of the same size. Tang et al. [7] utilize Generative Adversarial Networks (GANs) to identify optimal embedding regions at the pixel level, optimizing embedding quality and visual fidelity. Tang et al. [8] employ reinforcement learning and pixel-level operations to optimize embedding costs, enhancing undetectability in steganographic schemes. Li et al. [9] propose a novel image steganography scheme based on style transfer and quaternion exponential moments, improving resistance against steganalysis attacks. Lu et al. [28] deploy invertible neural networks (INN) to improve the steganography method in terms of the recovery quality with a large-capacity. To achieve higher steganography robustness, Zhu et al. [10] and Wengrowski and Dana [29] train DL-based models through imperceptible perturbations or using specialised datasets to encode useful information, to ensure accurate message recovery. Xu et al. [30] design a normalising flow to model the distribution for the recovery of secret images from attacked images.

B. STEGANOGRAPHY WITHOUT EMBEDDING METHODS

In recent years, a novel technique known as steganography without embedding (SWE) has garnered significant attention. This technique aims to avoid direct modifications to the container image, thus offering theoretical immunity against conventional steganalysis methods [11]. Instead of altering the carrier image itself, SWE methods involve the careful selection or generation of container images capable of inherently accommodating concealed messages. The current landscape of SWE methods can be broadly classified into two categories: synthesis-based [12], [13], [31] and mapping-based techniques [15], [16], [17].

1) SYNTHESIS-BASED METHODS

Synthesis-based methods leverage sophisticated deep synthesis techniques, such as generative adversarial networks (GANs) [18], [19], [20], to generate images with latent spaces that serve as carriers for the secret message. Hu et. al and Wang et al. [18], [32] train GANs together with an extractor network, to synthesise container images for concealed message transmission. To improve the quality of synthesis, Yu et. al [33] extend this work by introducing self-attention blocks while Li et al. [34] use Wasserstein loss with gradient penalty. Liu et al. [12] propose a carrier-free information hiding method using ACGAN to achieve good performance in terms of embedding capacity, distortion resilience, security, and reliability. To enhance the recovery quality, Peng et al. [35] recover the secret message by using an iterative vector updating strategy. You et al. [36] propose a method which trains the message hiding and recovery modules with JPEG compression to defend possible attacks in transmission channels.

These methods manipulate the parameters of the generative model to ensure that the desired hidden information is encoded within the generated images. However, a notable limitation of synthesis-based methods lies in the challenge of reliably recovering the complete secret message at the receiver's end, even in the absence of adversarial attacks.

2) MAPPING-BASED METHODS

Zhou et al. [11] compare the mean values of image blocks and binarise the compared results to generate an image hash for matching the secret message. To enhance the steganography robustness, Zheng et al. [37] employ the orientation of scale-invariant feature transform (SIFT) feature points as a stable image hash. To ensure that the candidate mapping images belong to the same topic, Zhang et al. [38] design a steganography method based on the latent Dirichlet allocation (LDA) classification mechanism and discrete cosine transform (DCT) features. To ensure the similarity of candidate images, Liu et al. [15] design a DenseNet-based retrieval mechanism and extract an image hash using a discrete wavelet transform (DWT). Liu et al. [39] propose an algorithm based on the DenseNet feature mapping method, utilizing deep learning to extract high-dimensional CNN features and map them into hash sequences. Luo et al. [16] introduce a coverless image steganography method based on multi-object recognition, utilizing Faster RCNN for object detection and a novel mapping rule for robust sequence generation,achieving improved robustness against geometric attacks. Zou et al. [17] present a method that focuses on the efficient construction of a coverless image dataset by extracting CNN-based deep hash and utilizing a specific mapping rule, thereby achieving higher dataset utilization and robustness.

This selection process relies on matching criteria between the secret message and the image hashes, facilitating an efficient mapping between the message and the chosen carriers. Nevertheless, mapping-based methods encounter an inherent limitation in terms of the payload capacity. The number of candidate images required for container selection grows exponentially with the secret message length. Consequently, even for relatively short secret messages, a substantial quantity of images must be employed for concealment, which may raise suspicion owing to the conspicuous behavior of transmitting an extensive array of images.

To summarize, while traditional embedding-based methods aim to enhance undetectability through modifications to carrier images, SWE techniques provide an alternative paradigm that circumvents such alterations. Synthesis-based methods focus on generating images intrinsically carrying the hidden messages, whereas mapping-based methods rely on judiciously selecting carriers from a pre-existing image set. However, both approaches possess inherent limitations, such as incomplete message recovery and restricted payload

