Latent Vector Optimization-Based Generative Image Steganography for Consumer Electronic Applications

Zhili Zhou*, *Senior Member, IEEE*, Zhipeng Bao, Weiwei Jiang*, Yuan Huang, Yun Peng, Achyut Shankar, Carsten Maple, Shitharth Selvarajan, *Member, IEEE*,

***Abstract*—In consumer electronic applications, to transmit secret images securely, it is required to explore the advanced covert communication technology, i.e., Generative Image Steganography (GIS). However, the existing GIS schemes suffer from the issues of poor stego-image quality and limited hiding capacity. Consequently, these GIS schemes cannot meet the requirements of consumer electronic applications, in which massive secret information needs to be transmitted securely. To address the above issues, we propose a Latent Vector Optimization (LVO)-based GIS scheme, in which the information hiding is implemented by the flow-based generative model during the image generation. Specifically, the LVO algorithm is introduced to compute the hiding probability of each element of latent vector according to its impact on the quality of the stego-image generated from the latent vector. Then, it hides more information in elements with higher hiding probability. The extensive experiments demonstrate that, compared to current GIS schemes, the proposed LVO-based GIS scheme generates higher-quality images, while maintaining hiding capacity (up to $5.0\,bpp$) and accurate information extraction (almost 100% accuracy rate).**

***Index Terms*—Generative model, Generative Steganography, AI-Generated Content, Consumer Electronics**

I. Introduction

In recent years, there has been a significant advancement in consumer electronic systems. These systems integrate a large number of Internet of Things IoT devices, such as smart sensors in consumer electronic products, and industrial equipments [1], [2], [3], [4]. These devices possess the capability of producing massive amounts of data, and a large proportion of those produced data is personal identity information and privacy data [5]. To transmit those secret data securely, it is required to explore the advanced covert communication technologies. To this end, image steganography has been extensively studied as an effective covert communication technology. To this end, image steganography has been extensively studied as an effective covert communication technology in consumer electronic applications. Fig. 1 shows the example of how the steganographic approach is used for covert communication in consumer electronic environment. Specifically, if the sender needs to send a secret message to the receiver, he can use the smartphone or tablet to encode and send the secret message to the cloud server; The cloud server learns a steganographic neural network by the use of its powerful computation ability to implement the steganography to generate the stego-image; Finally, the cloud server sends the generated stego-image to the receiver's smartphone or tablet, so that the receiver can extract and recover the secret message from the stego-image.

Traditional image steganography [6] generally makes subtle modifications to an existing natural image to embed secret information. However, these minor alterations could cause the hidden secret information to be successfully detected by steganalyzers [7], [8], [9]. In response to this challenge, generative image steganography (GIS) [10], [11], [12] has emerged as a promising covert communication technology. Without any modification, it directly generates a new image as the stego-image driven by any given secret data. However, the existing GIS schemes suffer from several issues. First, these GIS schemes produce lower-quality stego-images, causing the stego-images easily to be detected by human eyes. Second, a single stego-image typically carries only a small amount of secret information, which makes the GIS less practical in consumer electronic systems. Thus, it is urgent to enhance both image quality and hiding capacity for the practical

This work is supported in part by the National Natural Science Foundation of China under Grant 62372125, Grant 61972205, Grant U1936218, in part by the Guangdong Natural Science Funds for Distinguished Young Scholar under Grant 2023B1515020041, and in part by the Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET) fund, China.

Zhili Zhou* is with Institute of Artificial Intelligence, Guangzhou University, China (the first corresponding author, zhou_zhili@163.com).

Zhipeng Bao is with the School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, China, alexbao0206@outlook.com)

W. Jiang*, the second corresponding author, is with School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing, 100876, China, jww@bupt.edu.cn).

Yuan Huang, Senior Engineer Artificial Intelligence R&D Center, CNNC Equipment Technology Development Co., Ltd., China, hyuan2020@zju.edu.cn

Yun Peng is with Institute of Artificial Intelligence, Guangzhou University, China, yunpeng@gzhu.edu.cn

Achyut Shankar, Department of Cyber Systems Engineering, WMG, University of Warwick, Coventry, United Kingdom, CV74AL, ashankar2711@gmail.com

Carsten Maple, Secure Cyber Systems Research Group (SCSRG), WMG, University of Warwick, Coventry, UK, cm@warwick.ac.uk

Shitharth Selvarajan, School of Built Environment, Engineering and Computing, Leeds Beckett University, LS1 3HE Leeds, U.K. Email: s.selvarajan@leedsbeckett.ac.uk

consumer electronic applications.

To address the above issues, we introduce the Latent Vector Optimization (LVO)-based GIS scheme. Many GIS approaches [13], [14], [15], [16], [17] have been proposed based on the Generative Adversarial Networks (GAN) [18]. However, these approaches generally have small hiding capacity due to the limited size of the latent vector. To achieve high-capacity information hiding, some generative steganographic approaches [19] have been proposed based on the flow-based generative model. That is because the input latent vectors in flow-based generative models are with high dimension, resulting in high hiding capacity. Moreover, since the flow-based generative model is invertible between the input latent vector and the output stego-image, the extraction rate of flow-based approaches can reach up to almost 100%. Hence, our proposed LVO-based GIS scheme is designed based on the flow-based generative model (Glow Model).

The proposed LVO scheme can achieve high-quality image generation with a large data hiding capacity, thus meeting the requirements of consumer electronic applications. Specifically, the LVO algorithm is introduced to compute the hiding probability of each element of latent vector according to its impact on the quality of the stego-image generated from the latent vector. Then, it hides more information in elements with higher hiding probability.

The proposed LVO-based GIS scheme can realize the transmission of sufficient secret information by generating only a limited number of stego-images. This significantly reduces the computational burden on local devices, making it suitable for applications of consumer electronics. Figure.1 illustrates how the proposed generative image steganography is applied in consumer electronic applications.

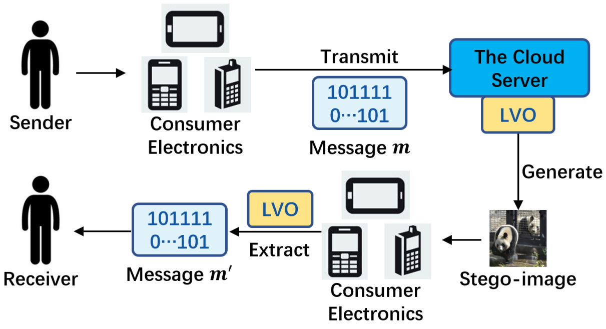

Fig. 1. The application of the steganographic approach in consumer electronic environment.

In this paper, we propose a novel GIS scheme based on LVO scheme for consumer electronic applications. This scheme has the ability of generating high-quality stego-images with large hiding capacity. The main contributions are summarized as follows.

- It is found that different dimensions of the latent vector in the flow-based model has different impacts on the stego-image quality differently. Thus, we introduce the concept of latent vector hiding probability, and compute the hiding probability for each element in the vector based on its expected impact on the stego-image quality.
- The proposed Latent Vector Optimization scheme (LVO) is implemented according to the hiding probability of elements of latent vectors. It can further improve the stego-image quality under a certain hiding payload.
- The experimental results confirm that the proposed LVO-based GIS scheme significantly improves stego-image quality. Additionally, the proposed GIS scheme shows high hiding capacity, i.e., up to $5.0\,bpp$, maintaining 100% accurate information extraction.

