Large-capacity and Flexible Video Steganography via Invertible Neural Network

Chong Mou¹, Youmin Xu¹, Jiechong Song¹, Chen Zhao², Bernard Ghanem², Jian Zhang¹,³,∗
¹Peking University Shenzhen Graduate School, Shenzhen, China
²King Abdullah University of Science and Technology (KAUST), Thuwal, Saudi Arabia
³Peng Cheng Laboratory, Shenzhen, China
{eechongm, youmin.xu}@stu.pku.edu.cn; {songjiechong, zhangjian.sz}@pku.edu.cn;
{chen.zhao, Bernard.Ghanem}@kaust.edu.sa

Abstract

Video steganography is the art of unobtrusively concealing secret data in a cover video and then recovering the secret data through a decoding protocol at the receiver end. Although several attempts have been made, most of them are limited to low-capacity and fixed steganography. To rectify these weaknesses, we propose a Large-capacity and Flexible Video Steganography Network (LF-VSN) in this paper. For large-capacity, we present a reversible pipeline to perform multiple videos hiding and recovering through a single invertible neural network (INN). Our method can hide/recover 7 secret videos in/from 1 cover video with promising performance. For flexibility, we propose a key-controllable scheme, enabling different receivers to recover particular secret videos from the same cover video through specific keys. Moreover, we further improve the flexibility by proposing a scalable strategy in multiple videos hiding, which can hide variable numbers of secret videos in a cover video with a single model and a single training session. Extensive experiments demonstrate that with the significant improvement of the video steganography performance, our proposed LF-VSN has high security, large hiding capacity, and flexibility. The source code is available at https://github.com/MC-E/LF-VSN.

1. Introduction

Steganography [10] is the technology of hiding some secret data into an inconspicuous cover medium to generate a stego output, which only allows the authorized receiver to recover the secret information. Unauthorized people can only access the content of the plain cover medium, and hard

to detect the existence of secret data. In the current digital world, image and video are commonly used covers, widely applied in digital communication [27], copyright protection [36], information certification [31], e-commerce [26], and many other practical fields [10, 12].

Traditional video steganography methods usually hide messages in the spatial domain or transform domain by manual design. Video steganography in the spatial domain means embedding is done directly to the pixel values of video frames. Least significant bits (LSB) [8, 45] is the most well-known spatial-domain method, replacing the n least significant bits of the cover image with the most significant n bits of the secret data. Many researchers have used LSB replacement [6] and LSB matching [34] for video steganography. The transform-domain hiding [5, 17, 39] is done by modifying certain frequency coefficients of the transformed frames. For instance, [44] proposed a video steganography technique by manipulating the quantized coefficients of DCT (Discrete Cosine Transformation). [9] proposed to compare the DWT (Discrete Wavelet Transformation) coefficients of the secret image and the cover video for hiding. However, these traditional methods have low hiding capacity and invisibility, easily being cracked by steganalysis methods [15, 28, 33].

Recently, some deep-learning methods were proposed to improve the hiding capacity and performance. Early works are presented in image steganography. Baluja [3, 4] proposed the first deep-learning method to hide a full-size image into another image. Recently, [21, 32] proposed designing the steganography model as an invertible neural network (INN) [13, 14] to perform image hiding and recovering with a single model. For video steganography, Khare et al. [22] first utilized back propagation neural networks to improve the performance of the LSB-based scheme. [43] is the first deep-learning method to hide a video into another video. Unfortunately, it simply aims to hide the residual across adjacent frames in a frame-by-frame manner, and it requires several separate steps to complete the video hiding and re-
covering. [35] utilize 3D-CNN to explore the temporal correlation in video hiding. However, it utilizes two separated 3D UNet to perform hiding and recovering, and it has high model complexity (367.2 million parameters). While video steganography has achieved impressive success in terms of hiding capacity to hide a full-size video, the more challenging multiple videos hiding has hardly been studied. Also, the steganography pipeline is rigid.