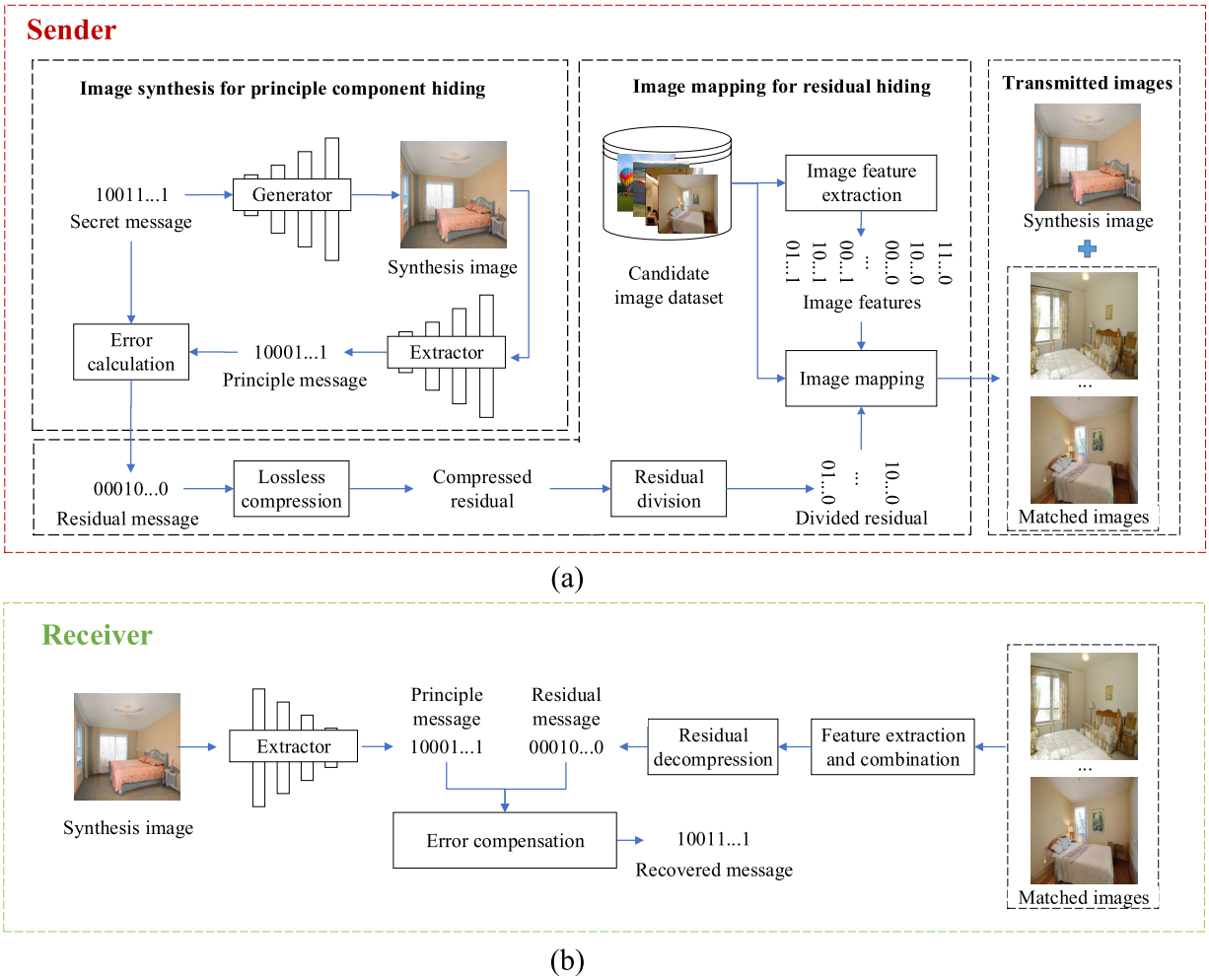

FIGURE 1. The framework of the proposed method:(a) secret message hiding phase in the sender (b) secret message extraction phase in the receiver.

capacity. Addressing these challenges represents an active research area within the realm of image steganography.

III. METHODS

As shown in Figure 1, our proposed SMH-SWE comprises a secret message hiding phase in the sender and an extraction phase in the receiver.

A. SECRET MESSAGE HIDING PHASE

The hiding phase consists of two stages, as depicted in Figure 1(a). The first stage employs an image synthesis module to conceal the principal component of the secret message. The second stage utilizes an image mapping module to hide the residual component of the secret message.

1) IMAGE SYNTHESIS MODULE

In the image synthesis module, an auto-encoder (AE) architecture is employed to hide the message by swapping the structural features within the synthesized image. This operation ensures that no image modification is introduced, thus fundamentally avoiding the risk of detection by steganalysis tools.

a: NETWORK ARCHITECTURES

Figure 2 illustrates our designed steganography AE, which includes encoder E, generator G, discriminative network D, co-occurrence discriminative network D_{CO}, distribution discriminator D_{DIST}, structure encoding generation network G_{STRU} and extraction network E_x. The encoder E and generator G are employed for texture swapping in the images. The discriminative network D and co-occurrence discriminative network D_{CO} supervise the image generation quality and the disentanglement of structure and texture encoding in the encoding and generation networks. The distribution discriminator D_{DIST} is utilized to train the texture encoding component of encoder E, ensuring that the generated texture encoding adheres to a specific explicit distribution. The structure encoding generation network G_{STRU} establishes a mapping from the secret tensor to structure encoding. Finally,

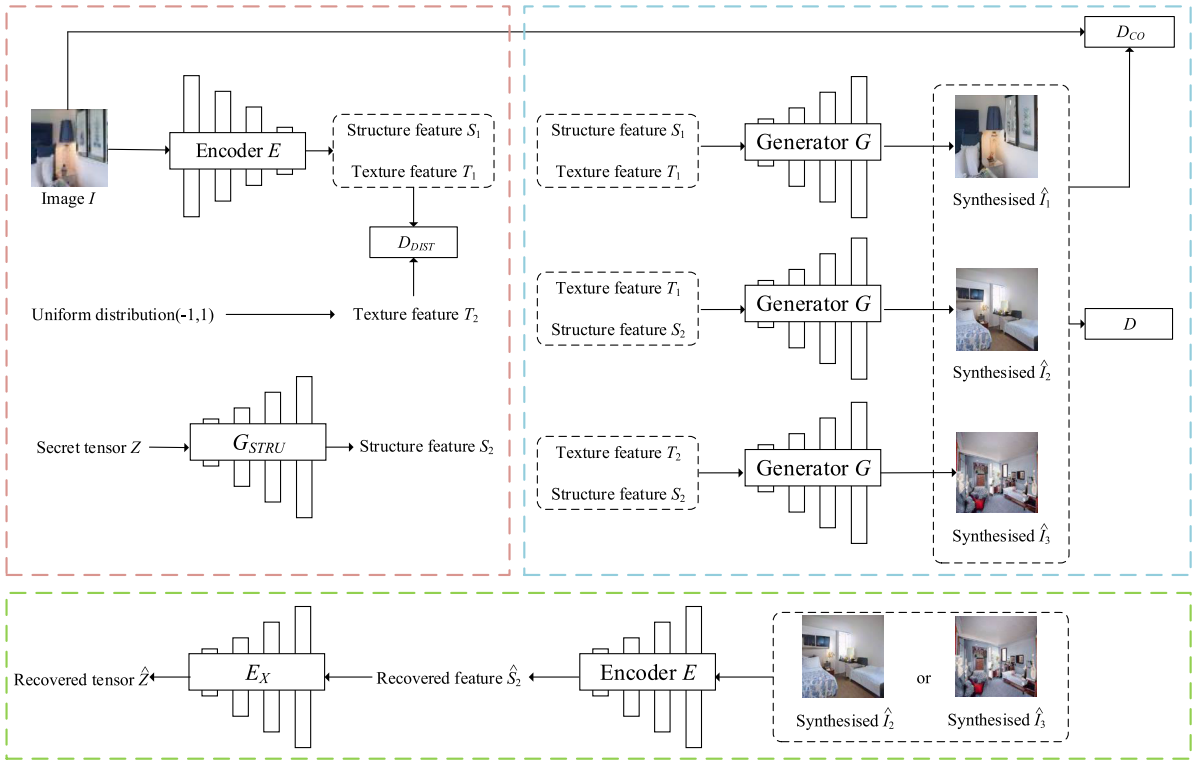

FIGURE 2. The image synthesis module of our proposed method.

the extraction network E_x extracts the secret tensor from the recovered structure feature.

The encoder *E* encodes input image I and produces both structure features S_1 and texture features T_1. Our proposed encoder applies 1×1 convolutions to expand the dimensions of the input image and then employs down-sampling residual convolution blocks four times. Subsequently, the encoder branches into two branches based on the different features: the structure feature branch focuses on encoding local features such as key-points and edges, requiring the neural network to capture the spatial relationships between neighboring pixels. Therefore, a fully convolutional structure is used to better encode the neighborhood information at each position in the feature map. In contrast, the texture feature branch encodes the global texture features of the input image and needs to be position-agnostic. To achieve this, a convolutional network with zero padding, combined with average pooling layers and fully connected layers, effectively encodes global texture features while masking positional information. For a 256×256 input image, an 8×16^2 feature map is produced as the structure feature, while a one-dimensional vector of length 2048 is generated as the texture feature. The network architecture of the encoder is illustrated in Figure 3.

