Co-Design Secure Control Based on Image Attack Detection and Data Compensation for Networked Visual Control Systems

Dajun Du, Member, IEEE, Lang Wu, Member, IEEE, Changda Zhang, Member, IEEE, Zixiang Fei, Member, IEEE, Lisi Yang, Minrui Fei, and Huiyu Zhou

Abstract — The incomplete and untrue data caused by cyberattacks (e.g., image information leakage and tampering) will affect the control performance and even lead to system instability. To address this problem, a novel co-design secure control method based on image attack detection and data compensation for networked visual control systems (NVCSs) is proposed. First, the existing problems of NVCSs under image attacks are analyzed, and a co-design secure control method, including image encryption, watermarking-based attack detection, and online data compensation, is presented. Then, a detector based on double-layer detection mechanism of timeout and digital watermarking is designed for real time, integrity, and authenticity discrimination of the images. Furthermore, according to the detection results, an online compensation scheme based on cubic spline interpolation and postprediction update is proposed to reduce the effect of cumulative errors and improve the control performance. Finally, the online compensation scheme is optimized by considering the characters of networked inverted pendulum visual control systems, and experimental results demonstrate the feasibility and effectiveness of the proposed detection and control method.

Index Terms—Attack detection, cyberattacks, networked visual control systems (NVCSs), online data compensation, secure control.

I. INTRODUCTION

VISION-BASED instrumentation and measurement systems [1], [2] have been applied for acquiring and processing signals, also known as noncontact, noninvasive, or nondestructive inspection. The technologies of visual sensing and image processing are widely used in different industrial automation fields, e.g., robot control, unmanned driving, and unmanned aircraft control [3], [4], [5]. This leads to the rapid development of networked visual control systems (NVCSs) [6]. However, when the images from vision-based measurement are transmitted through the network, NVCSs will face the challenge of image security such as image leakage and tampering. It in turn leads to the incomplete and untrue data and ultimately affects the stability of NVCSs [7], [8].

Such incomplete and untrue data mainly derive from two categories: 1) network inherent factors such as data packet losses and network-induced delay [9], [10], [11], [12] and 2) cyberattacks [13], [14], [15], [16], [17] such as denial-of-service (DoS) attacks, crop attacks, and noise attacks, leading to information forgery or even loss [18], [19], [20], [21]. These factors pose huge challenges to the security control of NVCSs.

These problems have stimulated some research works by considering incomplete and untrue data caused by cyberattacks. For example, DoS attacks decline system performance by blocking data transmission [22], and a compensation mechanism using the latest received data packets is designed to alleviate the influence of DoS attacks [23]. Deception attacks, such as replay attacks and false data injection attacks (FDIAs), destroy data authenticity [24], and a distributed observer combined with attack detection algorithm is designed to resist random or intermittent replay attacks [25]. To reduce the oscillation caused by FDIAs, a terminal integral adaptive sliding mode control algorithm using the estimation error as an adaptive factor is proposed [26]. Moreover, different methods on attack detection, state estimation, and security control under cyberattacks are summarized in [27] and [28]. However, these studies have not considered cyberattacks against the images.

In NVCSs, the mechanism of image attacks is more complex than nonimage attacks because image attacks will damage the quality of the transmitted images and lead to being unable to extract complete and true state information. To explore secure control methods of NVCSs under image attacks, the existing studies are basically aimed at image information leakage and tampering. To protect the security of the images, a chaos theory is employed to design some image encryption techniques based on image pixels [29], [30]. Furthermore, by using the cyclic generation of confrontation network, the

1557-9662 © 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.
encryption and decryption of the images are achieved based on deep learning [31]. To detect image attacks, the fragile image watermarking methods [32], [33], [34] are proposed to find image tampering and its locations. Some approaches based on image attack detection are studied. For example, an image restoration method is presented by integrating nonlocal self-similarity and global structure sparsity [35]. A diagonal mapping algorithm is proposed to guarantee the image tampered content recovery [36], and a flexible deep framework is proposed based on discriminant convolutional neural network for various image restoration tasks [37].

However, these existing methods are difficult to simultaneously satisfy real-time and image security requirements in NVCSs. There are the following challenging problems and difficulties.

1) The existing image security algorithms have usually high complexity and relatively low efficiency, leading to their inapplicability to high real-time environments. How to design high-efficiency image security algorithm for NVCSs is the first challenge.

2) An image security approach can only achieve the corresponding information confidentiality functions, but how to design image security detection is the second difficulty.

3) Most existing studies have been performed based on known assumption of data loss or tampering characteristics, but the assumption that the attacks obey a specific probability distribution is not always consistent with actual diverse and random image attacks. How to further guarantee the stability of NVCSs based on attack detection is the third challenge.

Therefore, considering real-time and accuracy requirements of NVCSs under image attacks, a novel co-design secure control method is proposed. The main contributions of this article are summarized as follows.

1) The existing problems of traditional NVCSs under image attacks are analyzed, and the overall framework of co-design secure control method, including image encryption, watermarking-based attack detection, and online data compensation, is elaborated.

2) A detector based on double-layer detection mechanism of timeout strategy and digital watermarking is designed for real-time and integrity discrimination of the images, which can judge whether the image is valid and provide the detection result by a trigger signal.

3) Considering detection results and cumulative errors, a cubic spline interpolation online compensation scheme based on postprediction update is proposed to improve the control performance of NVCSs.

