Joint Coverless Steganography and Image Transformation for Covert Communication of Secret Messages

Wenying Wen, *Member, IEEE*, Haigang Huang, Shuren Qi, Yushu Zhang, *Senior Member, IEEE*, and Yuming Fang, *Senior Member, IEEE*

***Abstract*—With the rapid development of internet applications, privacy protection of secret messages in covert communication has become increasingly important. To address the issue of attacks received in covert communication, such as eavesdropping attacks, steganalysis attacks, and tempering attacks, we propose a novel scheme that combines coverless steganography and image transformation for the covert communication of secret messages. Instead of using an image as the carrier to embed secret messages, our coverless steganography approach hides secret messages by exploiting a generative network to take it and a latent as input to synthesize a stego image, thus essentially avoiding both eavesdropping and typical steganalysis attacks. Furthermore, the generated pseudorealistic stego image with distortion vulnerabilities leads to tampering, which ultimately results in the receiver not being able to correctly extract secret information. In response to this problem, we design an image transformation method, which converts the stego image into another realistic image (i.e., camouflage image) and thus provides ambiguity for spoofing attackers while preventing stego images from being tampered with. Additionally, the authentication information is embedded into the camouflage image to obtain the transmitted authentication image (AuI) and can be used by the receiver to validate the completeness and authenticity of the camouflage image. Compared with related steganography methods in recent years, our proposed scheme synthesizes more high-quality stego images, and the stego image can be restored losslessly from the camouflage image. Most importantly, the PSNR of the camouflage image with authentication information (i.e., AuI) is 31.78, which is enough to deceive the attacker; moreover, the secret message extraction rate can reach 100%.**

***Index Terms*—Ambiguity, coverless steganography, covert communication, image transformation.**

Manuscript received 5 September 2023; revised 12 December 2023; accepted 13 January 2024. Date of publication 16 January 2024; date of current version 30 April 2024. This work was supported in part by the Natural Science Foundation of China under Grants 62201233 and 61961022, in part by the Double Thousand Plan of Jiangxi Province under Grant jxsq2023201118, in part by the Outstanding Youth Fund Program of Jiangxi Province under Grant 20232ACB212004, in part by the Natural Science Foundation of Jiangxi Province under Grants 20224BAB212012 and 20224BAB211002. Recommended for acceptance by Dr. Chau Yuen. *(Corresponding author: Yushu Zhang.)*

Wenying Wen, Haigang Huang, and Yuming Fang are with the School of Information Technology, Jiangxi University of Finance and Economics, Nanchang 330013, China (e-mail: wenyingwen@sina.cn; seahg1031@163.com; leo.fangyuming@foxmail.com).

Shuren Qi and Yushu Zhang are with the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China (e-mail: shurenqi@nuaa.edu.cn; yushu@nuaa.edu.cn).

Digital Object Identifier 10.1109/TNSE.2024.3354941

I. Introduction

COVERT communication is a communication method that avoids surveillance by hiding communication content, and it has been widely used in military, intelligence operations, and online social networks to coordinate protest activities or to ensure user privacy [1]. The parties in this mode of communication can hide information through embedded covert channels or can confuse information by using encryption technology. To achieve covert communication, multiple technologies may be applied, including information hiding, digital watermarking, and encryption [2]. Due to traditional communication methods, being easily monitored and attacked; covert communication has become an important means of secure communication. However, with the constant growth of network technology, existing covert communication technologies are also facing increasingly severe challenges, such as eavesdropping attacks, steganalysis attacks, and tampering attacks in Fig. 1.

As described in Fig. 1(a), hackers engage in attacks by eavesdropping on communication lines or network traffic to obtain communication content. If text secret information is not encrypted and protected during transmission, attackers can easily obtain its content, leading to secret information leakage. Thus, the first matter is how to transmit confidential information invisibly in covert communication. Specifically, steganography [22] is an effective way to protect messages during data communication transmission. The entire process of image steganography can be depicted as follows: the sender acquires the stego image by using a cover image as a medium to embed secret messages and then distributes it to the receiver. The attackers do not illegally discover the presence of the secret message even if these stego images are intercepted during transmission [3]. Some traditional steganography technologies [23], [24], [25], [26], [27], [28] embed secret information into a carrier, realizing the invisibility of secret information in covert communication. However, the embedding-based technologies enable the secret messages carried to have an inherent risk of being corrupted by using the steganalysis tools.

To resist steganalysis as shown in Fig. 1(b), the second critical issue is to improve the undetectability of stego images after hiding secret messages. Coverless steganography [4] is a burgeoning concept that can hide secret messages by synthesizing them into image form. Therefore, it has the unique advantage of

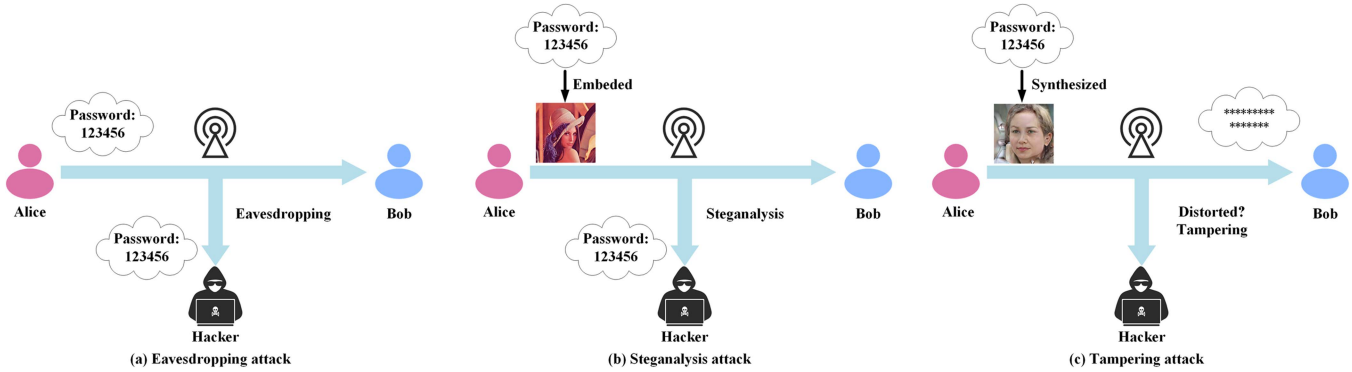

Fig. 1. Three types of attacks in covert communication.

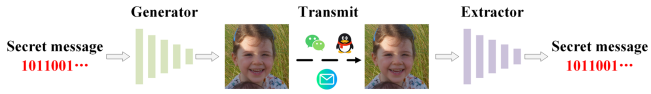

Fig. 2. Schematic diagram of generation-based steganography.

being immune to typical steganalysis tools [29]. As illustrated in Fig. 2, generation-based coverless steganography methods aim to generate stego images directly from secret messages instead of embedding them by altering the cover image. Under this premise, some schemes [5], [6], [7], [8] can synthesize special image types such as texture images and fingerprint images. To make the secret information transmitted more secure and not suspected, generative adversarial networks (GANs) [40] can be used to compose realistic images. The stego image can be obtained by learning textured objects [9] or noise vectors [10] of GANs according to the prebuilt mapping mechanism. In this way, the method [15] can synthesize stego images that are very similar to real images. Nevertheless, abovementioned schemes [5], [6], [7], [8] can synthesize only some special image types, while GAN-based coverless steganography methods can synthesize relatively more realistic stego images. However, all these stego images exhibit significant distortion to some extent, which makes it difficult to deceive attackers with them.

The third problem that must be considered is that low-quality stego images are susceptible to tampering by attackers. As shown in Fig. 1(c), tampering attacks on stego images can lead to damage or unavailability of image files, directly affecting the extraction and recovery of secret information. In response to this issue, image ambiguity is a common means to ensure the security of transmitted images. Image transformation, which is a type of image ambiguity method, was first proposed by Lai et al. [31]. Inspired by GAN-based techniques, some deep learning-based image transformation methods [21], [22], [23], [24] have been developed to transform the original image into a reference image with faster speed and lower computational complexity. Although these methods have better advantages in image quality and visual effect, the original image cannot be completely recovered from the reference image. With the transformation methods (e.g., [33], [34]), the sender can convert the secret image into another image based on the reference image to prevent leakage of protected information [32] and can restore the secret image without any loss. Although the secret image has been changed, the licensor can obtain it by using the correct key, while unauthorized people can only see the transformed image. However, on the receiving end, these methods provide no means to verify the authenticity and the integrity of the transformed image.