The generator *G* has a similar structure to StyleGAN2 [40], which consists of multiple Style Residual Blocks (SRBs) and takes both the structure feature and

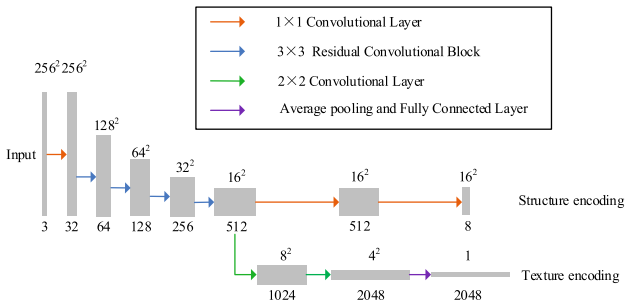

FIGURE 3. The network architecture of encoder.

texture feature as inputs to generate images. The generator utilizes the structure feature as the initial feature map and performs convolution and up-sampling using four style residual blocks and four up-sampling style residual blocks. During the convolution process, the generator feeds the texture feature into the modulation and demodulation layers of each style residual block to modulate the convolutional kernel weights, thereby controlling the global texture features of the generated images.

The discriminator network *D* and co-occurrence discriminator network D_{CO} together ensure the image generation quality and decoupling of the structure and texture encoding and decoding for the encoder and generator

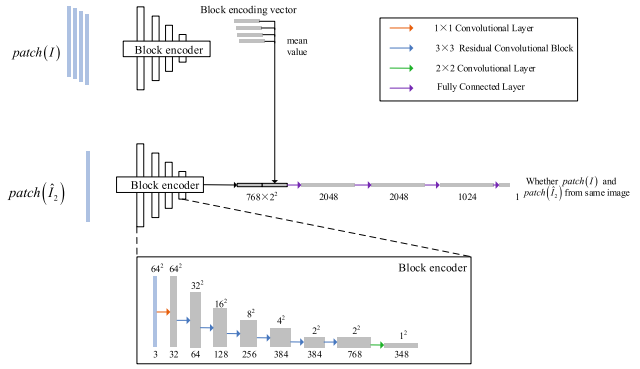

FIGURE 4. The structure of the co-occurrence discriminator network.

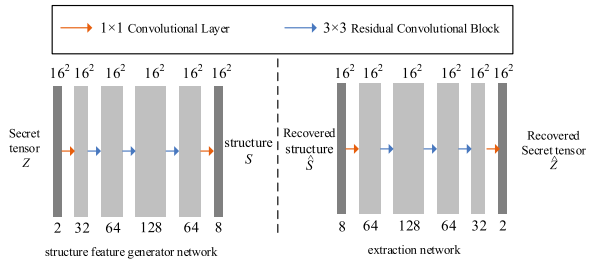

FIGURE 5. The network architecture of structure feature generator network and extraction network.

networks. Specifically, the discriminator network has a similar structure to that in [40], which distinguishes between generated images and real images to assist the generator network in generating images that closely resemble the real image distribution. while the structure of the co-occurrence discriminator network are illustrated in Figure 4. This network takes multiple randomly cropped reference image blocks from real images *patch* (I) and one randomly cropped image block from the generated images *patch* $\left(\hat{I}_2\right)$ as the input. As shown in Figure 4, the network first uses the same structure feature network to encode each image block and obtain their respective structure feature vectors. The mean value of the encoded reference image blocks is then taken as the reference encoding vector. The block of the generated image is then encoded as a target encoding vector. Finally, both the reference encoding vector and the target encoding vector are concatenated together and distinguished using a classification network.

The distribution discriminator network D_{DIST} is utilized to train the texture feature extraction part of the encoder network, which ensures that the generated texture features conform to a specific explicit distribution. In testing and practical applications, we can directly sample texture features from a specific distribution and combine them with the structure features to generate images. This distribution discriminator network is implemented based on a multi-layer perceptron (MLP) classification model.

The structure encoding generator network G_{STRU} establishes a mapping from the secret tensor to the structure feature, enabling the generation of structure feature. Simultaneously, it facilitates coverless image steganography by embedding secret information into the structure feature of an image. The architecture of the structure encoding generator network is illustrated in Figure 5.

The extraction network E_x is finally employed to extract the secret tensor. As the extraction network can be regarded as the inverse process of the structure feature generator network, its architecture is designed symmetrically. The specific network structure of the extraction network is illustrated in Figure 5.

b: LOSS FUNCTION

In our method, the total loss L_{total} to train the encoder E, generator G, structure encoding generator G_{STRU}, and extractor Ex is formulated as shown in Equation 1.

$$L_{total} = L_E + L_G + \alpha_{Ex} \times L_{Ex} \tag{1}$$

where α_{Ex} enables a balance between the synthesis quality and extraction accuracy. In our study, α_{Ex} is 15 to ensure the successful hiding of the principal component of the secret message.

The encoding loss L_E is obtained by combining the encoder distance loss $L_{E,dist}$ and encoder structure loss $L_{E,stru}$ as defined in Equation 2. Here, D_{DIST} is utilized to ensure that T_1 conforms to a uniform distribution $U(-1, 1)$. $L_{E,stru}$ is defined as $L_{E,stru} = \left|\hat{S}_2 - \hat{S}_1\right|^1$. $\hat{S}_i$ indicates the structure feature of the reconstructed image.

$$L_E = L_{E,dist} + L_{E,stru} \tag{2}$$

The generation loss L_G is formed by combining a reconstruction loss $L_{G,rec}$, a texture loss $L_{G,texture}$ and an adversarial loss $L_{G,real}$ because they work collaboratively for image synthesis. Specifically, L_G is defined in Equation 3, and the higher weight for $L_{G,real}$ guarantees the generation quality. $L_{G,rec}$ is calculated using $L1$ loss between the original image I and the reconstructed image $\hat{I}_1$. $L_{G,texture}$is calculated by generating $\hat{I}_2$ with the same texture feature as image I but different structure S_2, which is then passed along with randomly cropped patches of I and $\hat{I}_2$ to the co-occurrence discriminator D_{co}, from [41]. $L_{G,real}$ is introduced to make all synthesized images $\hat{I}_1$, $\hat{I}_2$ and $\hat{I}_3$ indiscriminative from real images, as shown in Equation 4.

$$L_G = L_{G,rec} + L_{G,texture} + 2 \times L_{G,real} \tag{3}$$

$$L_{G,real} = D\left(\hat{I}_1\right) + D\left(\hat{I}_2\right) + D\left(\hat{I}_3\right) \tag{4}$$

The tensor extracting loss, L_{Ex} is calculated by $L1$ loss as shown in Equation 5.

$$L_{Ex} = \left|\hat{Z} - Z\right|^1 \tag{5}$$

where $\hat{Z}$ represents the secret tensor extracted from E_x, Z represents the secret tensor.

c: HIDING PROCESS OF PRINCIPAL COMPONENT

Firstly, we map secret message M to secret tensor Z_M. Then, G_{STRU} is used to translate Z_M into structure feature S_M. Afterward, the texture feature T_M is generated with a uniform sampling from $U(-1, 1)$. Finally, we input the secret S_M and T_M into the pre-trained image generation network described above to generate an image containing hidden information. The following is a description of the information hiding with the image generation network process:

Step 1: Divide secret information M into L segments, each with a length of σ bits referring to Equation 6. In our study, σ is set to 512 according to the designed structure encoding generator network.

$$L = \frac{len}{\sigma} \tag{6}$$

where len is the length of secret information M.