The remainder of this article is organized as follows. In Section II, we have analyzed the vision-based measurement of NVCSs and the necessity of new secure control method. In Section III, a co-design secure control method for NVCSs is proposed, including double-layer detection and online compensation method. Section IV optimizes the online compensation scheme and discusses different experimental results for the NVCSs. The conclusions and future research are given in Section V.

II. PROBLEM FORMULATION

A. Vision-Based Measurement of NVCSs

The vision-based measurement of NVCSs is shown in Fig. 1, which includes the controlled plant, industrial camera (i.e., visual sensor), remote control terminal (including image processing unit and controller), and the actuator. First, the real-time images of the controlled plant are captured by an industrial camera, which are then transmitted to the remote control terminal via the network. Then, the states $x_k$ of the controlled plant are extracted from the received images in the image processing unit. Furthermore, according to $x_k$, the control signals $u_k$ will be calculated in the controller and transmitted to the actuator via the network. Finally, the actuator derives the controlled plant to keep stability.

To well construct the above NVCSs, three basics of vision-based measurement [2] are discussed by taking the networked inverted pendulum visual control system (NIPVCS) [38] as an example.

1) Visual Sensor: There are three main aspects on the visual sensor.

a) Visual sensor can be a visible-light camera, an infrared camera, a laser scanner, an X-ray scanner, or other similar sensor, e.g., a visible-light Aca640-120-gm monochrome industrial camera with the adjusted frame rate is used in our experiments.

b) The lighting conditions and the parallelism of the planes between the camera and the controlled plant directly affect the quality of the captured image. To solve these two problems, five light-emitting diode stroboscopic fluorescent lamps with adjustable illumination levels are taken as the light sources and a level meter is used to guarantee the parallelism of the planes.

c) For an industrial camera, an appropriate sampling mechanism should be set, e.g., a time-triggered sampling mechanism [39] is designed to capture the images.

2) Image Preprocessing: The image acquired by the visual sensor could have deficiencies such as noise and data redundancy [2]. For instance, to reduce data redundancy,
the regions containing the cart and pendulum motion areas are found from the original image, and then, the canny edge detection algorithm [38] is used to detect their edge information.

3) **Image Analysis:** The purpose of this stage is to analyze the images and extract the necessary information in the remote control terminal. For instance, since the camera and the moving plane are fixed, the cart position is obtained by applying the translation between the pixel coordinate system and the world coordinate system, and the pendulum angle is measured in the pixel coordinate system by using the edge detection technique based on the Hough transformation [38].

For now, with the well-established vision-based measurement, to achieve the integrity and authenticity of the state information, secure detection of the images has become the primary issue of NVCSs.

### B. Problem Analysis of Image Attacks Detection

The states $x_k$ depend importantly on the images, and when the images suffer from cyberattacks, the integrity and authenticity of the images are destroyed, leading to incomplete and untrue state and control information. The specific reasons are listed as follows.

1) It is difficult to accurately detect the types and areas of attacks in real time from the transmitted images. Image attacks usually include copy-move, slicing, noise attacks, and geometric attacks, which need to be identified through image target detection or forensics. However, for control systems with high real-time requirements, the large amount of image data will bring a great image processing delay.

2) It is tough to describe attacks quantitatively from the extracted information. Due to the characteristic of image attacks, the impact of image tampering on the extracted information is indirect, which is different from direct attacks on traditional sensing acquisition data. The extracted information from the image may involve only part of the area, and the impact of the attack on the extracted information cannot be estimated.

3) NVCSs take data availability as the highest priority. Assuming that image attacks conforming to a specific emergence pattern do not satisfy the real random attack situation. Unilateral consideration from attack detection or data compensation cannot guarantee system stability under cyberattacks.

**Remark 1:** Although accurate detection of image attacks can identify attacks, the system cannot afford the delay cost. Even if the type and area of the attack are detected, the impact of the attack on the extracted information is difficult to quantify. Assuming that the attacked image is directly discarded, there will be greater pressure on system information compensation, which is only suitable for a good network environment. Therefore, it is necessary to weigh the attack recognition accuracy and recognition speed. Moreover, to guarantee secure control of NVCSs, attack detection and data compensation need to be co-designed urgently.

### III. Co-Design Secure Control Method for NVCSs

The above has presented the framework of traditional NVCSs and analyzed the corresponding drawbacks. To cope with the drawbacks, a new co-design secure control method for NVCSs is fully designed.

#### A. Framework of Co-Design Secure Control

To achieve secure control of NVCSs under image attacks, a co-design security control method is proposed, and the corresponding framework is shown in Fig. 2. Unlike traditional NVCSs shown in Fig. 1, extra four units are added, i.e., image preprocessing, attack detector, data compensation, and buffer units. These four units are analyzed as follows.

1) **Image Preprocessing:** The controlled plant is sampled periodically by the industrial camera, and these captured real-time images are preprocessed by watermarking encryption. They are then transmitted to the remote control terminal via the network.

2) **Attack Detector:** Since the image may be lost or corrupted from attacks, an image detector is deployed in the remote control terminal. When the image arrives at the attack detector beyond the maximum allowable time, it will be discarded, going directly to data compensation unit; otherwise, the image tampering detection is performed and the whole process will be analyzed in Section III-B.

3) **Data Compensation:** When the image is judged as “invalid” by the attack detector, the lost state information will be online compensated by the following Section III-D.

4) **Buffer:** The states $x_k$ of the controlled plant are extracted and stored in the buffer to support controller design and data compensation.