Thus, when Alice shares a secret message with her friend Bob in covert communication, there are always three attributes to protect privacy that must be considered: invisibility, undetectability, and ambiguity.

Invisibility: To prevent hackers from directly obtaining secret information through eavesdropping, the invisibility of secret messages is necessary.

Undetectability: Due to the cover-based steganography method making stego images vulnerable to attacks from recent steganalysis tools, we strive to improve the undetectability of stego images to withstand steganalysis.

Ambiguity: The quality of stego images obtained based on cover steganography methods is relatively low, with obvious distortions, leading hackers to suspect and to tamper with these images. To address this issue, a means of ambiguity should be provided to improve the composite quality of stego images, thereby mitigating the suspicion of attackers.

For the sake of meeting three characteristics of privacy protection in covert communication, we proposes a scheme that joins coverless steganography and image transformation for the covert communication of secret messages, and Fig. 3 is an example that illustrates this case. To disguise secret messages and to resist steganalysis, we design an image generator that can freely compose relatively realistic stego images based on the input information. In addition, to protect the stego image from tempering attacks during transmission, we obscure the stego image and transform it into another image (i.e., camouflage image) that can be any style. Additionally, through a reversible data hiding method, the authentication information is embedded into the camouflage image to derive the transmitted authentication image, which can be used by the receiver to validate the completeness and authenticity of the camouflage image. In this way, the more realistic authentication image can deceive the hacker, or even if the hacker illegally obtains the authentication image and secret extractor. It is extremely difficult to know that the real stego image has been transformed without having access to any

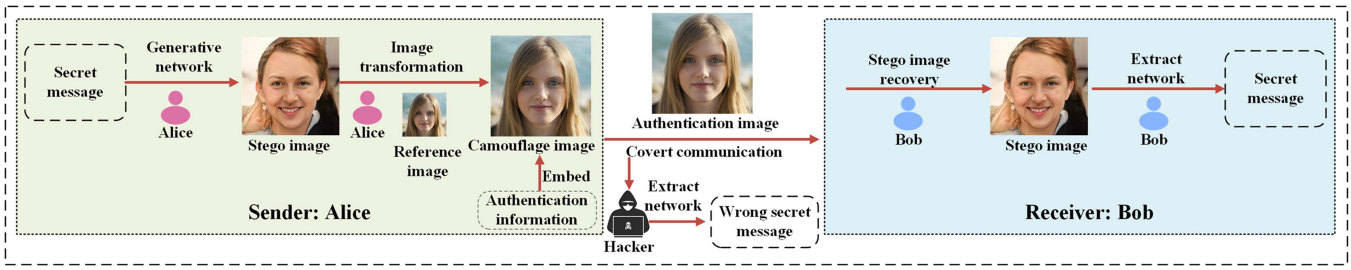

Fig. 3. **Sender:** the secret message is used to generate stego image and then Alice obscure the stego image into the form of reference image. **Receiver:** when Bob receives authentication image from Alice, he can reverse it back to the stego image using reversible image transformation algorithm according to the authentication information and then inputs it to extract network to obtain the secret message. **Hacker:** a wrong secret message is extracted from the authentication image.

other information, since the hacker can extract secret messages through the authentication image–regardless of whether it is correct or not. Our major contributions are summarized below.

- Instead of using an image as the carrier to embed secret messages, we propose a coverless steganography network that achieves the invisibility and undetectability of secret messages by synthesizing it into a stego image. Thus, typical eavesdropping and steganalysis attacks are blocked.
- We design an image transformation method to provide ambiguity by converting stego images into other more realistic camouflage images. The integrity and authenticity of the transmitted image is provided to the receiver by embedding the authentication information into the camouflage image.
- Compared with those proposed by related methods in recent years, our proposed scheme synthesizes more high-quality stego images and the stego image can be restored losslessly from the camouflage image. Most importantly, the PSNR of the transmitted authentication image is 31.78, which is sufficient to deceive the attacker; moreover, the extraction rate of secret messages can reach 100%.

The rest of this paper is structured as follows. In Section II, we provide an overview of related works. Section III provides a detailed description of the proposed method. Next, in Section IV, we present the experimental results and analysis. Finally, we conclude this paper in Section V.

II. Related Works

A. Traditional Steganography

Traditional nongenerative steganography methods, such as least significant bit (LSB) steganography [24] embed secret messages by altering the carrier image pixel values in the space domain. An earlier method in LSB steganography [35] embedded a secret message by exploiting most of the carrier image pixels. To simultaneously implement image quality and highly embedded capacity in the stego image, Weng et al. [28] proposed a scheme that exploits the reality that many DCT quantization factors are close to zero. However, due to the development of advanced steganalysis techniques, LSB methods are vulnerable to statistical attacks and operate rarely in stego images. Thus, scheme [36] performed the embedding process by using the most suitable regions or features in the cover image.

Traditional generative steganography methods utilize secret messages that are encoded into specific textures or patterns to synthesize stego images. Otori et al. [5] first encoded the secret data into dot patterns that are drawn to synthesize stego texture images. By pasting appropriate source textures in different positions of the composite image, Wu et al. [6] referred to the index table to embed confidential data. In [11], the authors transformed the image into different marbles by leveraging a reversible function after the secret data were stamped on the backdrop of the image. Li et al. [8] encoded the secret data as the location and politeness of nuances in the fingerprint image and then the stego fingerprint image can be constituted by utilizing the phase-based detuning in the encoded detail politeness. For these methods, embedding focuses on parts with more texture and edge detail rather than on smoothed areas, which helps prevent degradation of image quality because changes in texture and edge areas are not as easily detected as are smooth areas. In addition, their synthesized stego images are unrealistic, and are insecure, or even suspect, in covert communication.

B. Deep Learning-Based Steganography

Deep learning-based steganography methods focus on robustness, embedding capacity, and undetectability by analysing image details in a radical way. To enhance the undetectability of the stego image, GANs are usually utilized to optimize the pixel-level embedding cost by detecting the most appropriate part of the image [23]. Tao et al. [22] designed an autocost learner framework according to deep reinforcement learning, which is more suitable for embedded cost optimization, thus improving undetectability. To fundamentally oppose the detection of steganalysis tools and to enhance robustness, Zhou et al. [12] formally proposed "coverless", which hides confidential messages by searching for images that already contain secrets instead of modifying images.

Inspired by coverless methods, Zhang et al. [13] can generate different stego images with matching tags by mapping binary secret messages to auxiliary classifier GANs with class tags based on the given secret data and mapping rules. Liu et al. [30] proposed a method that trains an adversarial automatic encoder, which consists of an encoder that decomposes the image into structural and textural features and a decoder that uses both representations to synthesize high-quality and natural images.

Due to the inefficiency and irreversibility of the secret image transformation, it is difficult to find a good balance between information hiding ability and extraction accuracy. To address this problem, Zhou et al. [14] proposed a secret-to-image reversible transformation (S2IRT) scheme for generative steganography. To produce a more realistic stego image, Zhou et al. [15] introduced a contour generative adversarial network (CtrGAN) that comprises a contour generator and a contour discriminator, and these components are trained by using reinforcement learning in an adversarial manner. However, even the latest steganography technology cannot avoid slight distortion of the composite image, which makes the stego image vulnerable to the suspicion of attackers in the process of covert communication.

C. Traditional Image Transformation

Image transformation is a visually encrypted technology that was proposed based on reversible data hiding (RDH). Lee et al. [41] proposed a method to first sort the blocks based on the standard deviation of the pixel values. By using the colour shift in [42], the mean and the standard deviation of the secret blocks were made close to the respective reference blocks, thus allowing the secret image to be transformed into an arbitrarily chosen reference image. Nevertheless, the secret image can be almost reconstructed only because the truncation errors occur in covering real numbers into integers. Based on [33], a novel reversible transformation method was presented [34], in which an elegant clustering algorithm was leveraged to decrease the information of the log block index. This clustering algorithm did not only improve the optical quality of the transformed image produced by converting a secret image to a randomly picked reference image. However, since the methods proposed in [33] and [34] divide the secret image into blocks and manipulate them separately, block effects will be generated more or less. Due to the block effects, some visual disturbances are imported into the converted image, and block-based conversions are readily discovered by applying falsification detection and image forensic techniques.