Step 2: The decimal value m corresponding to each segment is mapped to a floating-point value z based on the following mapping rule as shown in Equation 7.

$$z = rand\left(\frac{m}{2^{\sigma-1}} - 1 + \delta, \frac{m+1}{2^{\sigma-1}} - 1 - \delta\right) \tag{7}$$

where, σ represents the length of the secret information after segmentation, m represents the decimal number corresponding to the binary secret information, δ represents the interval between subintervals and is set to 0.001 in our study. The function $rand(x, y)$ is used to calculate a random value of the interval [x, y], and z represents the floating-point value corresponding to the decimal number m after mapping. During the mapping process, a larger value of σ and leads to a greater hiding capacity of the model but a lower error tolerance, while a smaller value of σ leads to the opposite effect.

Step 3: Combine the floating-point values z that correspond to each segment of the secret information to form the secret tensor Z_M and generate a texture feature T_M by sampling from a uniform distribution.

Step 4: Obtain the structure feature S_M from secret tensor Z_M using the trained structure generator G_{STRU}.

Step 5: Use the image generator G, trained in Section III-A1a, with the structure feature S_M and texture feature T_M to generate an image I_M that contains secret information M.

Step 6: Calculate the residual message R_M by applying an Exclusive OR (XOR) function to the original secret information and its principal component P_M. This principal component is extracted from the synthesised image I_M using encoder E and extractor Ex together. Because our image synthesis module can successfully hide the principal component, most of the bit values of R_M are '0'.

2) IMAGE MAPPING MODULE

A mapping mechanism is proposed to conceal the inaccurately restored secret information (residual message) of our image synthesis module. The module consists of two main steps: residual processing and feature mapping based concealment.

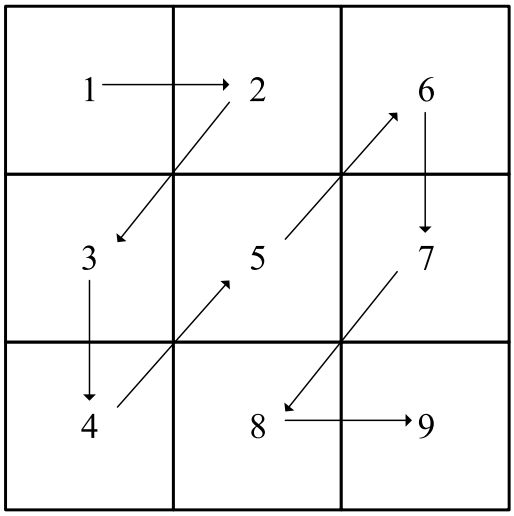

FIGURE 6. Divided blocks of an image with a Zig-Zag order.

a: RESIDUAL PROCESSING

In residual processing, the R_M is compressed using lossless compression, resulting in compressed residual secret information R_{CM}. Specifically, our lossless compression is first performed by the position coding of bit values '1' in the R_M. As a result, the information has a length of $k \times num\_bit$, in which k is the number of bit values '1' and the num_bit is defined as shown in Equation 8.

$$num\_bit = \log_2\sigma \tag{8}$$

where σ denotes the length of a segment of hidden message M. In this study, σ is set to 512. This information is then further compressed by Asymmetric Numeral Systems [42] to generate the R_{CM}. Finally, the R_{CM} is divided into non-overlapping compressed residual segments for feature mapping-based concealment. In our study, the length of the divided residual segments is 16 bits. Since the length of R_{CM} is significantly shorter than that of M because most of the bit values of R_M are '0', this approach effectively reduces the number of required container images.

b: FEATURE MAPPING BASED CONCEALMENT

In this section, image features are extracted by calculating the block statistical hashes. The feature extraction steps are described in detail below.

Step 1: Normalize all candidate images to a fixed size using nearest interpolation.

Step 2: Convert all the normalized images from RGB to the YUV color space, and use their Y components for feature extraction.

Step 3: Divide the normalized images into 3 × 3 non-overlapping blocks and label the 3 × 3 blocks in a Zig-Zag order as shown in Figure 6.

Step 4: Two statistics namely, the mean value and the variance, are calculated as follow:

$$\mu_k = \frac{1}{N_k} \sum_{i=1}^{N_k} P_k(i) \tag{9}$$

$$\delta_k = \frac{1}{N_k - 1} \sum_{i=1}^{N_k} (P_k(i) - \mu_k)^2 \tag{10}$$

where N_k is the number of pixels in the kth block, $k = 1, 2, \ldots, 9$, and $P_k(i)$ is the ith pixel in the kth block. The mean value reflects the energy concentration trend of each image block, whereas the variance can indicate the fluctuation of the pixel values of each block.

Step 5: Calculate the differences in the mean value and variance between adjacent blocks and binarize these differences by their median values in the equations below.

$$D_\mu(k) = \mu_{k+1} - \mu_k \tag{11}$$

$$D_\delta(k) = \delta_{k+1} - \delta_k \tag{12}$$

$$B_\mu(k) = \begin{cases} 1, & D_\mu(k) > T_\mu \\ 0, & D_\mu(k) \leq T_\mu \end{cases} \tag{13}$$

$$B_\delta(k) = \begin{cases} 1, & D_\delta(k) > T_\delta \\ 0, & D_\delta(k) \leq T_\delta \end{cases} \tag{14}$$

where $D_\mu(k)$ and $D_\delta(k)$ are the differences in the mean value and variance, $B_\mu(k)$ and $B_\delta(k)$ are their biniriased values; T_μ and T_δ are the median values of $D_\mu(k)$ and $D_\delta(k)$, and $k = 1, 2, \ldots, 8$.

Step 6: Combine the binarized differences of the mean value and the variance to generate the final feature.

Step 7: Select the suitable images of which the extracted features are equal to the compressed residual segments as the matched containers to further to hide the compressed residual secret information.

Step 8: Send matched images together with the image synthesised in Section III-A1 for conceal communication of a secret message.