The rest of this paper is organized as follows. Section II introduces the related works. Section III describes the proposed GIS scheme. Experiment results and analysis are introduced in Section IV, and conclusion is drawn in Section V.

II. Related Work

In this section, our focus lies on two mainstream generative image steganography schemes, which are based on GAN and based on FLOW, respectively, along with some secret image sharing methods.

A. GAN-based Generative Image Steganography

Due to the rapid development of GANs, many approaches for generative image steganography are based on GANs. In those approaches, the secret message is usually encoded as the entangled features such as latent noise vector [20], [21], [22], style vector [23], and abstract-structure vector [24]. Then the GAN can use the entangled features to generate the corresponding stego-image in a non-distribution preserving manner. Based on GAN, Hu et al. [25] proposed the steganography without embedding (SWE) approach, in which the secret information is encoded as a latent noise vector, and the deep convolutional GAN(DCGAN) [26] uses this latent noise vector to generate stego-images for carrier classification. GAN networks are the foundation of numerous image processing and picture generating techniques, all of which perform well. Liu et al. [27] proposed Sketch2Photo, it has great image quality and may be used to transform a draft image to a real image using GAN while preserving global information. Xu et al. [28] proposed a approach to remove specular highlights from a single grayscale image based on GAN, this method can effectively handle the highlights that are damaging the image. Singh et al. [29] proposed a GAN-based encryption method to secure digital images, it can possess a high level of security and save sufficient storage space for any practical application.

The latent noise vector used in GAN model is similar to the latent vector of flow-based model. The difference is that the former is generally smaller in size, limiting the hiding capacity, while the latter is larger in size, which is beneficial to the hiding capacity. Thus, most GAN-based approaches try to utilize other feature representations to improve generative steganography performance.

Liu et al. [24] proposed a GIS method based on Image Disentanglement Autoencoder for Steganography (IDEAS), in which the secret information is mapped into a latent noise vector and then is converted into a structural feature of the image; Then, the structural feature and the image texture feature obtained by random sampling are used as the input to the generator to generate the stego-image. Since the structural features of the image are more stable, IDEAS improves the accuracy of secret information extraction. In addition, by adding texture features obtained by random sampling, IDEAS can generate a variety of stego-images when hiding specific secret information. Thus, it can avoid the problem of generating only a single stego-image for the specific secret message, thus improving the security of steganography.

However, the secret message extraction rate of GAN-based approachs is hard to reach up 100% because GAN only fits a unidirectional mapping of the latent noise vector to the stego-image.

B. Flow-based Generative Image Steganography

The flow-based GIS schemes have the advantage of high extraction accuracy, due to the flow-based model's ability of achieving reversible mapping between the input latent vector and the output stego-image.

Zhou et al. [19] proposed the secret-to-image reversible transformation (S2IRT) scheme based on Glow [30] model to achieve efficient generative image steganography. In hiding stage, to increase the hiding capacity, the sender encodes the secret message into a high-dimensional vector using a location encoding algorithm, thus forming a high-dimensional latent vector based on the obtained position index; Then the latent vector is mapped to the stego-image by the Glow model. In extraction stage, the receiver can transform the pre-processed stego-image into a latent vector by the inverse transformation of the Glow model, and decode the latent vector to obtain the secret message. Due to the lossless of coding and the reversible mapping between latent and image space by the Glow model, the S2IRT scheme can extract the secret information accurately while greatly increasing the hiding capacity.

TABLE I
A BRIEF COMPARISON OF THE TWO MAINSTREAM GENERATIVE METHODS.

Base	Hiding capacity	Image quality	Extraction accuracy
GAN	small	Higher	$< 100\%$
Flow	large	High	$\approx 100\%$

However, the flow-based GIS schemes have the following drawbacks. The information hiding is implemented without consideration of the impact of different latent vector elements, resulting in inferior hiding performance and insufficient image diversity.

C. Secret Image Sharing approaches

Currently, there are many secret image sharing (SIS) methods for consumer electronic applications. The existing SIS methods are based on traditional image steganography.

Li et al. [31] proposed a SIS method based on Shamir's polynomials, allowing seamless image sharing over the cloud. However, this method is originally designed for gray-level image, and its hiding capacity is relatively small. Huang et al. [32] proposed an encrypted domain SMIS (Enc-SMIS) scheme with secure outsourcing computation for protecting and managing medical images in IoT environment and it can reduce computational burden on cloud servers through fully homomorphic encryption and grouping. However, to ensure the security of image shares, this scheme still requires lots of computation resources to support the encryption and decryption operations.

Zhou et al. [33] proposed a Blockchain-based Secure and Efficient Secret Image Sharing (BC-SESIS) scheme with outsourcing computation in wireless networks. In the BC-SESIS scheme, the shadow images are encrypted and stored in the blockchain to prevent them from being tampered and corrupted. This scheme allows secure communication and effective protection of secret image data in wireless networks. However, since the image sharing and recovery are implemented in the encryption domain, the computation complexity is relatively high, which makes this scheme less appealing in practice. Xiong et al. [34] proposed the SISA scheme, which is an authenticated secret image sharing method ensuring reliability in sharing and preventing data loss. Based on the extended RSIS, this scheme segments the secret image into a series of stego-images distributed across multiple edge servers within the IoT, thus enhancing security. This SISA scheme is more practical and efficient, and shows higher performance in practical applications.

Wu et al. [35] proposed a novel multigroup SIS method based on compressed sensing and chaos theory models. This approach enables simultaneous achievement of SIS and image data compression. With image compression and chaos theories, the security of data transmission is significantly enhanced. Zhou et al. [36] proposed a SIS scheme based on encrypted pixels. This scheme optimizes shadow images and improves the performance of SIS. Li et al. [37] proposed public key authenticated encryption with ciphertext update and keyword search(PAUKS scheme) to enable electronic medical data to be encrypted and retrieved without decryption. Thus, it achieve secure data sharing and storage.

III. OUR METHODOLOGY

The flow chart of our approach is illustrated in Figure.2. Specifically, the computed hiding probability of latent vector elements and a randomly chosen natural image are utilized for the latent vector optimization, and then the appropriate dimensions in the vector z obtained by random sampling are modified to hide the secret message m, and the modified vector is input into the Glow model, resulting in a high quality stego-image.