In this paper, we study the large-capacity and flexible video steganography, as shown in Fig. 1. Concretely, we propose a reversible video steganography pipeline, achieving large capacity to hide/recover multiple secret videos in/from a cover video. At the same time, our model complexity is also attractive by combining several weight-sharing designs. The flexibility of our method is twofold. First, we propose a key-controllable scheme, enabling different receivers to recover particular secret videos with specific keys. Second, we propose a scalable strategy, which can hide variable numbers of secret videos into a cover video with a single model and a single training session. To summarize, this work has the following contributions:

- We propose a large-capacity video steganography method, which can hide/recover multiple (up to 7) secret videos in/from a cover video. Our hiding and recovering are fully reversible via a single INN.
- We propose a key-controllable scheme with which different receivers can recover particular secret videos from the same cover video via specific keys.
- We propose a scalable embedding module, utilizing a single model and a single training session to satisfy different requirements for the number of secret videos hidden in a cover video.
- Extensive experiments demonstrate that our proposed method achieves state-of-the-art performance with large hiding capacity and flexibility.

2. Related Work

2.1. Video Steganography

Steganography can date back to the 15th century, whose goal is to encode a secret message in some transport mediums and covertly communicate with a potential receiver who knows the decoding protocol to recover the secret message. Since the human visual system is less sensitive to small changes in digital media, especially digital videos. Video steganography is becoming an important research area in various data-hiding technologies [10].

Traditional video steganography methods usually performed hiding and recovering in the spatial domain, e.g., Pixel Value Differencing (PVD) [20, 40] and Least Significant Bits (LSB) [6, 34, 41]. PVD embeds the secret data in the difference value of two adjacent pixels. In [40], a PVD-based video steganography system is proposed to embed the secret data in a compressed domain of the cover medium. [20] utilized enhanced pixel-value differencing (EPVD) to improve the video steganography performance. LSB methods work by replacing the n least significant bits of the cover data with the most significant n bits of the secret information. [41] utilized LSB replacement technique to hide secret text in grayscale video frames. To enhance the security in LSB-based methods, [2] shuffled the secret data and embedded the index of correct order into the cover video. In addition to spatial-domain methods, some transformed domain methods [9, 44] were proposed to perform hiding by modifying certain frequency coefficients of the transformed cover video. For instance, [44] proposed a video steganography technique by manipulating the quantized coefficients
of DCT transformation. [9] proposed to compare the DWT transformation coefficients of the secret image and the cover video for hiding. Nevertheless, the above traditional methods have low hiding capacity and invisibility, easily producing artificial markings and being cracked by steganalysis methods [15, 28, 33].

Motivated by the success of deep learning, some deep-learning methods were proposed. [16] introduced GAN to steganography, showing that the adversarial training scheme can improve hiding security. [49] improve the hiding quality by utilizing two independent adversarial networks to critique the video quality and optimize for robustness. [25] studied the lossless steganography below 3 bits per pixel (bpp) hiding. [38] embedded the secret data in the wavelet transform coefficients of the video frames. The above methods focus more on the robustness of low-capacity hiding. One of the important applications of low-capacity steganography is watermarking [1, 42, 52], in which the secret bit string represents the sign of the owner. Some deep-learning methods were proposed for large-capacity hiding. [3, 4] first explored hiding a full-size image into another image. [21, 32] proposed a cheaper pipeline by implementing image hiding and recovering with a single invertible neural network (INN) [13, 14]. Compared with image hiding, video hiding is a more challenging task, requiring a larger hiding capacity. [43] first studied to hide/recover a video in/from another video. However, this method simply hides the residual across adjacent frames in a frame-by-frame manner. [35] explores the temporal correlation by 3D CNN in video steganography. However, it utilizes two separate 3D UNet to perform hiding and recovering and has high model complexity (367.2M model parameters). These previous works demonstrate that deep networks have great potential in video hiding, inspiring us to study the more challenging task of multiple and flexible video hiding.

2.2. Invertible Neural Network

Since the concept of invertible neural network (INN) was proposed in [13, 14], INN has attracted more and more attention due to its pure invertible pipeline. Pioneering research on INN can be seen in image generation tasks. For instance, Glow [24] utilized INN to construct an invertible mapping between the latent variable z and nature images x. Specifically, the generative process x = fθ(z) given a latent variable can be specified by an INN architecture fθ. The direct access to the inverse mapping z = fθ−1(x) makes inference much cheaper. Up to now, INN has been studied in several vision tasks (e.g., image rescaling [19, 46], image restoration [29, 30], image coloring [51], and video temporal action localization [50]) and presents promising performance.