B. SECRET MESSAGE EXTRACTION PHASE

At the receiver, the principal component of the secret message P_M is extracted from the synthesis image I_M while the residual message R_M is recovered from the other matched images, as illustrated in Figure 1(b).

First, encoder E and extractor Ex are jointly used to extract $\hat{S}_M$ and $\hat{Z}_M$ sequentially from I_M, and the inverse mapping function is applied to extract the principal component of the secret message P_M according to Equation 15.

$$\hat{m} = floor\left((z + 1) \times 2^{\sigma - 1}\right) \tag{15}$$

where σ represents the length of the secret information segment, z denotes the elements of the secret tensor, $floor()$ represents the floor function, and $\hat{m}$ represents the restored secret information segment. The image features are then extracted from the other matched images following the same steps 1-5 in feature mapping-based concealment. Feature extraction is repeated until all the compressed residual segments are extracted, and the extracted hashes are connected to form the compressed residual R_{CM}. Subsequently, the residual R_{CM} is decompressed to recover the residual message R_M. Finally, the complete secret message is recovered losslessly by performing an XOR operation on the extracted P_M and R_M.

IV. EXPERIMENTAL RESULTS

A. EXPERIMENTAL SETUP

To demonstrate the superiority of our proposed SMH-SWE, we compare it with six SoTA synthesis-based SWE methods, namely DCGAN-Steg [32], SAGAN-Steg [33], SSteGAN [18], WGAN-Steg [34], GDA-Steg [35], and CIS-Net [36] and six SoTA mapping-based SWE methods, namely MEAN [11], DCT [38], DWT [15], DenseNet [39], MOR [16] and CID [17].

Three publicly available datasets, including LSUN [43] Bedrooms, LSUN [43] Churches, FFHQ [44] and CelebA [45], are used to train the different image synthesis models. All images are resized to a resolution of 256 × 256 pixels. All the results are obtained on an RTX 3090 GPU.

B. EVALUATION OF THE TWO STAGES IN SMH-SWE

We evaluate the effects of our designed image synthesis and mapping modules in terms of extraction accuracy and the number of container images used. The detailed results are presented in Table 1.

It is apparent that the image synthesis and mapping modules have complementary performances. Our designed image synthesis module successfully hide the principal component of the secret message with an extraction accuracy near to 99.70% on the Bedrooms, Churches FFHQ and CelebA datasets, which ensures the effectiveness of the lossless compression of residuals (extraction errors). Moreover, the extraction accuracy of the compressed residuals by using our designed image mapping module is perfect (100.00%). By combining the image synthesis and mapping modules, the complete recovery (100.00%) of the secret message is further satisfied, which is usually considered as the most important aspect for conceal communications. For the number of required container images, the synthesis module requires just one generated image. In contrast, the mapping module needs three additional matched images to guarantee a 100.00% recovery of the secret message's residual, which is still acceptable for real applications.

C. COMPARISON WITH SYNTHESIS-BASED SWE

First, we compare the extraction accuracy results with the corresponding hidden capacities in Table 2. It is evident that only our designed SMH-SWE can achieve 100.00%

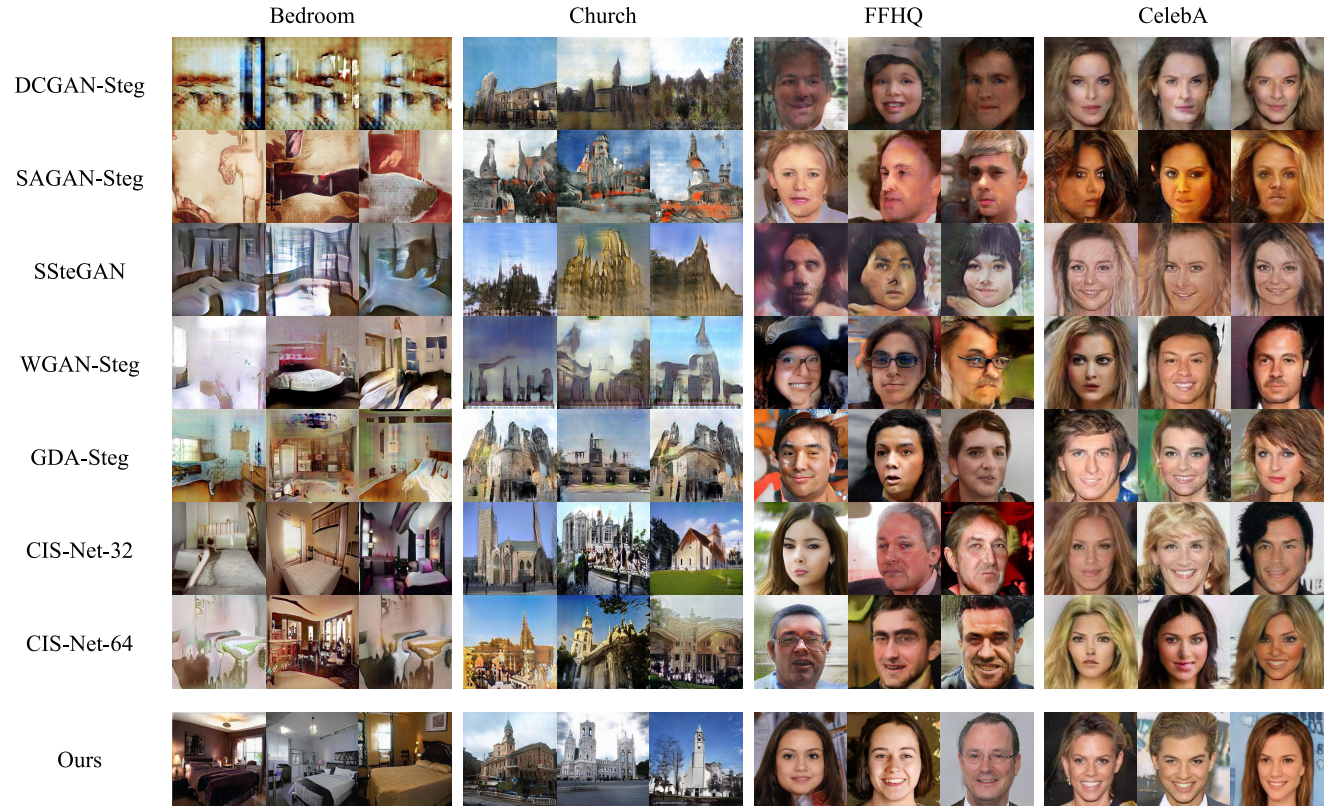

FIGURE 7. The container images synthesised using different messages by different synthesis-based SWE methods.

TABLE 1. Evaluation of the effects of designed image synthesis and mapping modules in terms of extraction accuracy.