To address the problems caused by block effects, Wu et al. [51] attempted to substitute the most significant bit (MSB) plane with the reference image. However, this method cannot be well applied to secret images with high texture since it has the shortcoming in which MSB planes cannot be validly compacted.

D. Deep Learning-Based Image Transformation

Inspired by GAN-based techniques, some deep learning-based image transformation methods have been developed to transform the original image into a reference image. Huo et al. [16] first proposed a method to generate a reference image like the original image by leveraging a synthetic network. Chang et al. [17] devised a field-invariant frame extraction framework that decomposes the image into domain structures and domain-specific texture representations, and thus, they further transform it into a cross-domain image. Cycle-GAN is also a deep learning image transformation method that expands the adversarial loss and nonadversarial loss of the GAN network through the following combination, such as cycle-consistency loss [18]. Zhu et al. [19] proposed a scheme for studying the translation of images from the source domain to a target domain without paired examples. Although the image transformation method based on deep learning has better advantages in image quality and visual effect, the original image cannot be completely recovered from the reference image.

III. Proposed Method

In this paper, we propose a novel scheme that combines coverless steganography and image transformation for the covert communication of secret messages. The proposed framework is shown in Fig. 4. Instead of using an image as the carrier to embed secret messages, our approach conceals it by exploiting a generative network to take the message and a latent as input to synthesize stego images (*SI*) to fundamentally avoid typical eavesdropping and steganalysis attacks. To address the issue that *SI* is illegally obtained and tempered by an attacker in the transmission process of covert communication, we introduce an image transformation algorithm that converts *SI* into another style image (i.e., camouflage image, *CI*), thus achieving the goal of protecting stego images. To verify the integrity of the *CI*, we obtain an authentication image (*AuI*) by embedding the authentication information into the *CI*. In this way, we provide security via ambiguity: Even if a hacker illegally obtains *AuI* and a secret extractor, it is extremely difficult to know that the real stego image has been transformed without having access to any other auxiliary information. Since hacker can extract secret messages through the *AuI*–regardless of whether it is correct or not. In the following, we explain the scheme in detail.

A. Network Architecture

As depicted in Fig. 5, the network consists of three subnets, namely, generator (G), discriminator (D), and extractor (E). They are used to synthesize stego images, to ensure image quality, and to extract secret messages. To resist steganalysis, we hope G can synthesize stego images that are as difficult to distinguish as possible from real images when the float secret message tensor d and latent z are input. First, at each iteration, we input the real image I to the extractor to capture two features that are mapped to the latent z and secret d. According to the forms of z and d, we sample different latents and secrets as the input of the generator to synthesize multiple stego images (i.e., SI_1, SI_2, and SI_3). Next, we elaborate on the training process and the loss of network architecture.

B. Secret Message Preprocessing

Before training our network, we first preprocess the secret message. To better decode the secret message into the structure information of the image, we match the decimal secret message s to the float values d through the formula

$$d = \frac{s + 0.5}{2^{\varepsilon-1}} + \text{rand}\left(-\eta \times \frac{1}{2^{\varepsilon-1}}, \eta \times \frac{1}{2^{\varepsilon-1}}\right), \quad (1)$$

where ε is a constant and η is a hyperparameter.

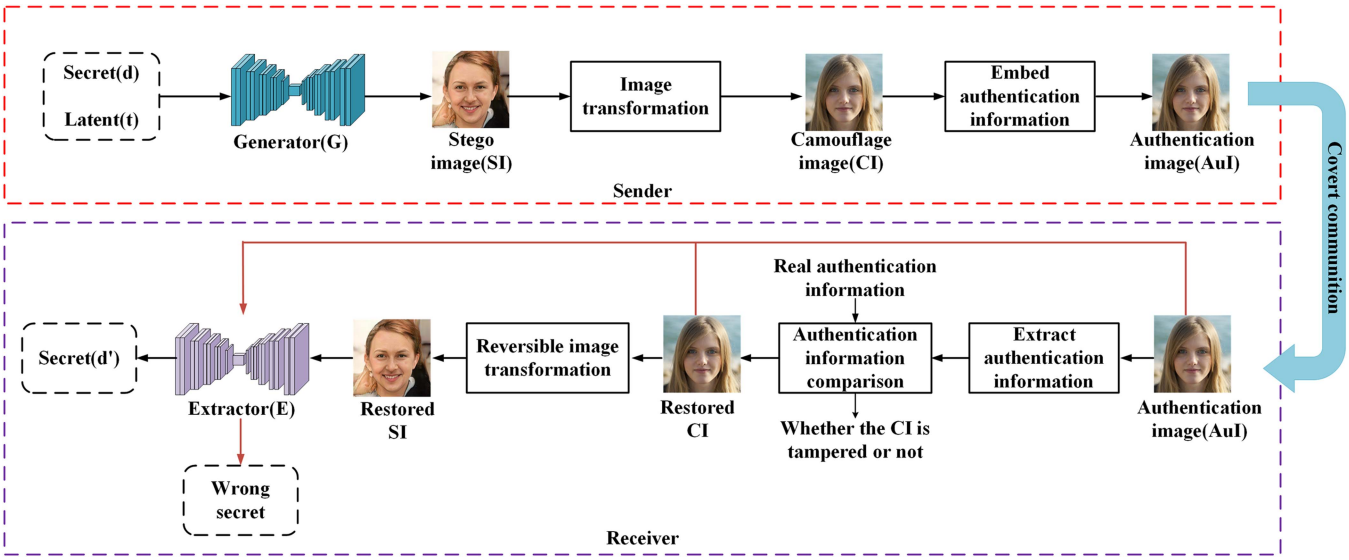

Fig. 4. Framework of our proposed model in this paper.

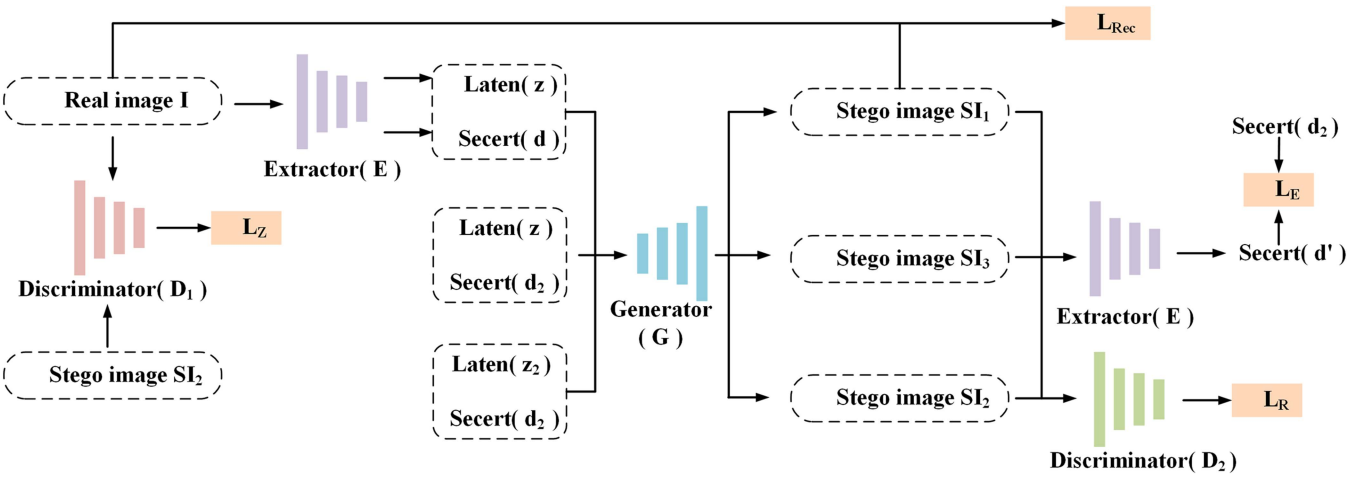

Fig. 5. Training flowchart of proposed network.