The architecture of INN needs to be carefully designed to guarantee the invertibility. Commonly, INN is composed of several invertible blocks, e.g., the coupling layer [13]. Given the input h, the coupling layer first splits h into two parts (h1 and h2) along the channel axis. Then they undergo the affine transformations with the affine parameters generated by each other:

\[
\begin{align*}
\hat{h}_1 &= h_1 \cdot \psi_1(h_2) + \phi_1(h_2) \\
\hat{h}_2 &= h_2 \cdot \psi_2(h_1) + \phi_2(h_1),
\end{align*}
\]

where \(\psi(\cdot)\) and \(\phi(\cdot)\) are arbitrary functions. \(\hat{h}_1\) and \(\hat{h}_2\) are the outputs of the coupling layer. Correspondingly, the inverse process is defined as:

\[
\begin{align*}
h_1 &= \frac{\hat{h}_1 - \phi_1(h_2)}{\psi_1(h_2)}; \\
h_2 &= \frac{\hat{h}_2 - \phi_2(h_1)}{\psi_2(h_1)}.
\end{align*}
\]

In this paper, we employ the reversible forward and backward processes of INN to perform multiple videos hiding and recovering, respectively. We further improve INN to explore flexible video steganography.

3. Methodology

3.1. Overview

An overview of our LF-VSN is presented in Fig. 2. Specifically, given \(N_s\) secret videos \(x_{se} = \{x_{se}(n)|n\}_{n=1}^{N_s}\) and a cover video \(x_{co}\), the forward hiding is operated group-by-group through a sliding window, traversing each video from head to tail. After hiding, a stego video \(x_{st}\) is produced, ostensibly indistinguishable from \(x_{co}\) to ensure that \(x_{se}\) is undetectable. In the backward recovering, a channel-wise broadcasting operation \((\mathbb{R}^{3\\times\\times W \\
H \\
H} \xrightarrow{cop} \mathbb{R}^{3\\times\\times W \\
H})\) copies each stego frame in the channel dimension to form the reversed input. During recovering, multiple secret videos are recovered frame-by-frame in parallel. It is worth noting that the forward hiding and backward recovering share the same model architecture and parameters.

3.2. Steganography Input and Output Design

At the beginning of each hiding step, a fusion module is applied to fuse frames in each group to take advantage of the inner temporal correlation. Considering that it is easy to produce texture artifacts and color distortion when hiding in the spatial dimension [15, 21], we perform the fusion by a frequency concatenation. Specifically, given the \(j\)-th cover group \(X_{co@j} \in \mathbb{R}^{L\\times\\times W \\
H}\) and secret groups \(\{X_{se@j}(n) \in \mathbb{R}^{L\\times\\times W \\
H}\}_{n=1}^{N_s}\) (each contains \(L\) frames), we adopt Haar discrete wavelet transform (DWT) to split each frame into four frequency bands (i.e., LL, HL, LH, HH). In each frame group, we concatenate the part in the same frequency band from different frames in the channel dimension and then concatenate these four bands in order of frequency magnitude, producing the final secret input \(\{X_{se@j}(n) \in \mathbb{R}^{12\\\\times W \\
H}\}_{n=1}^{N_s}\) and cover input \(X_{co@j} \in \mathbb{R}^{12\\\\times W \\
H}\). The output of the forward
hiding comprises a stego group $X_{se \otimes j}$ and several redundancy groups $\{X_{re \otimes j}(n)\}_{n=1}^{N_s}$. $X_{se \otimes j}$ is converted from the frequency domain to the spatial domain by a frequency separation, i.e., the inverse of the frequency concatenation. $X_{re \otimes j}(n)$ represents the redundancy of the $X_{se \otimes j}(n)$ that does not need to be hidden and will be discarded. In our LF-VSN, we utilize the adjacent frames to cooperate with hiding the central frame. Thus, we only output the central stego frame in each hiding step. The backward recovering is similarly operated in the frequency domain and converted to the spatial domain at the output.