Modules	Secret message				Compressed residual	Number of container images for hiding 512 bits
	Bedrooms	Churches	FFHQ	CelebA		
Synthesis Module	99.68%	99.72%	99.77%	99.75%	N.A.	1
Mapping Module	N.A.	N.A.	N.A.	N.A.	100%	3
Ours	100%	100%	100%	100%	100%	4

TABLE 2. Extraction accuracy results for different synthesis-based SWE methods.

Methods	Bedrooms	Churches	FFHQ	CelebA	Capacity(bit / bpp)
DCGAN-Steg	94.01%	94.56%	96.29%	97.09%	$100 / 1.53 \times 10^{-3}$
SAGAN-Steg	96.77%	95.86%	97.12%	96.19%	$200 / 3.05 \times 10^{-3}$
SSteGAN	98.41%	97.53%	97.23%	99.38%	$100 / 1.53 \times 10^{-3}$
WGAN-Steg	92.23%	90.04%	92.85%	91.17%	$100 / 1.53 \times 10^{-3}$
GDA-Steg	57.03%	61.33%	98.83%	96.51%	$256 / 3.91 \times 10^{-3}$
CIS-Net-32	99.90%	99.96%	99.92%	99.97%	$32 / 4.88 \times 10^{-4}$
CIS-Net-64	65.84%	77.75%	86.43%	89.70%	$64 / 9.77 \times 10^{-4}$
Ours	100%	100%	100%	100%	$128 / 1.95 \times 10^{-3}$

extraction accuracy in all three tested datasets with comparable hidden capacity which outperforms the other benchmark methods. This remarkable performance is attributed to our unique combination of image synthesis and image mapping modules, which aims to hide the principal component of the secret message and the other hides the residual values.

We then test the container images by using different SWE methods in terms of the resistance against steganalysis tools by using three well-known steganalysis tools including StegExpose [46], XuNet [47], YeNet [48] and SRNet [49]. The area under the curve (AUC) values of receiver operating characteristic (ROC) curves are presented in Table 3. It is

FIGURE 8. The images synthesised using the same message by different synthesis-based SWE methods.

TABLE 3. Steganalysis results for different synthesis-based SWE methods (in terms of AUC of ROC).

Methods	StegExpose	XuNet	YeNet	SRNet
DCGAN-Steg	0.586	0.568	0.573	0.591
SAGAN-Steg	0.578	0.500	0.569	0.540
SSteGAN	0.417	0.491	0.519	0.495
WGAN-Steg	0.594	0.542	0.548	0.569
GDA-Steg	0.626	0.539	0.521	0.574
CIS-Net-32	0.601	0.466	0.507	0.538
CIS-Net-64	0.623	0.435	0.502	0.512
Ours	0.496	0.476	0.510	0.498

TABLE 4. Container image quality results for different synthesis-based SWE models in terms of FID scores.

Methods	Bedrooms	Churches	FFHQ	CelebA	Average
DCGAN-Steg	283.32	105.79	74.24	109.43	143.20
SAGAN-Steg	159.51	99.59	82.60	76.78	104.62
SSteGAN	153.48	258.80	150.37	97.17	164.96
WGAN-Steg	147.45	181.20	67.95	50.19	111.70
GDA-Steg	73.55	148.28	81.86	48.01	87.93
CIS-Net-32	54.32	31.24	42.10	33.10	40.19
CIS-Net-64	152.01	26.53	44.34	37.53	65.10
Ours	13.69 (4.51)	16.48 (5.05)	28.59 (8.78)	17.82 (5.48)	19.15 (5.96)

evident that the AUC values of different SWE methods are close to 0.5, indicating that the steganalysis tools are similar to random guessing. These results demonstrate that SWE methods are immune to the detection of current steganalysis tools since secret messages are hidden without introducing any image modification.

TABLE 5. Comparison with different mapping-based SWE methods.

Methods	Hidden capacity(bit / bpp)	Candidate number	Container number (0.5K)	Container number (1K)	Container number (2K)
MEAN	$8 / 1.22 \times 10^{-4}$	2^8	64	128	256
DCT	$15 / 2.29 \times 10^{-4}$	2^{15}	35	69	137
DWT	$15 / 2.29 \times 10^{-4}$	2^{15}	35	69	137
DenseNet	$8 / 1.22 \times 10^{-4}$	2^8	64	128	256
MOR	$24 / 3.66 \times 10^{-4}$	2^6	22	43	86
CID	$16 / 2.44 \times 10^{-4}$	2^{16}	32	64	128
Ours	$128 / 1.95 \times 10^{-3}$	2^{16}	4	8	16

Further, we compare the synthesis fidelity of the synthesised images by testing their authenticity and diversity, which indicates their imperceptibility to visual inspection. In this experiment, a widely employed synthesis fidelity metric, the Fréchet inception distance (FID), is used to evaluate the synthesis fidelity, and the results are listed in Table 4. For SMH-SWE, it is noted that the values outside the brackets are the FID values of the synthesised images while the values in the brackets are the average FID values of the synthesised images and matched mapping images. As shown in Table 4, our SMH-SWE achieves the best FID scores on all four datasets, which outperforms all other methods by a wide margin. The reason for the remarkable fidelity lies in twofold: the disentangled structure feature guarantees high synthesis authenticity, while the uniformly sampled texture vectors enhance synthesis diversity.

Finally, examples of synthesised images of different models are shown in Figures 7 and 8 for subjective evaluation.

TABLE 6. Qualitative comparison.

Methods	Hidden capacity	Candidate number	Container number	Container quality	Complete recovery	Immune to steganalysis tools	Robustness
Embedding based method	High	N.A.	One	Acceptable	Yes	**Not Fundamentally**	No
Synthesis-based method	Acceptable	N.A.	One	Acceptable	**No**	Fundamentally	No
Mapping-based method	**Low**	Acceptable	**Large**	Perfect	Yes	Fundamentally	Yes
Ours	Acceptable	Acceptable	A few	High	Yes	Fundamentally	No

As shown in Figure 7, the quality of the images synthesised by our method is much higher, with more realistic structures and clearer textures. Moreover, as shown in Figure 8, our method achieves more diversified styles because of the uniformly sampled texture vectors when hiding identical secret messages.

D. COMPARISON WITH MAPPING-BASED SWE

In this section, we compare our proposed method with SoTA mapping-based SWE for different aspects in Table 5. As is apparent from this, our proposed method significantly outperforms the other methods in terms of the hidden capacity and number of container images when hiding secret messages with different lengths,meanwhile, it requires an acceptable number of candidate images. This result demonstrates that our method is much more suitable for real world applications because the unusual behavior of extensive image sending significantly increases the risk of suspicion. The reason for this is that in our methods, the mapping images are only used to hide the compressed residual message, which is significantly shorter than the original message, while the principle message is hidden by a synthesised image.