For convenience, a flag $γ_k$ is used to indicate whether data transmission is normal. $γ_k = 1$ represents the normal transmission of data, which means that true state information can be extracted from the received image. $γ_k = 0$ represents the invalidity of data, which means that the predicted value should be used to compensate. Then, the controller input signal can be expressed as

$$z_k = γ_k x_k + (1 - γ_k) \tilde{x}_k \quad (1)$$

![Fig. 2. Framework of co-design secure control method for NVCSs.](image-url)
where \( x_k \) represents the true state, \( \hat{x}_k \) represents the predicted value of \( x_k \), and \( z_k \) represents the controller input.

**Remark 2:** In comparison with the traditional NVCSs, the induced four new units can achieve image encryption, watermarking-based attack detection, and co-design of online data compensation with buffer.

### B. Double-Level Attack Detector for the Images

Let us begin achieving co-design secure control from the attack detector. To make real-time judgment for image integrity and authenticity, a double-level attack detector is shown in Section I.A of Supplementary Material, which will be detailed presented in the following.

1) **First-Level Detection, i.e., Time-Based Detection:** For real-time availability of the images, the time-based policy is treated as first-level detection. According to the time from the timer, if the image reaches attack detector timeout, it will be judged as “invalid” and then directly enter the data compensation unit; otherwise, it is “valid” image. Moreover, the timer will be reset after each image arrival or time-out.

2) **Second-Level Detection, i.e., Image Security Detection:**

To guarantee the security of the images and detect image attacks, some advanced image encryption and watermarking algorithms have been proposed. However, these approaches mainly solve the security problems of still images, which usually have high computational complexity.

**Remark 3:** To verify whether the existing advanced encryption or watermarking approaches meet the real-time requirement of NVCSs, they have operated on the NIPVCS experimental platform \([38]\). As analyzed in Section I.B of Supplementary Material, it is revealed that they directly destroy system stability due to being high time-consuming.

To satisfy real-time and detection requirements, a new image security detection method as shown in Fig. 3 is designed as the second-level detection. Unlike the watermarking-based security detection method directly based on state information \([40]\), it combines image encryption with random fragile watermarking to reduce both the sacrifice of image information and the computational complexity of the algorithm.

At the image preprocessing unit of the local preprocessing terminal, two pseudorandom sequences are generated first by iterating the logistic mapping

\[
\begin{align*}
\lambda_{en}^{n+1} &= \mu_{en} \lambda_{en}^{n} (1 - \lambda_{en}^{n}), \\
\lambda_{wm}^{n+1} &= \mu_{wm} \lambda_{wm}^{n} (1 - \lambda_{wm}^{n})
\end{align*}
\]  

where \( \lambda_{en,wm}^{n} \in (0,1), \mu_{en,wm} \in (0,4), \) and \( n \in \mathbb{Z} \). The relevant parameters of the logistic mapping are set as Key 1 (i.e., \( \lambda_{en,wm}^{0} \) and \( \mu_{en,wm}^{0} \)) and Key 2 (i.e., \( \lambda_{en,wm}^{1} \) and \( \mu_{en,wm}^{1} \)).

Then, the original image \( I_{0} \) is encrypted by Key 1, where the pixel of the images at the \( i \)th row and \( j \)th column is denoted by \( P_{i,j} \). The specific encryption steps are given as follows.

1) **Keys Updating:** Getting the image time stamp \( T_n \), offset Keys 1 and 2 by considering \( T_n \) as a disturbance

\[
\begin{align*}
\lambda_{en}^{n} &= \text{mod}(T_n, 1000)/1000, \\
\lambda_{wm}^{n} &= |\lambda_{en}^{0} - T_n|, \\
\lambda_{wm}^{n} &= |\lambda_{wm}^{0} - T_n|, \\
\mu_{en}^{n} &= 3.9 + |\mu_{en}^{n} - 3.9 - T_n|, \\
\mu_{wm}^{n} &= 3.9 + |\mu_{wm}^{n} - 3.9 - T_n|
\end{align*}
\]  

where “\( \text{mod} \)” represents the assignment operation.

2) **Recorders Initialization:** Get the row number \( N \) and column number \( M \) of the image to ensure that each row and column is encrypted only once. The unencrypted number of rows and columns is set as \( N_{row} = N \) and \( N_{col} = M \), the row and column recorder of the image are set as \( R[i] \), \( i = 0, 1, \ldots, N - 1 \), and \( C[j] \), \( j = 0, 1, \ldots, M - 1 \), respectively.

3) **Rows and Columns Selection:** First, set \( e_{en}^{row}[l] \) and \( e_{col}^{row}[l] \), \( l = 0, 1, 2, 3 \) to record the iteration values for logistic map of row and column selection. Then, iterate (2) twice to get \( e_{en}^{row}[l] \) by Key 1, and the row number \( P_{row}[l] \) or \( S_{row}[l] \) in row recorder is selected by (4).

Moreover, overwriting the selected sequence number with the last unselected sequence number stored in the recorder and update \( N_{row} \) by (4). After that, the unencrypted row numbers are stored in the first \( N_{row} \) positions of the recorder. Finally, repeat these steps four times to select four rows. It follows that:

\[
\begin{align*}
P_{row}[l] &= e_{en}^{row}[l] \oplus N_{row}, \\
S_{row}[l] &= R[P_{row}[l]], \\
R[P_{row}[l]] &= R[N_{row}], \\
N_{row} &= N_{row} - 1.
\end{align*}
\]

where \( \oplus \) represents a rounding down operation.