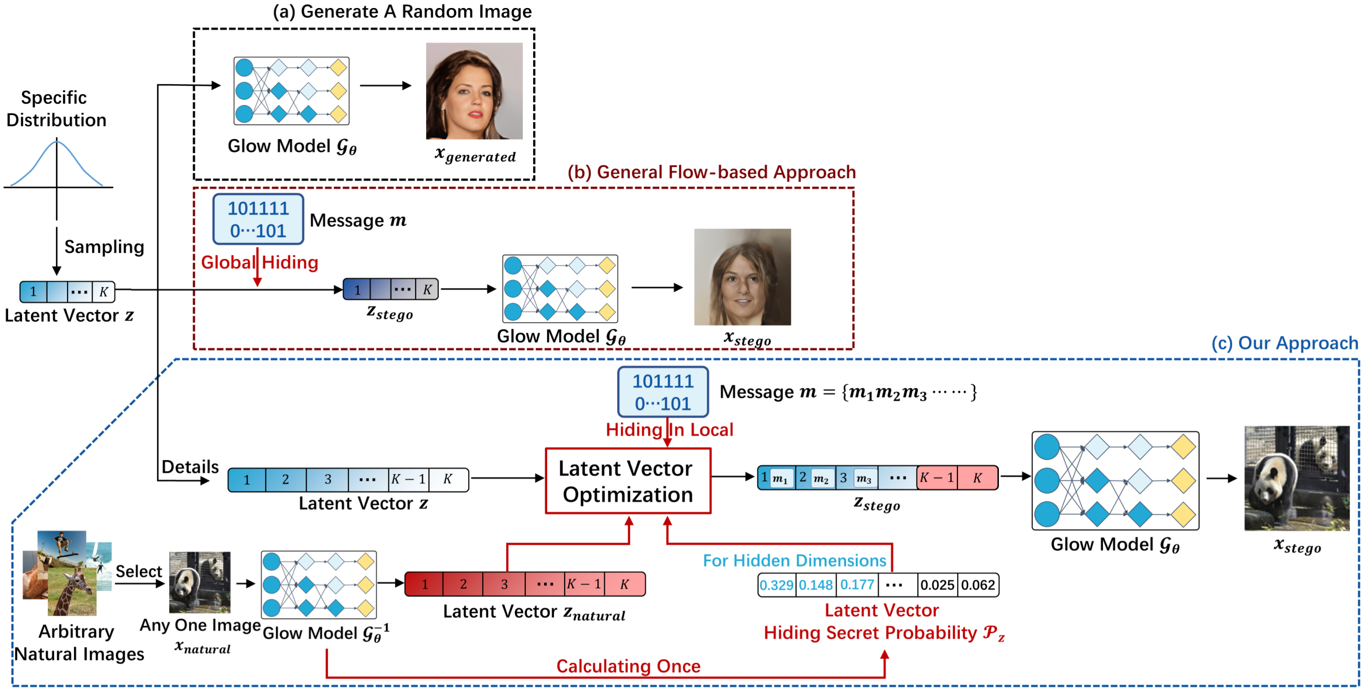

Fig. 2. Flowchart of flow-based generative image steganographic approaches, which consists of three parts: (a) generate a random image, (b) general flow-based approach to generate a stego-image, and (c) our approach to generate a stego-image.

A. Glow Model

The proposed LVO-based GIS scheme relies on flow-based generative models. Specifically, the hiding of secret information is implemented based on the input latent vector of the flow-based generative model. Flow-based generative models such as RealNVP [38] and Glow [30] are able to produce realistic natural images, which can learn a bijective-mapping between latent vector space with simple distribution and natural image pixel space with complex distribution.

In this paper, we focus on Glow [30] model to implement latent vector optimization scheme. The bijective-mapping in Glow model is described as follows:

Let z be the variable of latent space following the simple distribution $p_Z(z)$, i.e., spherical multivariate Gaussian distribution, and x the variable of image space following a complex distribution $p_X(x)$, i.e., natural image data space. To achieve the bijective-mapping, the training process of Glow model is to learn an invertible mapping function f. The function and its inverse function can be represented by

$$z = f_\theta(x) \tag{1}$$

$$x = g_\theta(z) = f_\theta^{-1}(z) \tag{2}$$

Where, the latent vector z, after undergoing the inverse function of f, can be transformed into an image x. We denote the inverse function of f as function g. The dimension of z is equal to that of x, and the components z_d are assumed to be independent.

Glow model relies on the Jacobian determinant, and according to the Jacobian determinant,the relationship between the distributions $p_X(x)$ and $p_Z(z)$ can be represented by

$$p_X(x) = p_Z(z)\left|det\frac{\partial z}{\partial x}\right| = p_Z(f_\theta(x))\left|det\frac{\partial f_\theta(x)}{\partial x}\right| \tag{3}$$

With Equation.1 and Equation.2, we can generate a realistic image x by randomly sampling the standard Gaussian distribution as the latent space vector z, or convert a natural image x into a latent space vector z that follows the standard Gaussian distribution.

B. Latent Vector Hiding Secret Probability

According to the transformation of Glow model, each dimension of the latent vector is theoretically independent and has some impact on the final generated image. However, in practice, due to the constraints of training set and training scale, the network weight parameters of the Glow model are difficult to be fully trained, causing different latent space vectors to have different degrees of impact on the quality of the final generated image.

By studying the latent vectors more thoroughly, we can achieve GIS by utilizing the latent vectors more efficiently. Specifically, we can measure the degree of impact of latent vectors in different dimensions on the final generated stego image quality, and thus calculate the distortion expectation caused by modifying latent vectors in different dimensions, and thus we define the hiding probability of latent vectors in each dimension.

In this paper, we use the following method to compute the expectation of distortion caused by adjusting the latent

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCE.2024.3354824

vectors of different dimensions. Using the inverse conversion function $g^{-1}()$ of the Glow model, we convert the real natural image data $x_{natural} \in \mathcal{R}$ into the latent vector $z_{natural} = g^{-1}(x_{natural})$, and then adjust each element value of the latent vector $z_{natural}$ to measure the difference of image distortion caused by the change of each element of the latent vector with the original image, so as to evaluate the degree of influence of each element on the image generation quality. Each element $z_{natural}(i)$ of the latent vector $z_{natural}$ is adjusted n times, and the value of expectation $\mathcal{E}_z(i)$ of the image quality change for each element of the latent vector $z_{natural}(i)$ is calculated according to the difference in image distortion before and after the adjustment as follows:

$$\mathcal{E}_z(i) = \frac{1}{n_{\Delta_z}} \sum_{\Delta_z=-a}^{a} \left[Diff\left(g\left(z'_{natural}\right), x_{natural}\right)\right] \qquad (4)$$

where,

$$z'_{natural}(j) = \begin{cases} z_{natural}(i) + \Delta_z, & j = i \\ z_{natural}(i), & j \neq i \end{cases}, for\ 1 \leq\ i \leq K, \qquad (5)$$

Where, the function $Diff()$ is used to determine the distortion difference between the modified reconstructed image $g\left(z'_{natural}\right)$ and the original image $x_{natural}$, according to the experimental results, since the Peak signal-to-noise ratio (PSNR) can reflect the more obvious difference between different elements of the hidden space vector, we use the commonly used PSNR criterion to calculate the difference between the two images. The magnitude of $z_{natural}(i)$ that can be adjusted is denoted as $\Delta_z \in [-a, +a]$, with Δ_z taking n_{Δ_z} values at medium intervals in the range $[-a, +a]$.