E. DISCUSSION AND LIMITATION

Finally, we qualitatively compare our proposed SMH-SWE with other methods in terms of seven metrics: i) the hidden capacity, ii) the required number of candidate images, iii) the required number of container images, iv) the quality of the container, v) the complete recovery of the secret message, vi) the resistance against steganalysis and vii) the robustness against image attack, as shown in Table 6. Based on these aspects, the proposed scheme addresses the core challenges (shown in bold) of the other approaches and thus achieves the superior performances.

Compared with embedding-based methods, our proposed SMH-SWE is fundamentally immune to typical steganalysis tools due to its modification-free hiding process.

Compared with synthesis-based SWE methods, our proposed SMH-SWE achieves completed recovery of the secret message, which is considered as one of the most core requirements for steganography since the secret message is usually considered as extremely valuable. In addition, the quality of container images is also higher than that of current synthesis-based SWE methods as discussed in Section IV-C.

Compared with mapping-based SWE methods, our proposed SMH-SWE method requires only a few matched container images to hide the compressed residual message while deploying a high quality synthesis image to hide the principal message. Therefore, our method avoids using large number of images for conceal communication and thus reduces the suspicion risks owing to the unusual behavior of extensive image sending, which is also very important for real-world applications.

Although the proposed SMH-SWE achieves significantly superior performance compared to the state-of-the-art SWE methods by fusing the synthesis-based and mapping-based methods to fully make use of their complementary advantages, our method still has some limitations to be further addressed. Firstly, our hidden capacity is still lower than that of embedding based methods. In addition, the recovery robustness of our method also needs to be improved. Specifically, it is unable to recover the principal message from synthesised images tampered by compression [50], [51], blurring, or image sterilization [52], [53]. We attribute this result to the fact that some components sensitive to high-frequency feature changes are encoded in structure features.

V. CONCLUSION

In this paper, we have proposed SMH-SWE, a novel two-stage hybrid framework that seamlessly combines an image synthesis module and an image mapping module. By designing the image synthesis module based on a disentanglement auto-encoder, the principal component of the secret message is hidden in the structure feature of a high fidelity synthesis image with FID lower than 20.00, which significantly reduces the number of container images required by current mapping based SWE. For example, the current mapping based SWE methods need more than 22 container images while our proposed method needs only 4 images when hiding 512 bits. In addition, by combining the image mapping module, the extraction error from the synthesis module are hidden by matching a few additional container images, which solves the challenge faced by current synthesis based SWE, i.e, the 100% recovery rate of the secret message. The limitations of our method are twofold: (i) the hidden capacity is still lower than that of embedding based method, (ii) and the robustness against image compression, blurring and sterilizations. Therefore, we aim to expand the hidden capacity and boost the robustness of our proposed SWE by incorporating concepts of full-image-to-image hiding and adversarial learning for future work.

REFERENCES

[1] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar. 2006.

[2] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognit. Lett.*, vol. 24, nos. 9–10, pp. 1613–1626, Jun. 2003.

[3] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on LSB matching revisited," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 201–214, Jun. 2010.

[4] F. Huang, X. Qu, H. J. Kim, and J. Huang, "Reversible data hiding in JPEG images," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 26, no. 9, pp. 1610–1621, Sep. 2016.

[5] S. Atawneh, A. Almomani, H. Al Bazar, P. Sumari, and B. Gupta, "Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain," *Multimedia Tools Appl.*, vol. 76, no. 18, pp. 18451–18472, Sep. 2017.

[6] S. Baluja, "Hiding images in plain sight: Deep steganography," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 30, 2017, pp. 1–11.

[7] W. Tang, S. Tan, B. Li, and J. Huang, "Automatic steganographic distortion learning using a generative adversarial network," *IEEE Signal Process. Lett.*, vol. 24, no. 10, pp. 1547–1551, Oct. 2017.

[8] W. Tang, B. Li, M. Barni, J. Li, and J. Huang, "An automatic cost learning framework for image steganography using deep reinforcement learning," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 952–967, 2021.

[9] Q. Li, X. Wang, B. Ma, X. Wang, C. Wang, Z. Xia, and Y. Shi, "Image steganography based on style transfer and quaternion exponent moments," *Appl. Soft Comput.*, vol. 110, Oct. 2021, Art. no. 107618.

[10] J. Zhu, R. Kaplan, J. Johnson, and L. Fei-Fei, "HiDDeN: Hiding data with deep networks," in *Proc. Eur. Conf. Comput. Vis.*, 2018, pp. 657–672.

[11] Z. Zhou, H. Sun, R. Harit, X. Chen, and X. Sun, "Coverless image steganography without embedding," in *Proc. Int. Conf. Cloud Comput. Secur.*, 2015, pp. 123–132.

[12] M.-M. Liu, M.-Q. Zhang, J. Liu, Y.-N. Zhang, and Y. Ke, "Coverless information hiding based on generative adversarial networks," 2017, *arXiv:1712.06951*.

[13] Y. Cao, Z. Zhou, Q. M. J. Wu, C. Yuan, and X. Sun, "Coverless information hiding based on the generation of anime characters," *EURASIP J. Image Video Process.*, vol. 2020, no. 1, pp. 1–15, Dec. 2020.

[14] X. Liu, Z. Ma, J. Ma, J. Zhang, G. Schaefer, and H. Fang, "Image disentanglement autoencoder for steganography without embedding," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2022, pp. 2293–2302.

[15] Q. Liu, X. Xiang, J. Qin, Y. Tan, J. Tan, and Y. Luo, "Coverless steganography based on image retrieval of DenseNet features and DWT sequence mapping," *Knowl.-Based Syst.*, vol. 192, Mar. 2020, Art. no. 105375.

[16] Y. Luo, J. Qin, X. Xiang, and Y. Tan, "Coverless image steganography based on multi-object recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 31, no. 7, pp. 2779–2791, Jul. 2021.

[17] L. Zou, J. Li, W. Wan, Q. M. J. Wu, and J. Sun, "Robust coverless image steganography based on neglected coverless image dataset construction," *IEEE Trans. Multimedia*, early access, Jul. 29, 2022, doi: 10.1109/TMM.2022.3194990.

[18] Z. Wang, N. Gao, X. Wang, X. Qu, and L. Li, "SSteGAN: Self-learning steganography based on generative adversarial networks," in *Proc. Int. Conf. Neural Inf. Process.*, 2018, pp. 253–264.

[19] P. L. Suárez, A. D. Sappa, and B. X. Vintimilla, "Infrared image colorization based on a triplet DCGAN architecture," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jul. 2017, pp. 212–217.

[20] A. Odena, C. Olah, and J. Shlens, "Conditional image synthesis with auxiliary classifier gans," in *Proc. Int. Conf. Mach. Learn.*, 2017, pp. 2642–2651.

[21] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in *Proc. 1st Int. Conf. Image Process.*, 1994, pp. 86–90.

[22] T. Pevny, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *Proc. Int. Workshop Inf. Hiding*, 2010, pp. 161–177.