4) **Encryption Parameters Generation:** Generate the encryption parameters \( \beta_{row}[l] \) and \( \beta_{col}[l] \) as follows for \( l = 0, 1, 2, 3 \):

\[
\begin{align*}
\beta_{row}[l] &= \text{mod}\left(e_{en}^{row}[3 \times l] \times 10000, 256\right), \\
\beta_{col}[l] &= \text{mod}\left(e_{en}^{col}[3 \times l] \times 10000, 256\right).
\end{align*}
\]

5) **Pixels Encryption and Rank Swapping:** Using the encryption parameters generated by (6) to encrypt the pixel values of the selected rows and columns, i.e.,

\[
\begin{align*}
P_{S_{row}[l],j} &= P_{S_{row}[l],j} \oplus (\beta_{row}[l] \equiv (\text{mod}(j, 4) \ll 1)) \\
P_{j,S_{col}[l]} &= P_{j,S_{col}[l]} \oplus (\beta_{col}[l] \equiv (\text{mod}(i, 4) \ll 1))
\end{align*}
\]  

where “\( \equiv \)” and “\( \ll \)” represent rotate right and left operation and \( \oplus \) represents the XOR operation. Then,
the detection efficiency of algorithm. In comparison with
authenticity detection of state information extracted from the
image, the proposed double-level attack detection has a higher
real-time capability. The former needs to extract information
from the image before detection, whereas the latter detects first
the validity of the image; only a “valid” image is processed to
extract the state information. Therefore, under the latter case,
state information extraction may be skipped if the detector
judges the image as “invalid,” which avoid the meaningless
time-consuming of image processing.

Remark 4: In comparison with the retransmission mecha-
nism [41], the proposed double-level detection mechanism
can detect tampering locations on the images. For instance,
if 1% of 1000 frames of the images (i.e., 10 frames) have
timed out and 2% (i.e., 20 frames) are judged as “invalid”
under image attacks, then more 30-time retransmission will
be produced based on the retransmission mechanism, which
cannot guarantee system stability because the retransmitted
image may not reach remote control terminal in time. How-
ever, the proposed double-level detection mechanism
does not need the retransmission, which can directly judge the
attacked images as “invalid.” They will then be compensated
in the data compensation unit, so it can improve the efficiency
because the computational time of compensation is far less
than retransmission time.

C. Analysis of Real Time and Computational Burden

A process control system has less strict requirement on
the control period, which is usually on the second or minute
level [42], [43]. However, a motion control system with
fast-changing characteristics and its control period is generally
on the millisecond level [44], [45]. As an ideal motion control
platform, NIPVCS can keep stability under high real-time
conditions.

High real-time requirements can be met by low compu-
tational burden of the algorithm. The computational complexity
of the proposed algorithm based on the logistic map iteration is

\[
\begin{align*}
P_{S_{row}}(l, j) &\leftrightarrow P_{S_{row}}(l+1, j), P_{l, S_{col}}(l) &\leftrightarrow P_{l, S_{col}}(l+1) \\
\text{if } l &\text{ is even}
\end{align*}
\]

where “\(\leftrightarrow\)” represents the replacement operator.

6) Repeating 3)–5) until \(N_{row} = 0\) or \(N_{col} = 0\).

During the image encryption process, the cross iteration of
rows and columns is used, while the intersection of rows and
columns (i.e., \(P_{S_{row}}(l_1), S_{col}(l_2)\), \(l_1 = 0, 1, 2, 3\) and \(l_2 = 0, 1, 2, 3\))
is selected as the watermarking embedding location, as shown
in Fig. 4. Here, the specific watermarking embedding method
is given as follows.

1) Watermarking Parameters Generation: Iterating 2) once
to get \(\zeta^{wm}[s], s = 0, 1, 2, \ldots, 15\) by Key 2 in (3),
and set \(g[s] = \text{mod}(\zeta^{wm}[s] \times 1000, 2^2)\). Then, the
watermarking parameters are split to get the watermarking
information \(wm_l[s] = g[s]\&3\) and pixel shift distance
\(wm_H[s] = (g[s]\&12) \gg 1\).

2) Watermarkings Embedding: Embed watermarking
information in the lower two bits of the pixel, i.e.,

\[
\begin{align*}
P_{S_{row}}(l_1), S_{col}(l_2) &\leftarrow P_{S_{row}}(l_1), S_{col}(l_2) \& 252 \oplus wm_H[s] \\
P_{S_{row}}(l_1), S_{col}(l_2) &\leftarrow P_{S_{row}}(l_1), S_{col}(l_2) \gg wm_H[s].
\end{align*}
\]

3) Repeating 1) and 2) until all intersections are embedded
with watermarking.

At the second-level detection, after the encrypted image is
received, the embedded watermark is extracted from the
same position according to Keys 1 and 2 before decryption.
In comparison with the extracted watermarking and original
watermarking, it will be detected whether the encrypted image
has suffered tampering based on its intensity. If the intensity of
the detected tampering exceeds the attack detection threshold,
the image is judged as “invalid” and discarded; otherwise,
the image can be decrypted by Key 1, which is an inverse process
of image encryption.

The pseudocode of the image preprocessing (encryption and
watermarking embedding) is Algorithm 1.

The result from the double-level attack detector will be
represented by a trigger signal \(\gamma_k\). If the image is judged as
“invalid” (i.e., \(\gamma_k = 0\)), then the image is discarded and
the next process will directly enter the data compensation unit;
otherwise, \(\gamma_k = 1\), and the “valid” image will be decrypted by
Key 1 and the corresponding available state information \(x_k\)
is extracted at the information extraction unit.