### 3.3. Invertible Block

As shown in Fig. 2, our hiding and recovering have reverse information flow constructed by several invertible blocks (IBs). The architecture of IB is presented in Fig. 3. Concretely, in the $k$-th IB, there are two branches to process the input cover group $X_{co \otimes j}^k$ and secret groups $\{X_{se \otimes j}(n)\}_{n=1}^{N_s}$, respectively. Several interaction pathways between these two branches construct the invertible projection. We use an additive transformation to project the cover branch and employ an enhanced affine transformation to project the secret branch. The transformation parameters are generated from each other. Here we utilize weight-sharing modules ($\eta_k(\cdot)$ and $\phi_k(\cdot)$) to extract features from all secret groups, producing a feature set $\{F_{se}(n)\}_{n=1}^{N_s} = \{\eta_k(X_{se \otimes j}(n))\}_{n=1}^{N_s}$, $\eta_k(\cdot)$ and $\phi_k(\cdot)$ ($i = 1, 2, 3$) refer to a $3 \times 3$ convolution layer and a five-layer dense block [18], respectively. Then, we concatenate $F_{se}$ in the channel dimension and pass through an aggregation module $\xi_k(\cdot)$ to generate the transformation parameters of the cover branch. Note that $\xi_k(\cdot)$ is optional in different cases. In our fixed hiding, $\xi_k(\cdot)$ is a $3 \times 3$ convolution layer, and it is a scalable embedding module in our scalable hiding. The transformation parameters of the secret branch are generated from $X_{co \otimes j}^k$ and shared among different secret groups. Thus, in the $k$-th invertible block, the bijection of the forward propagation in Eq. (1) is reformulated as:

$$
X_{co \otimes j}^{k+1} = X_{co \otimes j}^k + \xi_k(||\phi^1_k(\eta^1_k(X_{se \otimes j}(n)))||_{n=1}^{N_s}) \\
\{X_{se \otimes j}(n)\}_{n=1}^{N_s} = X_{co \otimes j}^k \ast \exp(\phi^2_k(\eta^2_k(X_{co \otimes j}^k))) + \phi^3_k(\eta^3_k(X_{co \otimes j}^{k+1})),
$$

where $|| \cdot ||$ refers to the channel-wise concatenation. $\exp(\cdot)$ is the Exponential function. Accordingly, the backward propagation is defined as:

$$
\{X_{se \otimes j}(n)\}_{n=1}^{N_s} = X_{co \otimes j}^{k+1} - \xi_k(||\phi^1_k(\eta^1_k(X_{se \otimes j}(n)))||_{n=1}^{N_s}).
$$

Figure 2. Network architecture of our LF-VSN. It is composed of several invertible blocks. In the forward hiding process, multiple secret videos are hidden in a cover video to generate a stego video, together with redundancy. In the backward recovering process, the stego video and predicted redundancy are fed to the reverse data flow of the same network with the same parameters to recover secret videos.

Figure 3. Illustration of the architecture of our invertible block. The dashed line refers to weight sharing.
3.4. Redundancy Prediction Module (RPM) & Key-controllable Design

As illustrated previously, we retain the stego part and discard the redundancy information in the forward hiding. Therefore, we need to prepare a suitable redundancy in the backward process to utilize the reversibility of INN to reconstruct the forward input (i.e., secret and cover). In different tasks, most INN-based methods [21,24,32,46] constrain the generated redundancy information to obey the Gaussian distribution and utilize random Gaussian sampling to approximate this part in the backward process. Nevertheless, such random sampling lacks data specificity and adaptivity. In our LF-VSN, we predict the redundancy information from the stego group through a redundancy prediction module (RPM), as shown in Fig. 4(a). It is composed of several residual blocks (RB) without the Batch Normalization layer.

In this paper, we present a novel extension of RPM to construct key-controllable video steganography, with which we can hide multiple secret videos in a cover video and recover a secret video conditioned on a specific key. The architecture is shown in Fig. 4(b). Given the index \(n_{key}\) of a secret video \(X_{se}(n_{key})\), a specific key is generated by a key encoder, which is composed of several fully connected (FC) layers. The key is then fed into a FC layer at the end of each RB in RPM to generate a condition vector with \(2C_{rpm}\) channels, which is divided into two modulation vectors \(\alpha, \beta \in \mathbb{R}^{C_{rpm} \times 1 \times 1}\) in the channel dimension. \(C_{rpm}\) is the feature channel of each RB in RPM. Then we modulate the output feature \(F_{rpm}\) of each RB as \(F_{rpm} \cdot \alpha + \beta\). In the training process, we constrain the recovered output the same as the \(n_{key}\)-th secret video (i.e., \(X_{se}(n_{key})\)). More details can be found in Sec. 3.6.