Under the assumption that the distortion expectations of the elements of each dimension are independent of each other, the distortion expectation matrix $\mathcal{E}_z$ has K dimensions and can be indicated as $\mathcal{E}_z = [\mathcal{E}_z(1),\ \mathcal{E}_z(2), \cdots, \mathcal{E}_z(K)]$. This distortion expectation matrix $\mathcal{E}_z$ is applied to all input latent vectors z of this flow model and thus only requires to be calculated once. We can calculate the hiding secret probability matrix $\mathcal{P}_z = [\mathcal{P}_z(1), \mathcal{P}_z(2), \cdots, \mathcal{P}_z(K)]$ based on the distortion expectation matrix $\mathcal{E}$, where the hiding secret probability $\mathcal{P}_z(i)$ of each element $z_{natural}(i)$ of the latent vector $z_{natural}$ is given as follows:

$$\mathcal{P}_z(i) = \frac{e^{\mathcal{E}_z(i)}}{\sum_k^K e^{\mathcal{E}_z(k)}},\ for\ 1 \leq\ i \leq K \qquad (6)$$

Where, the Equation.6 represents the hiding secret probability $\mathcal{P}_z(i)$ of each dimension in the K-dimensional latent vector z.

In the latent vector z, those dimensions with smaller distortion expectation have higher hiding secret probability and tend to hide more secret information, while those dimensions with larger distortion expectation have lower hiding secret probability and are used to improve the image quality.

C. Latent Vector Optimization Scheme for Generative Image Steganography

After calculating the hiding secret probability of input latent vector of the Glow model, at this stage we start to optimize the latent vector to improve the quality of the generated stego-images effectively and achieve predictable generative image steganography with high hiding capacity and accurate information extraction simultaneously. In contrast to hiding secret information globally in the latent vector, our scheme will only hide it locally in the latent vector.

We leverage natural images to enhance image quality for three key reasons: (1) Natural images exhibit superior quality, serving as the ultimate visual benchmark for any generated image. Directly employing natural images can effectively enhance the quality of generated stego-images. (2) The Glow model's reversible characterization enables the utilization of natural images. While the Glow model generates images similar to its training dataset, its principle allows any non-training set natural image to be converted into a standard Gaussian-distributed latent vector of the same dimension. This vector can then reconstruct the original image. Hence, flow-based generative image steganography methods leverage natural images. For instance, our approach enables a Glow model trained on facial data to produce the stego-images, whereas typical generative image steganography is confined to the images from the training dataset. (3) Generative image steganography typically yields unpredictable stego- images corresponding to different secret messages. As a result, hiding some messages may lead to poor-quality stego- images. The proposed GIS scheme ensures predictable, high-quality generative image steganography across all secret messages.

In Hiding Phase, pseudocode Algorithm 1 demonstrates algorithm for the hiding phase. The proposed LVO-based GIS is specified as follows:

Step (1). First, K elements are randomly sampled from the standard Gaussian distribution to construct a K-dimensional latent vector z for generating stego-images. The elements of z in the ith dimension are denoted as z^i, $z = [z^1, z^2, z^i, \cdots, z^K]$. At this point, the latent vector z can be transformed by the Glow model transformation function $g()$ to generate an image $x = g(z)$.

Step (2). Select an arbitrary natural image, and use the inverse transform function $g^{-1}()$ of this Glow model(Eq. 4) to calculate once the expectation value $\mathcal{E}_z$ of the image quality change for each element of the latent vector z input to this Glow model. The K-dimensional distortion expectation matrix $\mathcal{E}_z$ can be indicated as $\mathcal{E}_z = [\mathcal{E}_z(1),\ \ \mathcal{E}_z(2), \cdots, \mathcal{E}_z(K)]$. According to Eq. 6, we can calculate the hiding secret probability matrix $\mathcal{P}_z = [\mathcal{P}_z(1), \mathcal{P}_z(2), \cdots, \mathcal{P}_z(K)]$ based on the distortion expectation matrix $\mathcal{E}_z$. The matrix $\mathcal{P}_z$ also requires only single calculation. Meanwhile, this image can be converted to the latent vector $z_{natural}$ by the inverse transform function $g^{-1}()$, which will be used for the next latent vector optimization.

Step (3). Given a secret message m with length M, we first

Algorithm 1 LVO scheme's algorithm for the hiding phase.

```
Require: $z^i (i = 1, 2, , K)\ and\ \mathcal{P}_z$
Ensure: $\frac{M}{7} < K$
Ensure: $Sort\ \mathcal{P}_z\ from\ largest\ to\ smallest$
for $i = 1$ to $K$ do
    Assigning the $11th$ decimal of $z^i$ to be 0.    ▷ Initializing the flag bit.
end for
for $i = 1$ to $\frac{M}{7}$ do
    for $q = 4$ to 10 do
        Modify the $qth$ decimal place of $z^i$ to the $m_i$.
    end for
    Assigning the $11th$ decimal of $z^i$ to be 1.    ▷ Marking that the $z^i$ contains information.
end for
```

divide it by length 7, each m_i contains $7bit$ binary numbers and $m = \{m_1, m_2, m_3, \cdots, m_{\frac{M}{7}}\}$. Therefore, a total of $\frac{M}{7}$ sub-secret messages m_i need to be hidden, and for each dimensional element z^i of a K-dimensional latent vector z, there will be $7bit$ of information that can be hidden into one m_i for each dimensional element. Iterate through the K-dimensional hiding secret probability matrix $\mathcal{P}_z$, select the $\frac{M}{7}$ dimensional elements z^i in the latent vector z for hiding secret information according to the hiding probability from the largest to the smallest, and modify the $4th$ to $10th$ decimal place of the value of each z^i to the $7bit$ binary value in m_i. Then, for those dimensions z^i that are not selected, the z^i in the corresponding position of the latent vector z is replaced with $z_{natural}$ using the natural image latent vector $z_{natural}$ in the previous step (2). Finally, among the elements of all dimensions of the latent vector z^i, the $11th$ decimal element of those used to hide the secret information m_i is modified to 1 for marking that dimension as hiding secret information, while the $11th$ element of z^i of the other dimensions is modified to 0 to indicate that there is no secret information in that dimension. Meanwhile, the optimized latent vector z is denoted as z_{stego}. Modifying the later decimal places of the value of z^i has little impact on the generation of the stego-image, and both $z_{natural}$ and z follow the standard Gaussian distribution, so the replacement of element values would not impact the distribution of the latent vector.

Step (4). After constructing the stego optimal latent vector z_{stego}, we input it into the Glow model to generate a high-quality stego-image x_{stego}, which can be used for covert communication.

In Extracting Phase, the message extraction process of proposed GIS is specified as follows:

Step (1). At the receiving end, the received image is reversely mapped to a latent vector z by the Glow model.

Step (2). In dimensional order, we scan each dimensional element z^i in the K-dimensional latent vector z. If the $11th$ decimal place of the value of z^i is 1, the $7bit$ binary value of the $4th$ to $10th$ decimal place of that z^i is recorded as $m_i^{'}$, and skipped if the value of the $11th$ decimal place is 0. After obtaining all the $m_i^{'}$, we concatenate these $m_i^{'}$ to extract the final secret message $m^{'}$.