The secret message is split into segments of ε bits, and ε is set to 1 in the training of the network. We deploy the stochastic intervals on both sides of the points to adjust η, which ranges in $[a, b]$ to achieve the diversity of the composite image, and the random intervals of each point are of total size $\eta \times 2^{2-\varepsilon}$. Finally, the float values are cascaded as the input of the generator. In the experimental part, we set three levels according to the value η, namely, level $= 1$ ($\eta = 0$) for highly stable message extraction, level $= 2$ ($\eta = 0.25$) for balancing extraction rate and image quality, and level $= 3$ ($\eta = 0.5$) for enhancing security with more diversities.

C. Loss Fuction

We exploit StyleGAN2 [44] as the core architecture of our generator for synthesizing more realistic stego images. It is noteworthy that the StyleGAN2 architecture no longer uses progressive growth but introduces skip connections and residual networks. The skip joints in the generator enormously improve the perceptual path length (PPL) [16] in all configurations, and a residual discriminator network is apparently advantageous for the Fréchet inception distance (FID) [45]. The generator architecture diagram is illustrated in Fig. 6, where Up denotes bilinear up, and tRGB is used to translate among RGB and high-dimensional per-pixel data.

The stego images (i.e., SI_1, SI_2, and SI_3) are generated by employing the generator with various groups of latent and secret message tensors, namely,

$$SI_1 = G(z, d), \tag{2}$$

$$SI_2 = G(z, d_2), \tag{3}$$

$$SI_3 = G(z_2, d_2), \tag{4}$$

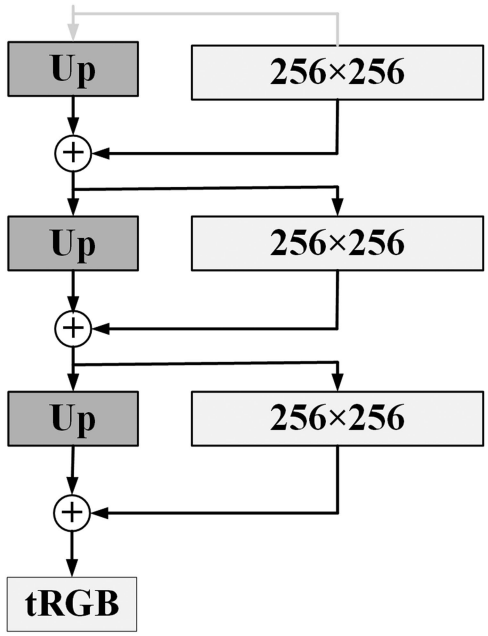

Fig. 6. Generator architecture.

and the reconstruction loss is described as

$$L_{rec} = ||I - SI_1||_1, \tag{5}$$

where I represents the real sample, and $||\cdot||_1$ denotes the L1 loss between images.

The stego image SI_2 is synthesized with the same latent z as I but with different a secret d_2. Then, the co-occurrence discriminator, which was initially proposed in [20] for latent similarity comparison, is used to calculate the latent loss by transferring random cropped patches from I and SI_2, and the latent loss is calculated as

$$L_Z = \text{softplus}(D_1(\text{patch}(SI_2), patch(I))), \tag{6}$$

where $softplus(x) = log(1 + e^x)$, and $patch(\cdot)$ represents the random cropping function.

To generate a realistic image that is independent of I, the latent z_2 and secret tensor d_2 are used as the input of G. The adversarial loss L_G is introduced to ensure the quality of the synthesized image as well as distinguish all composite images from real images and is represented as

$$L_R = \text{softplus}((D_2(SI_1) + D_2(SI_2) + D_2(SI_3))), \tag{7}$$

where D_2 has the same architecture as the above discriminator.

To avoid overfitting in the training phases, the extractor E for extracting the secret tensor from the composite image shares parameters with the extractor to decode the real image. Furthermore, based on experimental experience, SI_2 is used to train extractor E for 80% of the iterations and SI_3 for the last iterations to improve extract accuracy. Finally, the secret message tensor extraction loss L_E is derived as

$$L_E = ||d' - d||_1. \tag{8}$$

where d' is the extracted secret value and d denotes the float value of secret message. Since these losses L_{rec}, L_Z and L_R are related to the synthesized images, we combine them to obtain the generation loss of the generator, namely,

$$L_G = L_{rec} + L_Z + \beta L_R, \tag{9}$$

where the parameter β relates to the quality of synthesized images and it is set to 2. The total loss L_{total} to train the generator G and the extractor E in our network is then formulated as

$$L_{\text{total}} = L_G + \lambda L_E, \tag{10}$$

where λ allows us to balance the generated images quality and the extraction accuracy of the secret tensor.

D. Image Transformation

We take the single channel as an case to illustrate our image transformation algorithm because the colour channels R, G, B for colour images can be transformed in the same way. First, we separate the stego image O and reference image R into N blocks and then couple the blocks of O and R into a sequence $(A_1, B_1), \ldots, (A_N, B_N)$, where A_i represents the block of O and B_i denotes the block of R, $1 \leq i \leq N$. The goal of our proposed method is to transform A_i towards B_i and generate a B_i' like B_i. After transformation, each B_i can be replaced with B_i' to obtain the transformed image R'. Finally, we utilize an RDH method to embed authentication information in R'.

1) Block Matching: To make the transformed image R' as like the reference image R as possible, each block of R' should have a similar mean μ and standard deviation σ with the corresponding block of R. Let a block $C = \{p_1, \ldots, p_n\}$, and the mean value and the standard deviation of the block C are separately defined as

$$\mu = \frac{1}{n}\sum_{i=1}^{n} p_i, \tag{11}$$

$$\sigma = \sqrt{\frac{1}{n}\sum\nolimits_{i=1}^{n} (p_i - \mu)^2}. \tag{12}$$

We hope two closet blocks of standard deviation to be a pair when pairing blocks between the stego image and the reference image. Therefore, we split both the stego and reference images into 4×4 blocks and compute σ per block. Then, we distribute blocks with $\sigma \in [0, N_\alpha]$ to "class 0", and blocks with $\sigma \in (N_\alpha, N_{100}]$ to "class 1", where N_α denotes the $\%\alpha$ quantile of σ. Finally, we scan these blocks from left to right and from top to bottom and allocate a category label 0 or 1 to each block. After counting the stego image block number of the class, we mark the blocks of the reference image. Suppose that the $i\text{-}th$ class in the stego image consists of n_i blocks, where i can be either 0 or 1. Then, we sequentially scan the reference image following the same order as the stego image. We mark the first n_0 blocks with the smallest σ as class 0, while the remaining n_i blocks as class 1. In this way, each class in the reference image contains an identical number of blocks as the corresponding class in the stego image. The stego and reference images are scanned, and the $e\text{-}th$ block of class i in the stego image is matched with

the e-th block of class i in the reference image for $i = 0, 1$ and $e = 1, \ldots, n_i$.

2) Block Transformation: After block pairing, in every pair (A, B), the two blocks have similar σ. Therefore, a reversible mean shifting transformation is needed when transforming A towards B, and the specific steps are as follows. First, let $A = \{p_1, p_2, \ldots, p_n\}$, and the corresponding $B = \{p'_1, p'_2, \ldots, p'_n\}$. The average values of A and B are calculated by employing (11), and they are denoted as m_A and m_B, respectively. Then, the converted block $B' = \{p''_1, p''_2, \ldots, p''_n\}$ is obtained by the formula

$$p''_i = p_i + m_A - m_B. \tag{13}$$

To maintain reversibility in the transformation process, we apply rounding to the difference between the means of the target block and the original block. Specifically, we round this difference to the nearest integer as described in (13). By doing so, the converted block retains the same mean as the corresponding target block by shifting each original block pixel value by amplitude $(m_A - m_B)$, that is,

$$\Delta m = \text{round}(m_A - m_B). \tag{14}$$

After shifting the pixel value by Δm, the p''_i is gotten by

$$p''_i = p_i + \Delta m. \tag{15}$$

The transformed block pixel value p''_i should be an integer between 0 and 255, and (15) may lead to some overflow/underflow pixel values. To avoid this situation, we modify Δm as

$$\Delta m = \begin{cases} \Delta m + 255 - V, & \text{if } \Delta m \geq 0, \\ \Delta m - U, & \text{if } \Delta m < 0, \end{cases} \tag{16}$$

where V denotes the maximum overflow pixel value and U denotes the underflow pixel value; thus, all p''_i values are in the range of [0, 255]. We use Δm to shift the pixels of block A. To further compress the range of Δm, we introduce an even parameter θ, which is set to 8 in the following experiments, and the quantization process is described as

$$\Delta m = \begin{cases} \theta \times \text{round}(\frac{\Delta m}{\theta}), & \text{if } \Delta m \geq 0, \\ \theta \times \text{floor}(\frac{\Delta m}{\theta}) + \frac{\theta}{2}, & \text{if } \Delta m < 0. \end{cases} \tag{17}$$

Finally, we rotate the transformed block and choose an optimal direction for minimizing the root mean square error (RMSE) between the turned block and the target block to maintain most of the similarity between the transformed image and reference image. After transformation and rotation, we obtain the final blocks B' and use them to substitute the respective blocks in the reference image and generated the transformed image R'. The $\Delta m'$ and rotation orientations can be inserted into the transformed image R' to obtain the camouflage image CI.