For NVCSs, the complete and true image is the corner-
stone of system stability. Moreover, the large-granularity-
based row–column cross selection method greatly improves

**Algorithm 1 Image Security Detection Method**

**Input:** The image captured by industrial camera: \(I_o\), The
pixels of the image: \(P_{i,j}\), The image time-stamp: \(T_n\); The
image encryption key (Key 1): \(\gamma_{eq}^{0}\) and \(\mu_{eq}\), The fragile
watermarking key (Key 2): \(\lambda_{wm}^{0}\) and \(\mu_{wm}\).

**Output:** The encrypted image \(I_w\),
1: Keys updating (3),
2: Recorders initialization,
3: repeat
4: Rows and columns selection (4) and (5),
5: Encryption parameters generation (6),
6: Pixels encryption (7) and rank swapping (8),
7: repeat
8: Watermarking parameters generation,
9: Watermarkings embedding (9),
10: until All intersections are embedded with watermark-
ings.
11: until \(N_{row} = 0\) or \(N_{col} = 0\).
$O((M+N)+(MN)/2)$, which is much smaller than $O(2MN)$, $O(3MN)$, or $O(24MN)$ of some advanced pixel-based algorithms [31], [46], [47], that is, the proposed algorithm reduces time from generating encryption as well as watermarking parameters and converting floating-point numbers with the same size of the images. It is worth noting that the time of the decryption is about half of the whole algorithm. If the images can be prejudged as “invalid” after being attacked, it will avoid nearly half of the unnecessary image decryption time. Experimental results of the proposed method are analyzed in Section I.B of Supplementary Material, which meets the real-time requirement of NVCSs.

D. Online Compensation Based on Cubic Spline Interpolation

If the images are judged as “invalid” and discarded by the above double-level attack detector, data compensation must be designed to guarantee the stability of NVCSs. Due to good characteristics such as continuity of derivatives and interpolation and low computational burden, cubic spline interpolation algorithm [48] is adopted, as shown in Section I.C of Supplementary Material. Then, online compensation is described as follows.

1) Cubic Spline Interpolation Algorithm: To compensate for state information caused from “invalid” images, the predicted values in the $k$th sampling period can be calculated by spline interpolation. First, an interval $[t_i, t_{i+1}]$ is divided into $n - 1$ intervals, i.e., $t_1 < t_2, \ldots, t_{n-1} < t_n$. Then, the function $S(t)$ is a cubic polynomial on each interval $[t_i, t_{i+1}]$. Given $y_i = f(t_i), i = 1, \ldots, n$ on the node $t_i$ and $S(t_i) = t_i, S(t)$ is called spline function on the nodes $t_1, \ldots, t_n$.

To solve function coefficients of spline interpolation, the following conditions need to be satisfied.

1) In each interval $[t_i, t_{i+1}], S_i(t)$ is a cubic polynomial and $S_i(t) = a_i + b_i(t - t_i) + c_i(t - t_i)^2 + d_i(t - t_i)^3$, where $a_i, b_i, c_i$, and $d_i, i = 1, \ldots, n - 1$. Thus, there are $4(n - 1)$ unknown coefficients.

2) Zero error at the node is satisfied, i.e., $S_i(t_i) = y_i$.

3) The curve $S(t)$ is smooth. The first- and second-order derivatives $S'(t)$ and $S''(t)$ are all continuous in $[t_i, t_{i+1}]$, i.e., $S'_i(t_{i+1}) = S'_{i+1}(t_i), S''_i(t_{i+1}) = S''_{i+1}(t_i)$.

Letting $h_i = t_{i+1} - t_i$, $m_i = 2c_i$, 1–3 lead to $h_i, m_i + 2(h_i + h_{i+1})m_{i+1} + h_{i+1}m_{i+2} = 6((y_{i+1} - y_i)/(h_{i+1})) - ((y_{i+1} - y_i)/h_i))$. Hence, the parameters in $S'_i(t)$ are $a_i = y_i, b_i = ((y_{i+1} - y_i)/h_i) - (h_i/2)m_i - (h_i/6)(m_{i+1} - m_i), c_i = (1/2)m_i, d_i = (m_{i+1} - m_i)/6h_i$.

A non-node boundary (not-a-knot) is used to add extra restrictions on the differentiation between the endpoints $x_1$ and $x_n$, i.e., $S''_1(t_2) = S''_n(t_2)$ and $S''_{n-2}(t_{n-1}) = S''_{n-1}(t_{n-1})$. Then, the above restrictive conditions become $h_2(m_1 - m_2) + h_2(m_3 - m_2) = h_2(m_3 - m_2)$ and $h_{n-1}(m_{n-1} - m_{n-2}) = h_{n-2}(m_n - m_{n-1})$.

Therefore, the corresponding piecewise trinomial polynomial function curve coefficients $a_i, b_i, c_i$, and $d_i$ can be obtained by the solution of $m_i$.

Remark 5: The accuracy of the predicted data generated by interpolation gradually decreases as the number of “invalid” images increases. From the interpolation strategy, when the historical compensation data become historical data, they will have an impact on future data compensation. Therefore, only data prediction cannot fulfill stable operation requirements for high real-time control systems. It is necessary to improve the existing algorithm.

2) Design of Online Compensation Scheme: It is found by the experiments that when only predictions are made in the above cubic spline interpolation algorithm, there exist the following drawbacks.

1) If the current control signal $u_k$ is correlated with the current state $x_k$ and buffer $\{z_{k-1}\}$ including the previous states, the historical prediction error will decline the control performance when $x_k$ is not lost and $x_{k-1}$ is lost.

2) Under poor network environments, the historical data $\hat{x}_{k-1}$ will be used to predict the current lost data, but the prediction error will adversely affect the current prediction.