IV. Experimental Results

A. Experimental Setup

To demonstrate the superiority of proposed LVO-based GIS, we compare it with three state-of-the-art GIS approaches, namely SWE [25], IDEAS [24] and S2IRT [19].Among them, SWE and IDEAS are based on GAN, while S2IRT is based on flow model, and they all utilize the latent vector for generative image steganography. The Glow model is trained on three publicly available datasets, face images from FFHQ [39] and CelebA [40], and landscape images from COCO [41]. To enrich the dataset, we also included a larger set of LSUN [42] images, comprising 100,000 images of churches. Among these, in addition to the 100,000 LSUN churches dataset images, there are separate sets comprising 30,000 high-quality natural images each. For training convenience, we rescale the size of the images to 256x256 and train the Glow model on the rescaled images.

We evaluate the anti-detectability performance against a steganalyzer by detection error rate P_E, and visual imperceptibility using Fréchet inception distance (FID) [43]. Also, we compare information extraction accuracy by LVO under different hiding payloads with benchmark generative image steganographic approaches. All the experiments are conducted on an NVIDIA RTX 3090 GPU platform using PyTorch with Python interface.

B. Security Evaluation by Steganalysis

We evaluate the anti-detectability performances of those generative image steganographic approaches on well-known steganalyzers, including SRM [44] and Xunet [7] to detect whether the secret information is hidden in the stego-image. To compare with traditional steganography, we include the well-known traditional steganographic approach S-UNIWARD [45], and use the following detection error rate as a quantitative criterion:

$$P_E = \min_{P_{FA}} \frac{1}{2}(P_{FA} + P_{MD}) \tag{7}$$

Where, the probability of false alarm (FA) of the steganalyzer is denoted as P_{FA}, and the probability of missed detection (MD) of the steganalyzer is denoted as P_{MD}. The higher anti-detectability to the steganalyzer, the higher the P_E.

Table. II lists the values of P_E of the different approaches against the steganalyzers, and it can be seen that the generative steganography has a high anti-detectability performances ($P_E > 0.25$). Among them, when the hiding payloads is $0.1\,bpp$, the traditional approaches are able to have a high anti-detectability because they have only minimal modifications to the cover image, while the generative image steganography dominates absolutely when the hiding payload is greater than or equal to $0.5\,bpp$. Where there are empty

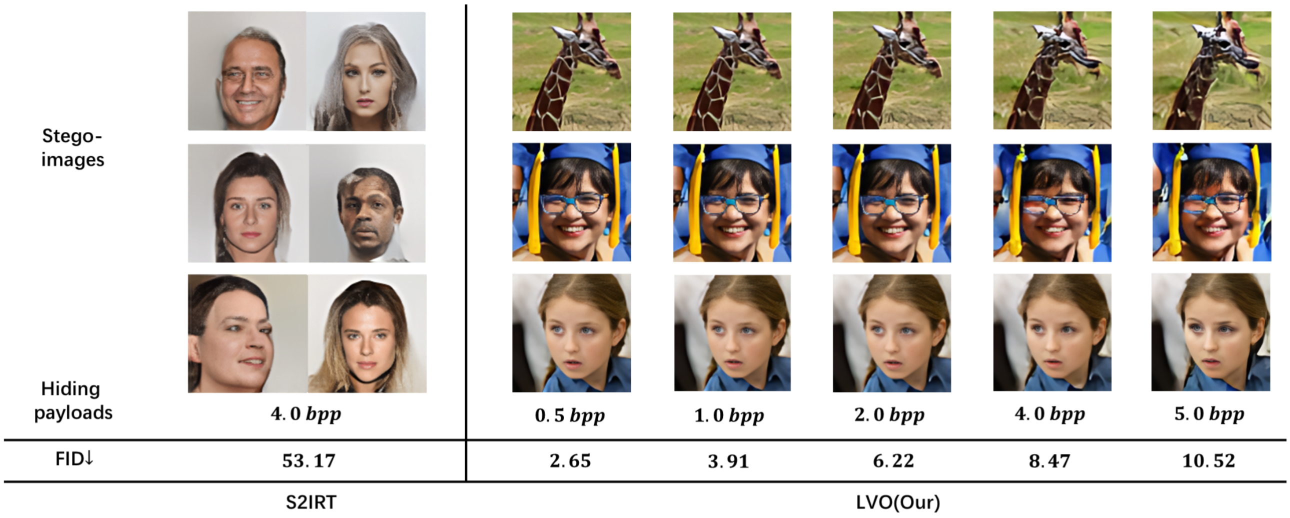

Fig. 3. Comparison of FID of stego-images generated by flow-based generative image steganographic approaches

TABLE II
THE P_E OF IMAGE STEGANOGRAPHIC APPROACHES WITH DIFFERENT HIDING PAYLOADS

	Approaches	Hiding payloads(*bpp*)				
		0.1	0.5	2.0	4.0	5.0
SRM [44]	S-UNIWARD	**0.451**	0.136	-	-	-
	SWE	0.266	-	-	-	-
	IDEAS	0.255	-	-	-	-
	S2IRT	0.263	0.273	0.289	**0.281**	0.280
	LVO(Our)	0.271	**0.290**	**2.295**	0.280	**0.299**
XuNet [7]	S-UNIWARD	**0.421**	0.120	-	-	-
	SWE	0.269	-	-	-	-
	IDEAS	0.279	-	-	-	-
	S2IRT	0.273	0.270	**0.288**	0.277	0.281
	LVO(Our)	0.271	**0.281**	2.275	**0.280**	**0.299**

*The larger the P_E means the better.

cells in the table, it indicates that the corresponding method does not achieve such a large hiding capacity. In comparison, the proposed GIS scheme can achieve a large hiding capacity.

The existing mainstream generative image steganography approaches, whether based on GANs or Flows, perform similarly in terms of security. This may be due to the similarity of the kernel of the process of generating images, where both of those apporaches map low-dimensional latent vectors into image space. Therefore, the steganalyzers' detection process is not significantly affected by different models. Moreover, since information does not exist solely in a specific area of the stego-image and has an impact across the entire image, the hiding capacity does not have a direct correlation with security. It can be seen that the anti-detectability of our LVO is almost independent of the hiding capacity. And it also shows the hiding capacity of the flow-based approaches is significantly larger than that of the GAN-based approaches.

We use the most common bits per pixel (*bpp*) to evaluate the information hiding ability and hiding capacity of steganographic approaches, which means the number of secret bits hidden in per pixel per channel of an image. It is defined as:

$$bpp = \frac{N_{Bit}}{W \times H \times C} \tag{8}$$

Where, the total number of hidden secret bits is noted as N_{Bit}, W, H, and C the width, the height, and the number of channels of the image, respectively.

Since the elements of each dimension of the latent vector z can be hidden into $7\,bit$ binary numbers, and the dimension of the latent vector is equal to the total dimension of the stego-image, the theoretical maximum hiding capacity of LVO is $7\,bpp$; However, in practice, when the hiding capacity is larger than $5\,bpp$, the stego-image quality decreases significantly because the elements of the latent vector which have high impact on the image quality are adjusted. The imperceptibility is decreased and the security of steganography is insufficient. The details can be found in the following sub-section D.