IV. Experimental Results and Analysis

Our model is trained on PyTorch 1.8 with one GTX-2080Ti GPU, and the software platforms are MATLAB R2019a and Pyhcarm. It is evaluated on datasets FFHQ [46] and bedroom images from LSUN [47], and the size of training images are cropped to 256 × 256. We set $\lambda = 10$ for the performance evaluation in (10).

A. Performance of the Proposed Network

Fréchet inception distance (Fid) is leveraged to measure the invisibility of generated stego images and subjective visual perception, while extraction accuracy (Acc) is used to evaluate the secret extraction accuracy. If the Fid value is smaller, then the degree of similarity is higher, and indicating better modelling. The best case, i.e., Fid = 0, both images are the same. Lower Fid represents better image quality, while high Acc denotes that we can recover secret messages more accurately. In this section, we use the two metrics Acc and Fid to evaluate the extraction accuracy and the invisibility of our model for secret messages. Different steganography capacities are obtained by inputting different sizes of secret messages, and then, each model is trained with different parameters and datasets. Evaluating two metrics with each of the trained models, and the best performance is shown in Table I.

On datasets FFHQ and Bedrooms, the secret message capacities are limited to 3.91e-3 bpp, 7.81e-3 bpp, and 1.56e-2 bpp, respectively. Then, we set three levels (level = 1, 2, 3) according to the needed composite image quality, and level = 3 has the highest composite image quality, which decreases in order. Table I shows the Fid metrics of stego images and the Acc of recovered secret messages under different payloads. From the table, on the two selected datasets, both level = 1 and level = 2 ensure that the Acc of the secret message can reach 100% under all three payloads, and the values of Fid show the high invisibility of secret messages. In addition, when the steganography level is set to 3, the Fid indicator is lower, that is, the steganography composite performance is better, and the Acc can be guaranteed to be more than 98%. Fig. 7 shows some examples of stego images under various payloads (i.e., 3.91e-3 bpp, 7.81e-3 bpp, and 1.56e-2 bpp), which illustrate that the synthesis of secret information into images makes it invisible. These images look indistinguishable from real images but are accompanied by slight distortion. In this way, it can effectively prevent secret information from being subjected to eavesdropping attacks in covert communication.

B. Steganalysis Resistance

The good visual effect of the stego image does not mean that it can avoid attacks from recent steganalysis tools. Therefore, we verify the security and undetectability of the stego image generated by our proposed method under two sophisticated steganalysis approaches, namely, Xu-Net [48] and Ye-Net [49]. The area under the curve (AUC) of the receiver operating characteristic (ROC) produced by the detection of these steganalysis methods is graphed in Fig. 8. In the context of steganography, the ideal ROC curve aligns with the diagonal line, and the optimal AUC value is 0.5. As we can see, under different payloads, all AUC values of our model are smaller or nearly ideal, which demonstrates that our proposed method is safe and verifies

TABLE I
THE ACC AND FID OF PROPOSED MODEL

		3.91e-3 bpp			7.81e-3 bpp			1.56e-2 bpp		
Database		level=1	level=2	level=3	level=1	level=2	level=3	level=1	level=2	level=3
FFHQ	Acc(%)	100	100	99.61	100	100	99.41	100	100	98.56
	Fid	36.52	35.29	32.95	34.69	29.74	27.47	27.25	26.82	26.44
Bedrooms	Acc(%)	100	100	99.61	100	100	99.22	100	100	98.13
	Fid	21.49	18.16	16.49	35.36	29.96	20.49	13.86	13.64	12.54

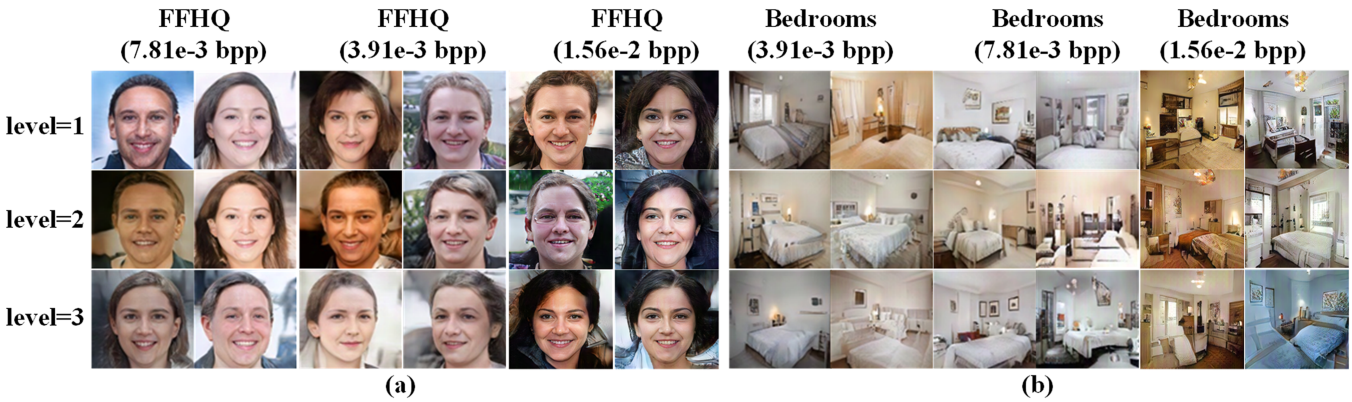

Fig. 7. Examples of generated stego image from our network on dataset FFHQ and Bedrooms. (a) Stego face images from different steganography level are with the different payloads 3.91e-3 bpp, 7.81e-3 bpp, and 1.56e-2 bpp; (b) Stego bedroom images from different steganography level are with the payloads 3.91e-3 bpp, 7.81e-3 bpp, and 1.56e-2 bpp.

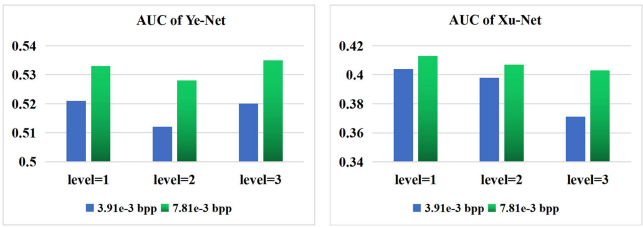

Fig. 8. AUC values of different steganalysis algorithms.

TABLE II
THE P_e VALUES UNDER DIFFERENT PAYLOADS

Datasets	payload	3.91e-3 bpp	7.81e-3 bpp	1.56e-2 bpp
FFHQ	P_e	0.472	0.455	0.428
Bedrooms	P_e	0.486	0.460	0.449

that our method fundamentally resists detection by advanced steganalysis methods.

Additionally, we use the detection error rate (P_e) to evaluate the performance against steganalysis. P_e is a commonly used metric for evaluating the undetectability of stego images, and its ideal value is 0.5. P_e is defined by $P_e = \min_{P_{FA}} \frac{1}{2}(P_{FA} + P_{MD})$, where P_{FA} is the false alarm rate and P_{MD} is the missed detection rate. The steganalysis tool cannot distinguish the source of an image when P_e is equal to 0.5. As seen from Table II, all P_e values obtained by Xu-Net training are close to 0.5 for different payloads as well as level = 1, which indicates that our proposed model resists steganalysis well.