Due to the existence of prediction errors described above, the cumulative errors will lead to an excessive accumulation of errors after a period of operation, which affects the stability of NVCSs. To solve the above problems, we propose an online compensation strategy based on cubic spline interpolation, which is mainly divided into the data prediction phase and repredicting phase of historical prediction data. The data from the prediction phase will be transmitted to the controller to calculate control signals, while the repredicting phase of historical prediction data reduces the accumulated errors to provide more accurate historical data for the next prediction by improving the accuracy of historical prediction data.

To achieve an online compensation strategy, a buffer is first deployed to record historical data $\{z_k\}$ for supporting data compensation of invalid images. When invalid images are discarded, the lost data are replaced by $\hat{x}_k$, which is predicted in the data compensation unit by $\{z_k\}$ from the buffer. Then, the received first valid states $x_k$ after discarding data will be used to update historical compensation data and will be transferred to the buffer.

Specifically, three cases (i.e., the current data are invalid, the current data are valid and previous data were invalid, and both the current data and previous data are valid) are processed.

1) When the current data $x_k$ are judged as invalid, taking the previous data $\{z_{k-1}\}$ as known data, the current data are predicted by a cubic spline external interpolation algorithm, and $\{z_k\}$ will be updated by the predicted value $\hat{x}_k$. It is treated as the prediction phase.

2) When $x_k$ is valid but $x_{k-1}$ is judged as invalid, the latest historical predicted data $\hat{x}_{k-1}$, $\hat{x}_{k-2}$ will be updated to $\hat{x}_k$, $\hat{x}_{k-1}$, $\hat{x}_{k-2}$ by $x_k$. Then, the buffers $\Lambda = \{z_{k-1}, \ldots, z_{k-1-k}\}$ will be updated by $\hat{x}_k$, $\hat{x}_{k-1}$, $\hat{x}_{k-2}$ and $x_k$. It is treated as the update phase.

3) When both $x_k$ and $x_{k-1}$ are valid, the buffer $\{z_k\}$ is updated directly.

Considering continuous character of attacks, $r_k$ is used to record the continuous invalidation at the $k$th instant, representing the number of equivalent continuous packet losses. If $r_k = 1$, set $\tau_k = 0$; if $r_k = 0$, set $\tau_k = \tau_k - 1 + 1$.

Therefore, the pseudocode of online compensation strategy is summarized in Algorithm 2.
Algorithm 2 Online Compensation Strategy Based on Cubic Spline Interpolation

Input: $\gamma_k, \tau_k, x_k$

Output: $z_k, \hat{x}_k$

1: Initial $t_0 \leftarrow 0$ and $k \leftarrow 1$,
2: for each $k \in [1, \infty)$ do
3:  if $\gamma_k = 0$ then
4:   $\tau_k \leftarrow \tau_{k-1} + 1$,
5:  Using cubic spline interpolation prediction to obtain $\hat{x}_k$,
6:  $z_k \leftarrow \hat{x}_k$,
7:  else
8:   if $\tau_{k-1} \neq 0$ then
9:     Using cubic spline interpolation to update $\hat{x}'_{k-1}, \ldots, \hat{x}'_{\tau_{k-1}}$, 
10:    Update historical values in the buffer $z_{k-1}, \ldots, z_{k-\tau}$,
11:  end if
12: $\tau_k \leftarrow 0$,
13: $z_k \leftarrow x_k$,
14: end if
15: $k \leftarrow k + 1$,
16: end for

As mentioned above, the compensation of invalid data is divided into two main phases: prediction and update.

The prediction phase uses a multistep prediction approach. When invalid data occur, the invalid data $x_k$ are predicted by interpolation based on the known historical data $x_{k-1}, \ldots, x_{k-i}$ ($i$ is the number of known historical data selected in the prediction phase). Each prediction is based on previous $i$ steps, regardless of the presence of historical predicted data in previous $i$ steps. Taking the prediction phase shown in Fig. 5 as an example, the coefficients of the segmented cubic polynomial are obtained by interpolating cubic splines with the known sampled values (which may contain historical prediction data, such as $t_1$) at $t_1, \ldots, t_i$. Then, the last segment function $S_i(t)$ is used as the motion trajectory of the controlled plant, and the corresponding function value obtained at the corresponding instant is the predicted value of the invalid sampling value at instant $t_i$.

Remark 6: The predicted values $\hat{x}_k$ will be used in the calculation of control signal $u^*_k$, which has an effect on the motion of the controlled plant, so historical prediction data are also considered as known historical data for next invalid data in the case of successive invalidation. It is worth noting that as the time interval between the prediction data and real valid data increases, the accuracy of the prediction gradually decreases in a short-period sampling system.

To improve the accuracy of historical prediction data when the next continuous invalid data occur, an update phase after prediction is proposed to form prepredict and postupdate strategies. When the first valid data $x_k$ appear after continuous data invalidation at $t_{k-1}$, a multistep update is used to interpolate historical prediction data $x_{k-1}, \ldots, x_{k-\tau}$ one by one based on the current real data $x_k$ and historical data $x_{k-1}, \ldots, x_{k-j}$ ($j > \tau_{k-1}$, where $j$ is the number of known data selected in the update phase) to ensure that the used historical data are closer to the real data when data invalidation occurs again.

Remark 7: A multistep update is defined as a process of $\tau$ update based on historical forecast data, and the corresponding updation process is shown in Fig. 6. According to the number of $\tau$ of historical prediction data, $\tau$ rounds of updation are performed, in the order of time interval between historical prediction data and the latest real data from near to far. Only one historical prediction data are updated in each round, and the buffer will be updated at the end.