C. Security Evaluation by Stego-image Quality

Besides the anti-detectability of generative steganographic approaches to typical steganalysis tools, perceptual imperceptibility is very important for the security of steganography. The common image quality assessment criterion Fréchet Inception Distance (FID) [43] can effectively determine image quality and diversity, and can be used to determine the perceptual imperceptibility of stego-images. Table.IV lists the FID scores between real and stego-images of those generative steganographic approaches.

As shown in Table. IV, LVO-based GIS performs much better than the other approaches in all datasets, achieving the lowest FID scores, since LVO optimizes the latent vector. LVO-based GIS also has a larger hiding payload. Compared with another flow-based method S2IRT, LVO-based GIS has made great advance in stego-image quality, greatly improving the imperceptibility of flow-based generative image steganography and the security of generative image steganography. When the FID score is less than 10, the perceptibility of the

TABLE III
THE FID RESULTS OF STEGO-IMAGES OF GENERATIVE STEGANOGRAPHIC APPROACHES

Approaches(bpp)	Dataset				avg.±std.dev
	FFHQ	CelebA	COCO	LSUN	
SWE(0.1)	149.37	136.22	98.37	96.21	131.3±44.5
IDEAS(0.0026)	29.02	27.13	18.08	17.20	20.51±8.9
S2IRT(4.0)	62.59	54.22	89.21	49.99	55.61±32.2
Our					
LVO(2.0)	**7.89**	**6.22**	**9.12**	**8.25**	6.89±3.0
LVO(5.0)	9.91	9.15	12.25	9.65	9.66±3.12

*The lower the FID score means the better.

stego-image with the natural image is difficult to be detected visually, therefore, the steganographic image generated by LVO can have better security. Besides, the higher diversity of the COCO dataset compared to the face datasets FFHQ and CelebA results in lower generation performance of some approaches.

D. Stego-image Quality / Hiding Capacity Flexibility

Figure. 3 shows the stego-images of two flow-based generative image steganographic approaches, LVO-based GIS and S2IRT. The quality of the generated stego-images of our LVO-based GIS approach differs under different hiding payloads, but even with a high hiding payload of $5.0\,bpp$. The quality of our stego-images is very high, outperforming the other flow-based approach by a wide margin. The image quality of S2IRT is not influenced by the hiding payload, but the quality of some stego-images is particularly poor, and some the secret information will lead to poorly contained images, while our LVO can generate the stego-images with predictable quality.

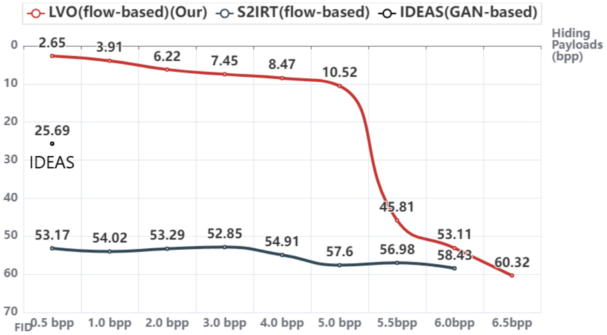

Fig. 4. The FID of the stego-images generated by several approaches under different hiding payloads

The line chart in Fig. 4 shows the image quality average FID scores of the stego-images generated by several approaches under different hiding payloads. Among them, the maximum hiding capacity of the GAN-based IDEAS approach is very small, and its FID is only used as a comparison. It can be seen that when the hiding payloads are very high ($>= 5.5\,bpp$), the quality of the stego-images generated by our approach decreases, because the perturbation of the elements in the latent vector z has a high degree of impact on the quality of the stego-images. Therefore, the effective hiding capacity of LVO-based GIS approach is about $5.0\,bpp$.

E. Extraction Accuracy

The extraction accuracy is an important metric of steganographic approaches, which determines whether the secret information can be delivered accurately. Table.IV gives the extraction accuracy results of the different generative steganographic approaches and their corresponding hiding capacities.

TABLE IV
THE INFORMATION EXTRACTION ACCURACY OF THOSE APPROACHES WITH DIFFERENT HIDING PAYLOADS

Approaches	Hiding payloads(bpp)				
	0.1	0.5	2.0	4.0	5.0
SWE	78.51%	71.89%	69.02%	-	-
IDEAS	96.23%	-	-	-	-
S2IRT	100%	100%	100%	99.48%	97.43%
LVO(Our)	100%	100%	100%	100%	100%

It is obvious that he extraction accuracy rates of LVO-based GIS keep at 100% when the hiding payload ranges from $0.1\,bpp$ to $5.0\,bpp$. The reason for this remarkable extraction accuracy is that the flow-based approaches are able to achieve a perfect reversible mapping between the latent vector and the stego-image, while the GAN-based approaches have difficulty in achieving 100% extraction rate. When the hiding payload exceeds $5.0\,bpp$, the extraction rate of the LVO method is slightly less than 100%. Among them, IDEAS and SWE have a very small hiding capacity, hence, some data cellsare empty in this table.

Although S2IRT is also a flow-based approach, it does not optimize the latent vector and uses position encoding to oper- ate on the latent vector, which causes the position information of a few dimensional elements to be lost in the case of high hiding payloads, resulting in the extraction rate less than 100% under high hiding payloads. In contrast, the proposed LVO-based GIS optimizes the latent vector without losing the information of the elements on all dimensions and can be perfectly reversible to achieve 100% extraction rate even under high hiding payloads.

V. CONCLUSION

The proposed LVO-based GIS scheme exhibits high stego-image quality with a large hiding capacity. It effectively overcomes the issues in the existing GIS schemes for consumer electronic applications. In the future, we will develop the proposed GIS to further improve the quality and diversity of generated stego-images in consumer electronic applications. For example, we can optimize the flow-based generation models to realize controllable generation of images with certain semantic information or explore the other image generation models (such as diffusion models) to generated stego-images for GIS.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCE.2024.3354824

REFERENCES

[1] Y. Yi, Z. Zhang, L. T. Yang, X. Wang, and C. Gan, "Edge-aided control dynamics for information diffusion in social internet of things," *Neurocomputing*, vol. 485, pp. 274–284, 2022.

[2] L. Ren, Y. Laili, X. Li, and X. Wang, "Coding-based large-scale task assignment for industrial edge intelligence," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, pp. 2286–2297, 2019.

[3] M. Zhao, H. Wang, Y. Han, X. Wang, H.-N. Dai, X. Sun, J. Zhang, and M. Pedersen, "Seens: Nuclei segmentation in pap smear images with selective edge enhancement," *Future Generation Computer Systems*, vol. 114, pp. 185–194, 2021.

[4] K. Doulani, A. Rajput, A. Hazra, M. Adhikari, and A. K. Singh, "Explainable ai for communicable disease prediction and sustainable living: Implications for consumer electronics," *IEEE Transactions on Consumer Electronics*, 2023.

[5] R. Patole, N. Singh, M. Adhikari, and A. K. Singh, "Multi-view ensemble federated learning for efficient prediction of consumer electronics applications in fog networks," *IEEE Transactions on Consumer Electronics*, 2023.