C. Camouflage and Authentication Image Quality

To prevent attackers or hackers from tempering or attacking the transmitted image and the data extractor to illegally obtain secret messages, we design an image transformation method that converts the stego image into a completely different camouflage image CI to achieve ambiguity. Inspired by [54], we embed the authentication information into CI to obtain the authentication image AuI, and AuI is utilized for transmission in the covert communication.

In this part, we verify the authenticity of camouflage images and authentication images through the following three indicators to ensure that they cannot be tempered during transmission. that they The peak signal-to-noise ratio (PSNR) is an objective standard for evaluating images. The RMSE and structural similarity (SSIM) [53] are adopted to measure the similarity of two images and subjectively assess the quality of image structure through visual inspection. As shown in Fig. 9, we select a stego face image SI from the training model based on that they the FFHQ dataset. For reference images RIs, we that they select two images with similar styles from FFHQ to verify the feasibility of our algorithm that they by using three images with very different styles from the stego face images for realizing the diversification of image transformation.

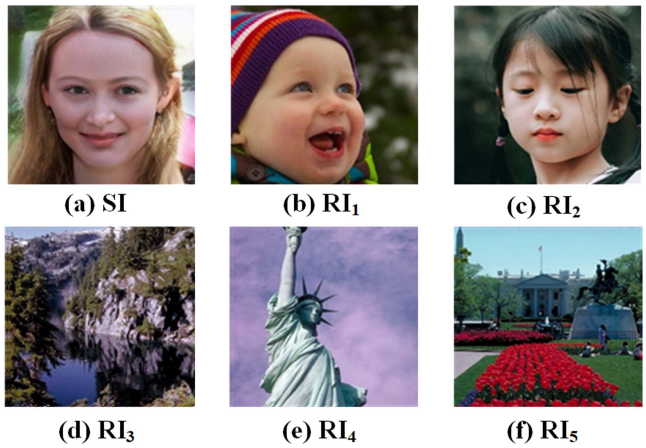

Fig. 9. (a) Stego face image; (b)-(f) Original reference images.

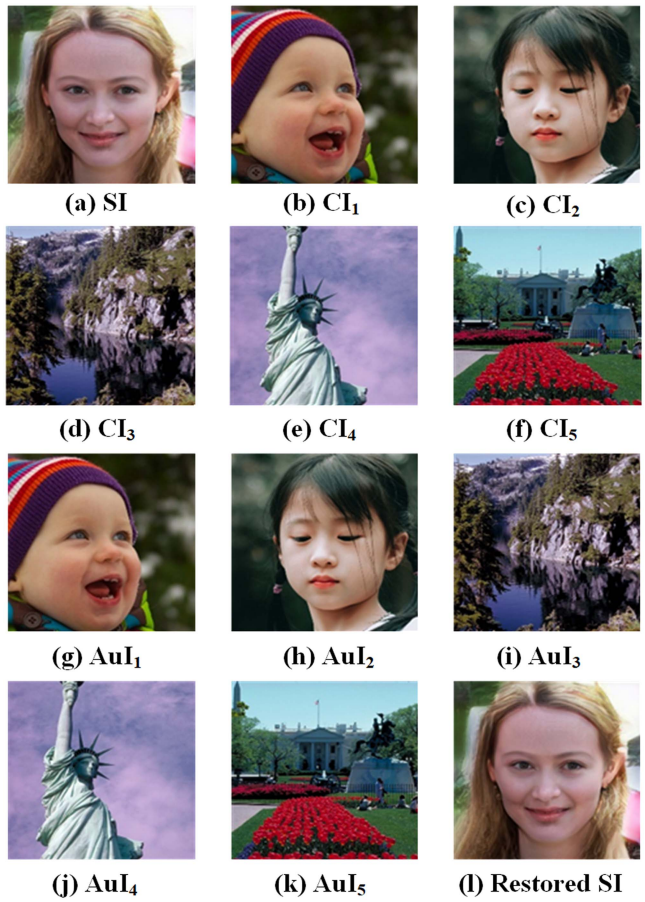

Fig. 10. (a) Stego image; (b)-(f) Camouflag images; (g)-(k) Authentication images; (l) Restored stego face image.

The experimental display effect is shown in Fig. 10. The camouflag images and authentication images are almost the same as the reference images from the visual effect, which greatly improves the security of the image during transmission. Moreover, from Table III, we see that when transforming stego face images to reference images of the same style, the image quality is better than that of the conversion of images with other styles. The PSNR greater than 30 indicates that the converted image is sufficient to deceive the attacker. Even if the hacker attacks to obtain the authentication image and secret extractor, the hacker cannot obtain a correct secret message by the wrong image. Most importantly, the PSNR is Inf, indicating that our proposed method in this paper can restore the stego image without any loss; thus, it is not affected in the secret message extraction phase, and the extraction accuracy of secret information is guaranteed.

D. Security

The primary objective of image steganography is to successfully transmit confidential information while concealing the embedding process. Security naturally takes precedence in image steganography. In the experiments, we assume that both the authentication images and the data extractor are accessible to an eavesdropper, allowing them to extract a message from them. The accuracy of extracting secret information is typically evaluated by using the bit error rate (BER).

The experimental findings depicted in Fig. 11 reveal that the bit error rate (BER) of the authentication images remains low. This indicates that even if the transmitted images are fully exposed, they do not raise suspicions or reveal the hidden secret information to an eavesdropper. Furthermore, when comparing the histograms of the R components of the restored stego images and the authentication images, they are nearly indistinguishable. This finding verifies that the transmitted camouflage images do not arouse suspicion as stego images to potential hackers. Moreover, it is important to note that the encryption process allows for a flexible selection of camouflage image styles. Consequently, even if the camouflage images are fully exposed, there is no leakage of secret information. These experimental results provide convincing evidence that the proposed scheme effectively safeguards the transmission of secret information by concealing the embedding process and thus preventing unauthorized disclosure. The scheme demonstrates a high level of reliability and security.

E. Comparison With State-of-the-Art Methods

1) Quantitative Comparison: We compare our steganography network with four SOTA coverless methods without directly embedding secret messages, as illustrated in Table IV. The comparative methods are reimplemented on the FFHQ dataset, in which 256 $\times$ 256 stego images are synthesized for evaluation. Hu et al. [50] employed a technique where the secret information is encoded into a noise vector, which is then utilized by a trained generator neural network model to generate the cover image. This method has high Acc values close to 96.29% but possesses low payloads less than 1.53e-3 bpp and bad Fid scores. Li et al. [55] introduced a novel steganography method that builds upon the Wasserstein GAN Gradient Penalty (WGAN-GP) framework. This method enables steganography without modifying the original data. Under the same load, the work in [55] has a lower Acc but slightly higher Fid scores. To address the problem of capacity and recovery accuracy, Yu et al. [10] presented a steganography method that does not involve

TABLE III
THE METRICS OF CAMOUFLAGE IMAGES CIs AND AUTHENTICATION IMAGES $AuIs$

	CI_1	AuI_1	CI_2	AuI_2	CI_3	AuI_3	CI_4	AuI_4	CI_5	AuI_5	Restored SI
PSNR	32.11	31.78	32.77	30.74	26.25	21.04	31.69	26.88	28.62	23.34	Inf
SSIM	0.9695	0.9655	0.9556	0.9177	0.8873	0.6339	0.9737	0.9320	0.9456	0.8351	1.0
RMSE	6.3314	6.5705	5.8647	7.4077	12.4108	22.6109	6.6399	11.5501	9.4508	17.3667	0.0