3.5. Scalable Embedding Module

The scalable design is used to handle the case where there are different requirements for the number of secret videos hidden in a cover video. It is succinctly designed on the feature aggregation part \(E_k(\cdot)\) in each IB, as shown in Fig. 3. The illustration of our scalable embedding module is presented in Fig. 5. It can be regarded as a special convolution layer, whose dimension of the convolution kernel can be changed according to the input. All convolution kernels \(\mathbf{M}\) with different dimensions are parameter-shared from the same base kernel \(\mathbf{M}\). Technically, given the input feature \(F_{in} \in \mathbb{R}^{C_{in} \times W \times H}\), we truncate a convolution kernel \(\mathbf{M} \in \mathbb{R}^{C_{in} \times C_{out} \times k \times k}\) from \(\mathbf{M} \in \mathbb{R}^{C \times C_{out} \times k \times k}\) to match the input dimension and then perform convolution: \(F_{out} = \mathbf{M} \ast F_{in}\). In this way, the training of \(\mathbf{M}\) is completed through the training of all sub-kernels \(\mathbf{M}\).

3.6. Loss Function

In our LF-VSN, the loss function is used to constrain two parts, i.e., forward hiding and backward recovering. The forward hiding is to hide multiple secret videos in the cover video. The generated stego video \(X_{st}\) should be undetectable to secret videos and as similar as possible to the cover video. Therefore, we constrain \(X_{st}\) to be the same as the cover video \(X_{co}\):

\[
\mathcal{L}_f = ||X_{st}[I_c] - X_{co}[I_c]||_2^2,
\]

where \(|| \cdot ||_2^2\) donates the \(L_2\) norm. \(I_c\) is the index of the central frame in each group. In the backward recovering, there are two patterns: with and without key controlling. In both patterns, we aim to recover the secret information from the cover video. The difference stands between recovering a specific secret video and all secret videos. In the pattern without key controlling, the loss function is defined as:

\[
\mathcal{L}_b = \sum_{n=1}^{N_c} \left( ||X_{se@j}(n)[I_c] - X_{se@j}(n)[I_c]||_2^2 + ||X_{co@j}[I_c] - X_{co@j}[I_c]||_2^2 \right),
\]
Table 1. Quantitative comparison (PSNR/SSIM) on Vimeo-T200. The best and second-best results are highlighted and underlined. Our LF-VSN achieves the best performance in stego and secret quality with acceptable complexity.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Stego</td>
<td>29.43/0.862</td>
<td>34.14/0.860</td>
<td>42.08/0.965</td>
<td>42.09/0.962</td>
<td>43.50/0.951</td>
<td>-</td>
<td><strong>45.17/0.980</strong></td>
</tr>
<tr>
<td>Secret</td>
<td>32.08/0.899</td>
<td>35.21/0.931</td>
<td>42.11/0.984</td>
<td>44.44/0.991</td>
<td>44.08/0.964</td>
<td>36.48/0.939</td>
<td><strong>48.39/0.996</strong></td>
</tr>
<tr>
<td>Params.</td>
<td>42.57M</td>
<td>2.65M</td>
<td>3.00M</td>
<td>4.05M</td>
<td>8.15M</td>
<td>0.67M</td>
<td><strong>7.40M</strong></td>
</tr>
</tbody>
</table>

Figure 6. Visual comparison between our LF-VSN, ISN [32], and PIH [11] in 4 videos Steganography. We present the secret reconstruction results of video 2 and video 4. Our LF-VSN produces better result with intact color and details.

Figure 7. Visualization of our LF-VSN in 7 videos steganography, showing promising performance in such an extreme case.

where \(\hat{X}_{se}\) and \(\hat{X}_{co}\) represent the recovered secret and cover videos. In the pattern with key controlling, the loss function is defined to guarantee that the key generated from the video index \(n_{key}\) can only recover the \(n_{key}\)-th secret video. Thus, the loss function is reformulated as:

\[
L_b = \frac{1}{N_s} \sum_{n=1}^{N_s} \| \hat{X}_{se\oplus j}(n)[I_c] - X_{se\oplus j}(n_{key})[I_c]\|^2 + \\
\| \hat{X}_{co\oplus j}[I_c] - X_{co\oplus j}[I_c]\|^2,
\]

(7)

We optimize our LF-VSN by minimizing the forward loss function \(L_f\) and backward loss function \(L_b\) as:

\[
L = L_f + \lambda L_b,
\]

(8)

where \(\lambda\) is a hyper-parameter to make a trade-off between forward hiding and backward recovering. We set \(\lambda = 4\) to balance these two loss portions.