[23] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Dec. 2012, pp. 234–239.

[24] V. Holub, J. Fridrich, and T. Denemark, "Universal distortion function for steganography in an arbitrary domain," *EURASIP J. Inf. Secur.*, vol. 2014, no. 1, pp. 1–13, Dec. 2014.

[25] B. Li, M. Wang, J. Huang, and X. Li, "A new cost function for spatial image steganography," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Oct. 2014, pp. 4206–4210.

[26] W. Zhou, W. Zhang, and N. Yu, "A new rule for cost reassignment in adaptive steganography," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2654–2667, Nov. 2017.

[27] X. Qin, B. Li, and J. Huang, "A new spatial steganographic scheme by modeling image residuals with multivariate Gaussian model," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2019, pp. 2617–2621.

[28] S.-P. Lu, R. Wang, T. Zhong, and P. L. Rosin, "Large-capacity image steganography based on invertible neural networks," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2021, pp. 10811–10820.

[29] E. Wengrowski and K. Dana, "Light field messaging with deep photographic steganography," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2019, pp. 1515–1524.

[30] Y. Xu, C. Mou, Y. Hu, J. Xie, and J. Zhang, "Robust invertible image steganography," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2022, pp. 7865–7874.

[31] Q. Li, X. Wang, X. Wang, B. Ma, C. Wang, and Y. Shi, "An encrypted coverless information hiding method based on generative models," *Inf. Sci.*, vol. 553, pp. 19–30, 2021.

[32] 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. 38303–38314, 2018.

[33] C. Yu, D. Hu, S. Zheng, W. Jiang, M. Li, and Z.-Q. Zhao, "An improved steganography without embedding based on attention GAN," *Peer-Peer Netw. Appl.*, vol. 14, no. 3, pp. 1446–1457, May 2021.

[34] J. Li, K. Niu, L. Liao, L. Wang, J. Liu, Y. Lei, and M. Zhang, "A generative steganography method based on WGAN-GP," in *Proc. Int. Conf. Artif. Intell. Secur.*, 2020, pp. 386–397.

[35] F. Peng, G. Chen, and M. Long, "A robust coverless steganography based on generative adversarial networks and gradient descent approximation," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 32, no. 9, pp. 5817–5829, Sep. 2022.

[36] Z. You, Q. Ying, S. Li, Z. Qian, and X. Zhang, "Image generation network for covert transmission in online social network," in *Proc. 30th ACM Int. Conf. Multimedia*, Oct. 2022, pp. 2834–2842.

[37] S. Zheng, L. Wang, B. Ling, and D. Hu, "Coverless information hiding based on robust image hashing," in *Proc. Int. Conf. Intell. Comput.*, 2017, pp. 536–547.

[38] X. Zhang, F. Peng, and M. Long, "Robust coverless image steganography based on DCT and LDA topic classification," *IEEE Trans. Multimedia*, vol. 20, no. 12, pp. 3223–3238, Dec. 2018.

[39] Q. Liu, X. Xiang, J. Qin, Y. Tan, and Y. Qiu, "Coverless image steganography based on DenseNet feature mapping," *EURASIP J. Image Video Process.*, vol. 2020, no. 1, pp. 1–18, Dec. 2020.

[40] T. Karras, S. Laine, M. Aittala, J. Hellsten, J. Lehtinen, and T. Aila, "Analyzing and improving the image quality of StyleGAN," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2020, pp. 8107–8116.

[41] T. Park, J.-Y. Zhu, O. Wang, J. Lu, E. Shechtman, A. Efros, and R. Zhang, "Swapping autoencoder for deep image manipulation," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 33, 2020, pp. 7198–7211.

[42] J. Duda, "Asymmetric numeral systems: Entropy coding combining speed of Huffman coding with compression rate of arithmetic coding," 2013, *arXiv:1311.2540*.

[43] F. Yu, A. Seff, Y. Zhang, S. Song, T. Funkhouser, and J. Xiao, "LSUN: Construction of a large-scale image dataset using deep learning with humans in the loop," 2015, *arXiv:1506.03365*.

[44] T. Karras, S. Laine, and T. Aila, "A style-based generator architecture for generative adversarial networks," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2019, pp. 4396–4405.

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

[46] B. Boehm, "StegExpose—A tool for detecting LSB steganography," 2014, *arXiv:1410.6656*.

[47] G. Xu, H.-Z. Wu, and Y.-Q. Shi, "Structural design of convolutional neural networks for steganalysis," *IEEE Signal Process. Lett.*, vol. 23, no. 5, pp. 708–712, May 2016.

[48] J. Ye, J. Ni, and Y. Yi, "Deep learning hierarchical representations for image steganalysis," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2545–2557, Nov. 2017.
[49] M. Boroumand, M. Chen, and J. Fridrich, "Deep residual network for steganalysis of digital images," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 5, pp. 1181–1193, May 2019.
[50] W. B. Pennebaker and J. L. Mitchell, *JPEG: Still Image Data Compression Standard*. Berlin, Germany: Springer, 1992.
[51] M. W. Marcellin, M. J. Gormish, A. Bilgin, and M. P. Boliek, "An overview of JPEG-2000," in *Proc. DCC. Data Compress. Conf.*, 2000, pp. 523–541.
[52] G. Paul and I. Mukherjee, "Image sterilization to prevent LSB-based steganographic transmission," 2010, *arXiv:1012.5573*.
[53] H. Liu, T. Xiang, S. Guo, H. Li, T. Zhang, and X. Liao, "Erase and repair: An efficient box-free removal attack on high-capacity deep hiding," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 5229–5242, 2023.

RONG HUANG received the B.S. degree in communication engineering from Xiangtan University, in 2004, and the M.S. degree in computer science and technology from Hunan University, in 2014. Since 2018, she has been an Assistant Professor with the Hunan Vocational College of Science and Technology. Her current research interests include natural language processing, big data, and machine learning.

CHUNYAN LIAN received the B.S. and M.S. degrees in computer science and technology from Central South University, in 2015 and 2018, respectively. She is currently a Teaching Assistant with the Hunan Vocational College of Science and Technology. Her current research interests include information security, deep learning, and computer vision.

ZHEN DAI received the B.S. degree in computer technology from Xiangtan University, in 2002, and the M.S. degree in software engineering from Central South University, in 2010. She is currently a Professor with the Hunan Vocational College of Science and Technology. Her current research interests include information security, deep learning, and data mining.

ZHAOYING LI received the B.S. degree in computer science and technology from Hunan First Normal University, in 2017, and the M.S. degree in computer technology from Central South University, in 2022. She is currently a Teaching Assistant with the Chenzhou Comprehensive Vocational Secondary School. Her current research interests include information security, deep learning, and computer vision.

ZIPING MA received the B.E. degree from Central South University, in 2021. His current research interests include image synthesis, steganography, and deep learning.