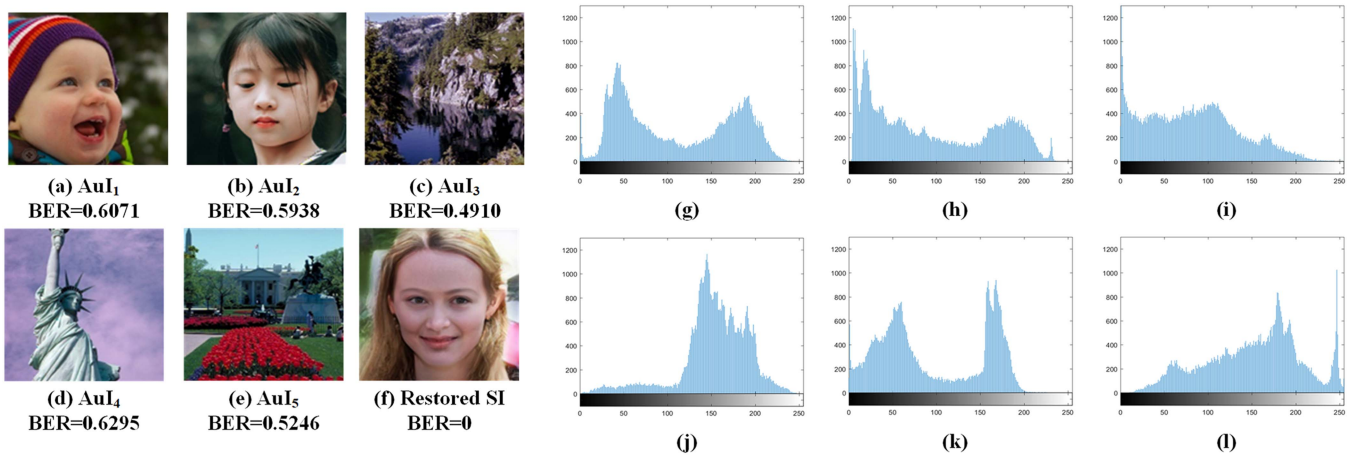

Fig. 11. (a)-(f) BER of Authentication images and Restored stego image; (g)-(l) Histograms corresponding to (a)-(f), respectively.

TABLE IV
COMPARISON WITH STATE-OF-THE-ART METHODS

Methods	Image type	Secret type	Payload(bpp)	Acc(%)	Fid
Hu [50]	natural	binary	1.53e-3	96.29	74.24
Li [55]	natural	binary	1.53e-3	92.85	67.95
Yu [10]	natural	binary	3.05e-3	97.12	82.60
Zhou [14]	natural	binary	1.00e-2	100	—
Ours	natural	float	1.56e-2	100	12.54

embedding, utilizing an attention-GAN model. This approach incorporates attention mechanisms to enhance pixel correlation and address issues such as image distortion and abnormal background. However, we note that this method has a higher Fid score than that of other techniques.

The abovementioned proposed coverless steganography methods without embedding have poor image quality that influences steganographic security, while our proposed steganography network displays better security performance with lower Fid values. Compared to that produced by those methods, our scheme can generate more realistic and natural-looking images with a higher steganography capacity. Our extraction accuracy is the same as that of Zhou [14] for approximately the same payload but slightly lower for other payloads. Moreover, we achieve better Acc and Fid values, further highlighting the effectiveness of our approach.

2) Qualitative Comparison: In terms of steganography techniques, existing image steganography methods are typically categorized as embedding-, mapping- and generation-based methods. Traditional embedding-based steganography in which a secret message is usually embedded into the carrier image by altering the pixel values or factors in the transform fields [27], [28], [52]. These methods inevitably introduce distortions to the cover image while also making resistance of stego images to steganalysis difficult. While mapping-based methods [7], [8], [13] utilize deep networks to establish mapping relationships between secret information and images, which improves embedding efficiency and resistance to steganalysis, such methods suffer from low steganography capacity. Generation-based approaches use generative models to generate stego images according to the secret data [15], [30], which are essentially immune to steganalysis attacks. However, existing generation-based steganography methods still suffer from low data extraction accuracy. To address these problems, we propose a novel scheme that joints coverless steganography and image transformation to achieve a balance between capacity, anti-steganalysis and extraction accuracy. Our proposed solution not only resists eavesdropping and steganalysis but also provides camouflage for stego images while enabling lossless extraction of secret data. To further demonstrate the superiority of the proposed scheme in this paper, three types of steganography schemes Su [52], Zhang [13], and Liu [30] are compared in terms of types of

TABLE V
COMPARISON OF DIFFERENT STEGANOGRAPHY SCHEMES

Analysis indicators	Su [52]	Zhang [13]	Liu [30]	Our
Generation-based	✗	✗	✔	✔
Anti-eavesdropping	✔	✔	✔	✔
Anti-steganalysis	✗	✔	✔	✔
Coverless	✗	✔	✔	✔
No image distortion	✗	✔	✗	✔
Lossless	✗	✗	✗	✔
Ambiguity	✗	✗	✗	✔

steganography, anti-eavesdropping, anti-steganalysis, coverless, no image distortion, lossless and ambiguity. As shown in the Table V, "✔" means yes and "✗" means no.

V. CONCLUSION

In this article, we design a novel framework by joining coverless steganography and image transformation to address the challenges posed by eavesdropping attacks, steganalysis attacks, and tampering attacks during the transmission of covert communication. Instead of using an image as the carrier to embed secret messages, our coverless steganography approach hides secret messages by exploiting generative network to take it and a latent as input to synthesize a stego image, thus essentially avoiding the eavesdropping and typical steganalysis attacks. In addition, we introduce an image transformation method, which converts the stego image into the a camouflage image, and thus our approach provides ambiguity to deceive attackers. Our proposed approach not only addresses these issues, but also goes beyond synthesizing high-quality stego images while ensuring the utmost security of the covert communication. Through extensive experimentation and comparison with state-of-the-art techniques, our proposed method has emerged as the superior choice. It surpasses others in terms of security, ensuring that covert communication remains undetectable, while also achieving a higher accuracy in the extraction of secret messages.

REFERENCES

[1] M. Imran, M. Abolhasan, and J. Lipman, "A comprehensive survey of covert communication techniques, limitations and future challenges," *Comput. Secur.*, vol. 120, 2022, Art. no. 102784, doi: 10.1016/j.cose.2022.102784.

[2] X. Chen et al., "Covert communications: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1173–1198, Secondquarter 2023, doi: 10.1109/COMST.2023.3263921.

[3] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," in *Proc. IEEE Int. Workshop Inf. Forensics Secur.*, 2017, pp. 234–239.

[4] J. Qin, Y. Luo, X. Xiang, Y. Tan, and H. Huang, "Coverless image steganography: A survey," *IEEE Access*, vol. 7, pp. 171372–171394, 2019.

[5] H. Otori and S. Kuriyama, "Texture synthesis for mobile data communications," *IEEE Comput. Graph. Appl.*, vol. 29, no. 6, pp. 74–81, Nov./Dec. 2009.

[6] K. Wu and C. Wang, "Steganography using reversible texture synthesis," *IEEE Trans. Image Process.*, vol. 24, no. 1, pp. 130–139, Jan. 2015.

[7] Z. Qian, H. Zhou, W. Zhang, and X. Zhang, "Robust steganography using texture synthesis," in *Proc. Adv. Intell. Inf. Hiding Multimedia Signal Process.*, 2017, pp. 25–33.

[8] S. Li and X. Zhang, "Toward construction-based data hiding: From secrets to fingerprint images," *IEEE Trans. Image Process.*, vol. 28, no. 3, pp. 1482–1497, Mar. 2019.

[9] R. Meng, Q. Cui, Z. Zhou, Z. Li, Q. M. J. Wu, and X. Sun, "High-capacity steganography using object addition-based cover enhancement for secure communication in networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 2, pp. 848–862, Mar./Apr. 2022.

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

[11] J. Xu et al., "Hidden message in a deformation-based texture," *Vis. Comput.*, vol. 31, no. 12, pp. 1653–1669, 2015.

[12] 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.

[13] Z. Zhang, G. Fu, R. Ni, J. Liu, and X. Yang, "A generative method for steganography by cover synthesis with auxiliary semantics," *Tsinghua Sci. Technol.*, vol. 25, no. 4, pp. 516–527, 2020.

[14] Z. Zhou et al., "Secret-to-image reversible transformation for generative steganography," *IEEE Trans, Dependable Secure Comput.*, vol. 20, no. 5, pp. 4118–4134, Sep./Oct. 2023, doi: 10.1109/TDSC.2022.3217661.

[15] Z. Zhou et al., "Generative steganography via auto-generation of semantic object contours," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 2751–2765, 2023.