[6] P. Amrit, A. K. Singh, M. P. Singh, and A. K. Agrawal, "Embedr-net: Using cnn to embed mark with recovery through deep convolutional gan for secure ehealth systems," *IEEE Transactions on Consumer Electronics*, 2023.

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

[8] J. Fridrich and J. Kodovsky, "Rich models for steganalysis of digital images," *IEEE Transactions on information Forensics and Security*, vol. 7, no. 3, pp. 868–882, 2012.

[9] I. Avcibas, N. Memon, and B. Sankur, "Steganalysis using image quality metrics," *IEEE transactions on Image Processing*, vol. 12, no. 2, pp. 221–229, 2003.

[10] H. Shi, J. Dong, W. Wang, Y. Qian, and X. Zhang, "Ssgan: Secure steganography based on generative adversarial networks," in *Advances in Multimedia Information Processing–PCM 2017: 18th Pacific-Rim Conference on Multimedia, Harbin, China, September 28-29, 2017, Revised Selected Papers, Part I 18*. Springer, 2018, pp. 534–544.

[11] D. Volkhonskiy, I. Nazarov, and E. Burnaev, "Steganographic generative adversarial networks," in *Twelfth international conference on machine vision (ICMV 2019)*, vol. 11433. SPIE, 2020, pp. 991–1005.

[12] R. Zhang, S. Dong, and J. Liu, "Invisible steganography via generative adversarial networks," *Multimedia tools and applications*, vol. 78, pp. 8559–8575, 2019.

[13] C. Chu, A. Zhmoginov, and M. Sandler, "Cyclegan, a master of steganography," *arXiv preprint arXiv:1712.02950*, 2017.

[14] J. Li, K. Niu, L. Liao, L. Wang, J. Liu, Y. Lei, and M. Zhang, "A generative steganography method based on wgan-gp," in *Artificial Intelligence and Security: 6th International Conference, ICAIS 2020, Hohhot, China, July 17–20, 2020, Proceedings, Part I 6*. Springer, 2020, pp. 386–397.

[15] W. Tang, B. Li, S. Tan, M. Barni, and J. Huang, "Cnn-based adversarial embedding for image steganography," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 8, pp. 2074–2087, 2019.

[16] Y. Cao, Z. Zhou, Q. J. Wu, C. Yuan, and X. Sun, "Coverless information hiding based on the generation of anime characters," *EURASIP Journal on Image and Video Processing*, vol. 2020, pp. 1–15, 2020.

[17] C. Yu, D. Hu, S. Zheng, W. Jiang, M. Li, and Z.-q. Zhao, "An improved steganography without embedding based on attention gan," *Peer-to-Peer Networking and Applications*, vol. 14, pp. 1446–1457, 2021.

[18] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial networks," *Communications of the ACM*, vol. 63, no. 11, pp. 139–144, 2020.

[19] Z. Zhou, Y. Su, J. Li, K. Yu, Q. J. Wu, Z. Fu, and Y. Shi, "Secret-to-image reversible transformation for generative steganography," *IEEE Transactions on Dependable and Secure Computing*, 2022.

[20] S. Das, S. Das, B. Bandyopadhyay, and S. Sanyal, "Steganography and steganalysis: different approaches," *arXiv preprint arXiv:1111.3758*, 2011.

[21] J. Fridrich and M. Goljan, "Digital image steganography using stochastic modulation," in *Security and Watermarking of Multimedia Contents V*, vol. 5020. SPIE, 2003, pp. 191–202.

[22] K. Kordov and S. Zhelezov, "Steganography in color images with random order of pixel selection and encrypted text message embedding," *PeerJ Computer Science*, vol. 7, p. e380, 2021.

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

[24] X. Liu, Z. Ma, J. Ma, J. Zhang, G. Schaefer, and H. Fang, "Image disentanglement autoencoder for steganography without embedding," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2022, pp. 2303–2312.

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

[26] A. Radford, L. Metz, and S. Chintala, "Unsupervised representation learning with deep convolutional generative adversarial networks," *arXiv preprint arXiv:1511.06434*, 2015.

[27] H. Liu, Y. Xu, and F. Chen, "Sketch2photo: Synthesizing photo-realistic images from sketches via global contexts," *Engineering Applications of Artificial Intelligence*, vol. 117, p. 105608, 2023.

[28] H. Xu, Q. Li, and J. Chen, "Highlight removal from a single grayscale image using attentive gan," *Applied Artificial Intelligence*, vol. 36, no. 1, p. 1988441, 2022.

[29] M. Singh, N. Baranwal, K. N. Singh, and A. K. Singh, "Using gan-based encryption to secure digital images with reconstruction through customized super resolution network," *IEEE Transactions on Consumer Electronics*, 2023.

[30] D. P. Kingma and P. Dhariwal, "Glow: Generative flow with invertible 1x1 convolutions," *Advances in neural information processing systems*, vol. 31, 2018.

[31] L. Li, M. S. Hossain, A. A. A. El-Latif, and M. F. Alhamid, "Distortion less secret image sharing scheme for internet of things system," *Cluster Computing*, vol. 22, pp. 2293–2307, 2019.

[32] J. Huang, Q. Cui, Z. Zhou, K. Yu, C.-N. Yang, and K.-K. R. Choo, "Encrypted domain secret medical-image sharing with secure outsourcing computation in iot environment," *IEEE Internet of Things Journal*, 2023.

[33] Z. Zhou, Y. Wan, Q. Cui, K. Yu, S. Mumtaz, C.-N. Yang, and M. Guizani, "Blockchain-based secure and efficient secret image sharing with outsourcing computation in wireless networks," *IEEE Transactions on Wireless Communications*, 2023.

[34] L. Xiong, X. Han, X. Zhong, C.-N. Yang, and N. N. Xiong, "Rsis: A secure and reliable secret image sharing system based on extended hamming codes in industrial internet of things," *IEEE Internet of Things Journal*, vol. 10, no. 3, pp. 1933–1945, 2021.

[35] W. Wu, H. Peng, F. Tong, and L. Li, "A chaotic compressed sensing-based multigroup secret image sharing method for iot with critical information concealment function," *IEEE Internet of Things Journal*, vol. 10, no. 2, pp. 1192–1207, 2022.

[36] Z. Zhou, C.-N. Yang, Y. Cao, and X. Sun, "Secret image sharing based on encrypted pixels," *IEEE Access*, vol. 6, pp. 15 021–15 025, 2018.

[37] H. Li, Q. Huang, J. Huang, and W. Susilo, "Public-key authenticated encryption with keyword search supporting constant trapdoor generation and fast search," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 396–410, 2022.

[38] L. Dinh, J. Sohl-Dickstein, and S. Bengio, "Density estimation using real nvp," *arXiv preprint arXiv:1605.08803*, 2016.

[39] T. Karras, S. Laine, and T. Aila, "A style-based generator architecture for generative adversarial networks," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2019, pp. 4401–4410.

[40] T. Karras, T. Aila, S. Laine, and J. Lehtinen, "Progressive growing of gans for improved quality, stability, and variation," *arXiv preprint arXiv:1710.10196*, 2017.