Taking the update phase shown in Fig. 7 as an example, the data at $t_4$ and $t_5$ are historical prediction data, which means that the amount of historical prediction data is 2 and
two rounds of updates are required. In the first round, the data at \( t_5 \) will be predicted again. In the second round, the data at \( t_4 \) will be predicted again. The segmentation function between two moments before and after the update moment is used as the motion curve. The first round of updation takes data at \( t_1, t_2, t_3, t_4, \) and \( t_5 \) as known sampled data to obtain the coefficients of the segmented cubic polynomial. The segmentation function between \( t_4 \) and \( t_5 \) is used to take the updated data at the corresponding instant \( t_5 \). In the second round, the data at \( t_1, t_2, t_3, t_4, \) and \( t_5 \) are taken as known sampled data, where the data at \( t_5 \) are the updated data. The corresponding segmentation function between \( t_3 \) and \( t_5 \) is used to take the updated data at \( t_4 \).

This phase is based on the current valid data for reducing the impact of prediction errors. On the other hand, the next round of data prediction is operated to reduce the accumulation of prediction errors.

**Remark 8:** It is worth noting that the update phase requires multiple rounds of updations, which consumes a certain amount of computation time to update at the current instant. Therefore, it is considered to copy first the current buffered data and then judge the necessity of updating based on whether this information is adopted or not when the next round of consecutive predictions appears. If the historical prediction data are adopted by the next round of prediction, the time margin generated from skipping the image decryption and information extraction units at the prediction phase is used to update, which will reduce unnecessary data updation.

### IV. Experimental Analysis

#### A. Establishment of the Experimental Platform

With nonlinear and unstable characteristics, an inverted pendulum control system is an ideal platform for experiment verification. Therefore, NIPVCS is employed to verify the feasibility and effectiveness of the proposed secure control method, as shown in Fig. 8. NIPVCS is mainly composed of actuator, inverted pendulum, visual sensor (industrial camera), image preprocessing unit, double-layer detector, data compensation unit, image information extraction unit, and controller. A visual sensor has the highest frame rate up to 120 frames/s and the highest resolution up to 659 × 492, which can satisfy the measurement resolution and real-time requirements of inverted pendulum control system.

Considering NIPVCS under a time-triggered mechanism, the effective sampling period \( T_s \) needs to be selected to satisfy \( T_s > \overline{T} \) (\( \overline{T} \) represents the upper bound of system delay). In fact, system delay fluctuates due to the influence of computation processing ability, network environment, and other factors, so there exist upper bound \( \overline{T} \) and lower bound \( \underline{T} \). Therefore, to select a suitable \( T_s \), the fluctuation range of the delay needs to be analyzed of 2000 image samples is shown in Section I.D of Supplementary Material. \( \overline{T} \) and \( \underline{T} \) are obtained as

\[
\overline{T} = 26 \text{ ms}, \quad \underline{T} = 34 \text{ ms}.
\] (10)

Therefore, \( T_s = 35 \text{ ms} > \underline{T} \) is taken as the sampling period.

NIPVCS with fast time variation has large sawtooth fluctuations in the pendulum angle curve due to a short control period, which is not conducive to long-term data prediction compensation. Therefore, its state is considered to be segmented to obtain the smoother state curve. From the pendulum angle curves at the 2\( k \)th and (2\( k \) + 1)th shown in Section I.E of Supplementary Material, it appears the gentler motion trend between the interval sampling points of the state compared to the original one, which makes it more suitable for data compensation. Therefore, the state are divided into two time series (2\( k \)th and (2\( k \) + 1)th) for compensation.

However, the above division reduces the correlation of the prediction information. Therefore, to ensure the prediction accuracy, considering the correlation between \( x_k \) and \( x_{k-1} \), the prediction results are corrected by the state information of the previous instant in the prediction phase. It follows that:

\[
\hat{x}_{k|k-1} = e_{\text{pre}} \hat{x}_k + (1 - e_{\text{pre}}) z_{k-1}
\] (11)

where \( e_{\text{pre}} \) is the correction scale factor, \( e_{\text{pre}} \in (0, 1) \), \( \hat{x}_k \) is the predicted value of the invalid state \( x_k \), \( z_{k-1} \) is the state of previous instant cached in the buffer, and \( \hat{x}_{k|k-1} \) is the correction value of \( \hat{x}_k \), which will be recorded as \( z_k \).

In the update phase, assuming that the current new valid state belongs to the 2\( k \)th series, then only the historical predicted state of the 2\( k \)th series will be updated in the update phase, while the (2\( k \) + 1)th series can be updated until next valid state appears. However, the calculation of control signal is highly correlated with the state of previous instant, so the state update starts from a preupdate of the nearest neighboring historical prediction data. It follows that:

\[
\hat{x}_{k-1|k} = e_{\text{up}} z_{k-1} + (1 - e_{\text{up}}) x_k
\] (12)

where \( e_{\text{up}} \) is preupdate scale factor, \( e_{\text{up}} \in (0, 1) \), \( x_k \) is new valid state, and \( \hat{x}_{k-1|k} \) is the preupdate value of \( z_{k-1} \). The correction scale factor \( e_{\text{pre}} = 0.8 \) and the preupdated scale factor \( e_{\text{up}} = 0.7 \) are selected by several experiments.