4. Experiment

4.1. Implementation Details

In this work, we adopt the training set of Vimeo-90K [48] to train our LF-VSN. Each sequence has a fixed spatial resolution of 448 × 256. During training, we randomly crop training videos to 144 × 144 with random horizontal and vertical flipping to make a data augmentation. We use Adam optimizer [23], with \(\beta_1 = 0.9\), \(\beta_2 = 0.5\). We set the batch size as 16. The weight decay factor is set as \(1 \times 10^{-12}\). We use an initial learning rate of \(1 \times 10^{-4}\), which will decrease by half for every 30K iterations. The number of total iterations is set as 250K. The training process can be completed on one NVIDIA Tesla V100 GPU within 3 days. For testing, we select 200 sequences from the testing set of Vimeo-90K, denoted as Vimeo-T200 in this paper.

4.2. Comparison Against Other Methods

Here we compare our LF-VSN with other methods on single video steganography and challenging multiple videos steganography. The evaluation includes the stego quality in forward hiding and the secret quality in backward recovering. For single video steganography, we compare our LF-VSN with some well-known methods [4, 43] and recent proposed methods [11, 21, 32, 47]. Note that PIH [11] highlighted the need to quantize the stego image from the floating-point format of 32 × 3 to 8 × 3 bits per pixel. But PIH just added the quantization to the compared methods without retraining. Here we retrain HiNet [21] with...
Table 2. Multiple videos steganography comparison (PSNR) of our LF-VSN, ISN [32], and PIH [11] on Vimeo-T200 test set. Our LF-VSN can hide/recover 7 videos with promising performance.

<table>
<thead>
<tr>
<th>Num. videos</th>
<th>ISN</th>
<th>Stego</th>
<th>Secret</th>
<th>PIH</th>
<th>Stego</th>
<th>Secret</th>
<th>Ours</th>
<th>Stego</th>
<th>Secret</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
<td>37.60</td>
<td>36.41</td>
<td>32.56</td>
<td>31.46</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>41.47</td>
<td>38.76</td>
<td>33.42</td>
<td>33.39</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>38.55</td>
<td>37.55</td>
<td>35.67</td>
<td>35.01</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>37.55</td>
<td>34.96</td>
<td>34.20</td>
<td>-</td>
<td>35.95</td>
<td>34.96</td>
<td>-</td>
<td>34.20</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>34.20</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>34.96</td>
<td>-</td>
<td>34.20</td>
<td>-</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>34.20</td>
<td>-</td>
<td>34.20</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Table 3. Performance comparison between controllable (C) and non-controllable (NC) video steganography of our LF-VSN.

<table>
<thead>
<tr>
<th>Num. videos</th>
<th>2</th>
<th>4</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISN (NC/C)</td>
<td>40.97/38.67</td>
<td>37.55/34.41</td>
<td>35.68/30.48</td>
</tr>
<tr>
<td>Secret (NC/C)</td>
<td>44.24/41.04</td>
<td>40.21/37.15</td>
<td>36.94/31.95</td>
</tr>
</tbody>
</table>

Figure 9. Performance comparison between our scalable and fixed design in multiple videos steganography.

In this paper, we present a key-controllable scheme in multiple videos steganography. It enables different receivers to recover particular secret videos through specific keys. The comparison in Tab. 3 presents that our controllable scheme still has a large hiding capacity (up to 6 videos) with attractive performance (> 30dB). The visualization of recovering quality is presented in the second row of Fig. 8, showing the high-quality and key-controllable results of our LF-VSN in multiple videos steganography.

We also study the security of our controlling scheme, i.e., the key is sensitive and model-specific. Here we take two sets of parameters, producing from the 250K and 240K iterations in the same training process. We use the key produced by one model (*) to recover the secret video hidden by another. The result in the third row of Fig. 8 presents that the wrong key has no controlling and recovering ability. Thus, our key-controllable scheme not only has the controlling function but also enhances data security.

4.4. Scalable Video Steganography

In this paper, we present a scalable scheme in multiple videos steganography. It can hide a variable number of secret videos into a cover video with a single model. We evaluate the performance of our scalable design and compare it with the fixed version in Tab. 9. Obviously, our method has an attractive performance (> 31dB) in hiding a variable number (up to 7) of secret videos into a cover video by a single model. The performance degradation compared to fixed version is acceptable. With this design, a single model can satisfy multiple steganography demands.