[41] T.-Y. Lin, M. Maire, S. Belongie, J. Hays, P. Perona, D. Ramanan, P. Dollár, and C. L. Zitnick, "Microsoft coco: Common objects in context," in *Computer Vision–ECCV 2014: 13th European Conference, Zurich, Switzerland, September 6-12, 2014, Proceedings, Part V 13*. Springer, 2014, pp. 740–755.

[42] 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," *arXiv preprint arXiv:1506.03365*, 2015.

[43] 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,” *Advances in neural information processing systems*, vol. 30, 2017.

[44] Y. Qian, J. Dong, W. Wang, and T. Tan, “Learning and transferring representations for image steganalysis using convolutional neural network,” in *2016 IEEE international conference on image processing (ICIP)*. Ieee, 2016, pp. 2752–2756.

[45] V. Holub, J. Fridrich, and T. Denemark, “Universal distortion function for steganography in an arbitrary domain,” *EURASIP Journal on Information Security*, vol. 2014, pp. 1–13, 2014.

Zhili Zhou(SM’23) received his MS and PhD degrees in Computer Application at the School of Information Science and Engineering from Hunan University, in 2010 and 2014, respectively. He is currently a professor with Institute of Artificial Intelligence, Guangzhou University. Also, he was a Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Windsor, Canada. His current research interests include Multimedia Security, Artificial Intelligence Security and Information Hiding. He has authored or coauthored more than 130 refereed papers. He is serving as an Associate Editor of Journal of Real-Time Image Processing, Security and Communication Networks, International Journal on Semantic Web and Information Systems, CMC-Computers Materials & Continua, and Big Data Mining and Analytics. He has been selected as “World’s Top 2% Scientists” from 2020 to 2023 by Stanford University and Elsevier. He received ACM Rising Star Award and got Guangdong Natural Science Funds for Distinguished Young Scholar.

Zhipeng Bao was a graduate student. He is currently pursuing the M.S. degree with the Nanjing University of Information Science and Technology, China, in 2021. His research interests include steganography and information security.

Weiwei Jiang (M’19) received the B.Sc. and Ph.D. degrees from the Department of Electronic Engineering, Tsinghua University, Beijing, China, in 2013 and 2018, respectively. He is currently an assistant professor with the School of Information and Communication Engineering, Beijing University of Posts and Telecommunications. His current research interests include artificial intelligence for networking and communication, satellite communication and smart grid communication.

Yuan Huang received the titles of senior technician of reactor control and protection and senior engineer at China National Nuclear Corporation (CNNC), in 2021 and 2022 respectively. He also obtained the INCOSE certified system engineer in 2022. He is currently the director of the AI R&D Center at CNNC Equipment Technology Development Co., Ltd. Also, he is an international youth talent of CNNC and a talent of the second batch of ”Hundred Talents Plan” of Jiaxing City, Zhejiang Province. He has been engaged in nuclear power front-line work for 10 years, presided over multiple company-level major research projects, won the top 100 of the Central Enterprise Innovation Competition of SASAC, applied/authorized 21 patents and software copyrights, and won 8 national and provincial honors or above. He led the team to develop the first domestic nuclear industry large language model ”Dragon Says”, built the industry’s first digital productivity platform based on LLMs, and applied multiple LLM applications in the nuclear industry, with the aim of leading the digital intelligence transformation of nuclear industry with digital productivity.

Dr. Yun Peng received the Ph.D, MPhil, and BSc degrees in computer science from Hong Kong Baptist University (HKBU), Harbin Institute of Technology (HIT), and Shandong University (SDU) in 2013, 2008 and 2006, respectively. He currently is a Professor of the Institute of Artificial Intelligence at Guangzhou University. His research interests include graph databases, vector databases, and privacy computing. He has published several papers in top-tier conferences and journals, including SIGMOD, VLDB, VLDBJ, and TKDE. He has served as the program committee member of ICDE, IJCAI and DASFAA, and the reviewer of TKDE and IJIS, etc.

Dr. Achyut Shankar is currently working as a Postdoc Research Fellow at University of Warwick, United Kingdom and recently appointed as visiting Associate Professor at University of Johannesburg, South Africa. He obtained his PhD in Computer Science and Engineering majoring in wireless sensor network from VIT University, Vellore, India. He was at Birkbeck University, London from Jan 2022 to May 2022 for his research work. He has published more than 90 research papers in reputed international conferences & journals in which 65 papers are in SCIE journals. He is a member of ACM and has received research award for excellence in research for the year 2016 and 2017. He had organized many special sessions with Scopus Indexed International Conferences worldwide, proceedings of which were published by Springer, IEEE, Elsevier etc. He is currently serving as an Associate Editor in SAIEE Africa Research Journal(IEEE), Scientific Reports(Nature Journal, Q1), Human- Centric Computing and Information Sciences & SN applied sciences(SCOPUS & ESCI, Springer) and in year 2021 and 2022 handing few special issues as a Guest editor ACM transaction for TALIP, International Journal of Human Computer Interaction(Taylor and Francis) , International Journal of System Assurance Engineering and Management(Springer) and Journal of Interconnection networks(World Scientific journals). He is serving as reviewer of IEEE Transactions on Intelligent Transportation Systems, IEEE Sensors Journal, IEEE Internet of Things Journal, ACM Transactions on Asian and Low-Resource Language Information Processing and other prestigious conferences. His areas of interest include Wireless sensor network, Machine Learning, Internet of Thing, Block-chain and Cloud computing.

Professor Carsten Maple leads the Secure Cyber Systems Research Group in WMG at the University of Warwick, where he is also the Principal Investigator of the NCSC-EPSRC Academic Centre of Excellence in Cyber Security Research. He is a co-investigator of the PETRAS National Centre of Excellence for IoT Systems Cybersecurity where he leads on Transport & Mobility and Warwick PI on the Autotrust project. Carsten has an international research reputation and extensive experience of institutional strategy development and interacting with external agencies. He has published over 250 peer-reviewed papers and is co-author of the UK Security Breach Investigations Report 2010, supported by the Serious Organised Crime Agency and the Police Central e-crime Unit. Additionally he has advised executive and non-executive directors of public sector organisations and multibillion pound private organisations. Professor Maple is a past Chair of the Council of Professors and Heads of Computing in the UK, a member of the Zenzic Strategic Advisory Board, a member of the IoTSF Executive Steering Board, an executive committee member of the EPSRC RAS Network and a member of the UK Computing Research Committee, the ENISA CarSEC expert group, the Interpol Car Cybercrime Expert group and Europol European Cybercrime Centre.

Dr S. Shitharth completed his PhD in the Department of Computers Science & Engineering, Anna University. He completed his Postdoc at The University of Essex, Colchester, UK. He has worked in various institutions with a teaching experience of seven years. Now, he is working as a lecturer in cyber security at Leeds Beckett University, Leeds, UK. He has published in more than 85 International Journals and 20 International & National conferences. He has even published four patents in IPR. He is also an active member of IEEE Computer Society and five more professional bodies. He is also a member of the International Blockchain organization. He is a certified hyperledger expert and certified blockchain developer. His current research interests include Cyber Security, Blockchain, Critical Infrastructure & Systems, Network Security & Ethical Hacking. He is an active researcher, reviewer and editor for many international journals.