[16] Y. Huo et al., "SynSeg-Net: Synthetic segmentation without target modality ground truth," *IEEE Trans. Med. Imag.*, vol. 38, no. 4, pp. 1016–1025, Apr. 2019.

[17] W. Chang, H. Wang, W. Peng, and W. Chiu, "All about structure: Adapting structural information across domains for boosting semantic segmentation," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, 2019, pp. 1900–1909.

[18] D. Dwibedi, Y. Aytar, J. Tompson, P. Sermanet, and A. Zisserman, "Temporal cycle-consistency learning," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, 2019, pp. 1801–1810.

[19] J. Zhu, T. Park, P. Isola, and A. A. Efros, "Unpaired image-to-image translation using cycle-consistent adversarial networks," in *Proc. IEEE Int. Conf. Comput. Vis.*, 2017, pp. 2242–2251, doi: 10.1109/ICCV.2017.244.

[20] T. Park et al., "Swapping autoencoder for deep image manipulation," in *Proc. Adv. Neural Inf. Process. Syst.*, 2020, pp. 7198–7211.

[21] P. K. Singh, "Survey of robust and imperceptible watermarking," *Multimedia Tools Appl.*, vol. 78, no. 7, pp. 8603–8633, 2019.

[22] J. Tao, S. Li, X. Zhang, and Z. Wang, "Towards robust image steganography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 2, pp. 594–600, Feb. 2019.

[23] T. Lu, C. Tseng, and J. Wu, "Dual imaging-based reversible hiding technique using LSB matching," *Signal Process.*, vol. 108, pp. 77–89, 2015.

[24] W. Tai, C. Yeh, and C. Chang, "Reversible data hiding based on histogram modification of pixel differences," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 6, pp. 906–910, Jun. 2009.

[25] W. Chen, C. Chang, and T. H. N. Le, "High payload steganography mechanism using hybrid edge detector," *Expert Syst. Appl.*, vol. 37, pp. 3292–3301, 2010.

[26] C. Vanmathi and S. Prabu, "Image steganography using fuzzy logic and chaotic for large payload and high imperceptibility," *Int. J. Fuzzy Syst.*, vol. 20, pp. 460–473, 2018.

[27] C. Yang, X. Luo, J. Lu, and F. Liu, "Extracting hidden messages of MLSB steganography based on optimal stego subset," *Sci. China Inf. Sci.*, vol. 61, pp. 1–3, 2018.

[28] C. Weng, C. Huang, and H. Kao, "DCT-based compressed image with reversibility using modified quantization," in *Proc. Proc. Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, 2018, pp. 214–221.

[29] T. Pevn'y, 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.

[30] 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.*, 2022, pp. 2303–2312.

[31] I. Lai and W. Tsai, "Secret-fragment-visible mosaic image - A new computer art and its application to information hiding," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, pp. 936–945, Sep. 2011.

[32] H. Wu, R. Jia, J. Dugelay, and J. He, "Reversible image visual transformation for privacy and content protection," *Multimedia Tools Appl.*, vol. 80, no. 20, pp. 30863–30877, 2021.
[33] D. Hou, W. Zhang, and N. Yu, "Image camouflage by reversible image transformation," *J. Vis. Commun. Image Representation*, vol. 40, pp. 225–236, 2016.
[34] D. Hou, W. Zhang, Z. Zhan, R. Jiang, Y. Yang, and N. Yu, "Reversible image processing via reversible data hiding," in *Proc. IEEE Int. Conf. Digit. Signal Process.*, 2016, pp. 427–431.
[35] M. S. Sutaone and M. V. Khandare, "Image based steganography using LSB insertion," in *Proc. IET Int. Conf. Wireless Mobile Multimedia Netw.*, 2008, pp. 146–151, doi: 10.1049/cp:20080166.
[36] N. Hamid, A. Yahya, R. B. Ahmad, and O. M. Al-Qershi, "A comparison between using SIFT and SURF for characteristic region based image steganography," *Int. J. Comput. Sci. Issues*, vol. 9, pp. 110–116, 2012.
[37] 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.
[38] 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 Secur.*, vol. 16, pp. 952–967, 2021.
[39] Z. Zhou, Y. Cao, and X. Sun, "Coverless information hiding based on bag-of-words model of image," *J. Appl. Sci.*, vol. 34, no. 5, pp. 527–536, 2016.
[40] I. Goodfellow et al., "Generative adversarial nets," in *Proc. Int. Conf. Neural Inf. Process. Syst.*, 2014, pp. 2672–2680.
[41] Y. Lee and W. Tsai, "A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 24, no. 4, pp. 695–703, Apr. 2014.
[42] E. Reinhard, M. Ashikhmin, B. Gooch, and P. Shirley, "Color transfer between images," *IEEE Comput. Graph. Appl.*, vol. 21, no. 5, pp. 34–41, Jul./Aug. 2001.
[43] 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.*, 2019, pp. 4401–4410.
[44] 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.*, 2020, pp. 8110–8119.
[45] M. Heusel, H. Ramsauer, T. Unterthiner, B. Nessler, and S. Hochreiter, "GANs trained by a two time-scale update rule converge to a local Nash equilibrium," in *Proc. Adv. Neural Inf. Process. Syst.*, 2017, pp. 6626–6637.
[46] Z. Liu, P. Luo, X. Wang, and X. Tang, "Deep learning face attributes in the wild," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, 2015, pp. 3730–3738.
[47] 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*.
[48] G. Xu, H. Z. Wu, and Y. Shi, "Structural design of convolutional neural networks for steganalysis," *IEEE Signal Process. Lett.*, vol. 23, no. 5, pp. 708–712, May 2016.
[49] J. Ye, J. Ni, and Y. Yi, "Deep learning hierarchical representations for image steganalysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 11, pp. 2545–2557, Nov. 2017.
[50] 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.
[51] H. Wu, S. Tang, and J. Dugelay, "Image reversible visual transformation based on MSB replacement and histogram bin mapping," in *Proc. 10th Int. Conf. Adv. Comput. Intell.*, 2018, pp. 813–818.
[52] W. Su, J. Ni, X. Hu, and J. Fridrich, "Image steganography with symmetric embedding using Gaussian Markov random field model," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 31, no. 3, pp. 1001–1015, Mar. 2021.
[53] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004.
[54] R. Hu and S. Xiang, "Cover-lossless robust image watermarking against geometric deformations," *IEEE Trans. Image Process.*, vol. 30, pp. 318–331, 2021.
[55] J. Li et al., "A generative steganography method based on WGAN-GP," in *Proc. Int. Conf. Artif. Intell. Secur.*, 2020, pp. 386–397.

Wenying Wen (Member, IEEE) received the Ph.D. degree in computational mathematics from Chongqing University, Chongqing, China, in 2013. She is currently a Professor with the School of Information Technology, Jiangxi University of Finance and Economics, Nanchang, China. Her research interests include image processing, information hiding, and multimedia security.

Haigang Huang received the B.E. degree from Jiangxi Agricultural University, Nanchang, China, in 2021. He is currently working toward the M.E. degree with the School of Information Technology, Jiangxi University of Finance and Economics, Nanchang. His research interests include image processing and multimedia security.

Shuren Qi received the B.A. and M.E. degrees from Liaoning Normal University, Dalian, China, in 2017 and 2020, respectively. He is currently working toward the Ph.D. degree in computer science with the Nanjing University of Aeronautics and Astronautics, Nanjing, China. His research interests include invariant feature extraction and visual signal representation with applications in robust pattern recognition and multimedia forensics/security.

Yushu Zhang (Senior Member, IEEE) received the Ph.D. degree from the College of Computer Science, Chongqing University, Chongqing, China, in 2014. He is currently a Professor with the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China. His research interests include multimedia security, artificial intelligence, Big Data security, and blockchain. Dr. Zhang is the Editor of Information Sciences and Signal Processing.

Yuming Fang (Senior Member, IEEE) received the Ph.D. degree from Nanyang Technological University, Singapore, 2013. He is currently a Professor with the School of Information Management, Jiangxi University of Finance and Economics, Nanchang, China. His research interests include visual attention modeling, visual quality assessment, image retargeting, computer vision, 3D image/video processing.