4.5. Steganographic Analysis

The data security is one of the most important concerns in steganography. In this section, we evaluate the anti-
Table 4. The ablation study of different components in our LF-VSN. It includes the sliding window size, number of invertible blocks (IB), frequency concatenation (FreqCat), and redundancy prediction module (RPM).

<table>
<thead>
<tr>
<th>Num. videos</th>
<th>2</th>
<th>4</th>
<th>6</th>
<th>3 (ours)</th>
<th>3</th>
<th>3</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Window size</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Num. IB</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>12</td>
<td>16</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>FreqCat</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>RPM</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>Stego</td>
<td>39.64</td>
<td>40.97</td>
<td>41.08</td>
<td>36.41</td>
<td>37.55</td>
<td>37.86</td>
<td>38.03</td>
</tr>
<tr>
<td>Secret</td>
<td>42.97</td>
<td>44.24</td>
<td>44.43</td>
<td>37.67</td>
<td>40.21</td>
<td>40.42</td>
<td>41.99</td>
</tr>
</tbody>
</table>

Figure 10. Statistics-based steganalysis by StegExpose [7]. The closer the detection accuracy is to 50%, the higher the security is.

Steganalysis ability of different methods, which stands for the possibility of detecting stego frames from nature frames by steganalysis tools. We utilize the StegExpose [7] to attack different steganography methods. The detection set is built by mixing stego and cover with equal proportions. We vary the detection thresholds in a wide range in StegExpose and draw the receiver operating characteristic (ROC) curve in Fig. 10. Note that the ideal case represents that the detector has a 50% probability of detecting stego from an equally mixed cover and stego, the same as random sampling. Therefore, the closer the curve is to the ideal case, the higher the security is. Obviously, the stego frames generated by our LF-VSN are harder to be detected than other methods. Even in the multiple videos (e.g., 2 and 4 videos) hiding, our method can still achieve attractive performance, demonstrating the higher data security of our LF-VSN.

4.6. Ablation Study

In this subsection, we present the ablation study in Tab. 4 to investigate the effect of different components in our LF-VSN. The experiments are conducted on Vimeo-T200.

Sliding window size. In this paper, we utilize the temporal correlation within each frame group to improve the video steganography performance. To demonstrate the effectiveness, we evaluate the performance of our LF-VSN with the window size $L = \{1, 3, 5\}$ in 2, 4, and 6 videos steganography. The results in Tab. 4 present that the temporal correlation has obvious performance gains to the multiple videos steganography. Considering the model complexity, we set the sliding window size as 3 in our LF-VSN.

Number of invertible blocks (IB). As mentioned above, our LF-VSN is composed of several IBs. To investigate the effectiveness of IB, we evaluate the performance of our LF-VSN with the number of IB being 12, 16, and 20. The results in Tab. 4 present that the performance increases with the number of IB. To make a trade-off between performance and complexity, we utilize 16 IBs in our LF-VSN.

Frequency concatenation (FreqCat). In our LF-VSN, we use the DWT transform to merge each input group in the frequency domain. To demonstrate the effectiveness, we replace this operation with direct channel-wise concatenation. Tab. 4 presents that there are 1.76dB and 1.91dB gains of FreqCat on stego and secret quality in 3 videos steganography. The possible reason is that DWT transform can separate the low-frequency and high-frequency sub-bands, making it more effective for information fusion and hiding.

Redundancy prediction module (RPM). In our LF-VSN, we employ RPM to predict the redundancy in the backward process instead of randomly sampling. To demonstrate the effectiveness of RPM, we replace this module with a random Gaussian sampling. The result in Tab. 4 shows that RPM can be used not only to design key-controllable steganography, but also to improve performance.

5. Conclusion

In this paper, we propose a large-capacity and flexible video steganography network (LF-VSN). The novelty of our method is twofold. First, our LF-VSN has a large hiding capacity, with which we can hide 7 secret videos into a cover video and then recover them well (> 35dB). Second, we explore the flexibility in multiple videos steganography by proposing a key-controllable scheme and a scalable design. Specifically, our key-controllable scheme can enable different receivers to recover particular secret videos through specific keys. Also, the key controlling is sensitive and model-specific, which can enhance data security. Our scalable design further improves the flexibility to hide a variable number of secret videos into a cover video with a single model. Extensive experiments demonstrate that our proposed LF-VSN has state-of-the-art performance with high security, large hiding capacity, and flexibility.
References