#### B. Security Detection and Real-Time Control Experiments

1) Analysis of Watermarking Detection Method: The watermarking embedded pixels of the proposed algorithm are random and scattered for the located one. A block localization...
method is employed to support the detection, where the image with $640 \times 480$ pixels will be divided into $10 \times 10$ blocks for initial tampering detection. If a watermarking embedded pixel is detected to be tampered, the corresponding block will be marked as being tampered. After extraction and comparison of all watermarkings, a marked image with $64 \times 48$ pixels is obtained. Morphological operations are then performed on this marked image to exclude small black holes, as shown in Section I.F of Supplementary Material, which can achieve high attack recognition accuracy.

2) Real-Time Performance: The real-time performance of system with detector and system without detector is shown in Section I.G of Supplementary Material. It can be seen that the curve fluctuation of pendulum angle has slightly increased, but the system can still maintain stability after adding the detector, which demonstrates that the proposed detector can satisfy real-time requirements.

3) Threshold Selection of Attack Detection: To analyze the effect of attack intensity on system performance, the experiments are operated by considering typical attacks, including cropping attacks (rectangular cropping and irregular cropping), splicing attacks, copy-move attacks, replay attacks, and noise attacks (Gaussian noise and salt-and-pepper noise), as shown in Fig. 9. Among them, the encrypted images under attacks, initial marked images (initial tampering detection using block localization method), final marked images (after morphological operation of initial marked images), and decrypted images are from left to right, and the white part of the images is the tampered area detected; the range shown by the blue dashed line in the image under copy-move attack is the copied area and the range shown by the white dashed line is the moved area.

As shown in Fig. 9, regardless of regular shape of the clipping attack, the cropping region can be detected and effectively localized. The splicing attack, copy-move attack, and replay attack present the same results of tampering region as the cropping attack. Gaussian noise and salt-and-pepper noise are global tampering attacks, where initial marked images show global random distribution. It can be seen from the final marked images in Fig. 9(f) and (g) that further detection of the attack can more clearly reflect its global characteristics. Moreover, the decrypted image indicates that the information in the tampered area will not be completely lost under a certain intensity of attack, which is because the impact of the attack is dispersed to other regions of the image by encryption.

To guarantee the stability of NIPVCS, a suitable detection threshold needs to be set to achieve quantitative identification of images. Therefore, the tampering rates of typical attacks detected at different intensities are analyzed by the appropriate threshold. The proposed block localization method is used to detect different types of attacks with different attack intensities, and system stability is observed without warning, as shown in Tables I and II. Here, attack intensity refers to the ratio of the number of pixels suffering from tampering to the whole image, “tampering rate 1” represents the tamper rate obtained from the initial detection, “tampering rate 2” represents the tamper rate obtained from the final detection, and “√” represents the ability of the system to maintain stable operation under a continuous attack of the corresponding intensity; otherwise, “×.”

From Table I, it can be concluded that for local tampering (cropping, splicing, and copy-move attacks), tampering rate 2 can effectively represent the true tampering ratio and the ratio of tampering rate 1 to 2 is close to 1:2. Moreover, when the tampered area is greater than 17%, the inverted pendulum cannot maintain stability. For replay attack, the whole image is tampered and no valid information can be obtained to maintain system stability, but the ratio of tampering rate 1 to 2 is also close to 1:2. Therefore, these types of area-based tampering can be considered as having a ratio of “tampering rate 1” to “tampering rate 2” close to 1:2, and 17% can be selected as the threshold of “tampering rate 2.” The threshold of “tampering rate 2” is 17%, which means that the area-type attacks with “tampering rate 2” less than 17% can be resisted by the controller and the impact on image information can be ignored.

From Table II, it can be concluded that for global tampering (Gaussian noise and salt-and-pepper noise), the ratio of “tampering rate 2” to “tampering rate 1” increases and then decreases as the noise intensity increases, and the ratio of two
TABLE I
ATTACK DETECTION RESULTS UNDER DIFFERENT REGIONAL ATTACK TYPES

| Attack type          | Attack intensity | Tampering rate 1 | Tampering rate 2 | System stability |
|----------------------|------------------|------------------|------------------|------------------|
| Rectangular cropping attack | 4%               | 1.92%            | 4.13%            | ✓                |
|                      | 8%               | 3.79%            | 7.77%            | ✓                |
|                      | 16%              | 7.81%            | 15.59%           | ✓                |
|                      | 25%              | 11.59%           | 24.66%           | x                |
| Irregular cropping attack | 4%               | 1.91%            | 4.12%            | ✓                |
|                      | 8%               | 3.86%            | 7.83%            | ✓                |
|                      | 16%              | 7.92%            | 16.27%           | ✓                |
|                      | 25%              | 12.35%           | 25.18%           | x                |
| Splicing attack      | 4%               | 1.86%            | 3.87%            | ✓                |
|                      | 8%               | 3.91%            | 7.79%            | ✓                |
|                      | 16%              | 7.71%            | 15.79%           | ✓                |
|                      | 25%              | 11.97%           | 24.85%           | x                |
| Copy-move attack     | 4%               | 1.92%            | 4.09%            | ✓                |
|                      | 8%               | 3.81%            | 7.89%            | ✓                |
|                      | 16%              | 7.93%            | 15.87%           | ✓                |
|                      | 25%              | 11.46%           | 24.80%           | x                |
| Replay attack        | 1                | 45.67%           | 100.00%          | x                |

TABLE II
ATTACK DETECTION RESULTS UNDER DIFFERENT NOISE ATTACK TYPES

| Attack type          | Attack intensity | Tampering rate 1 | Tampering rate 2 | System stability |
|----------------------|------------------|------------------|------------------|------------------|
| Gaussian noise       | \(\mu = 0, \sigma = 1\) | 8.04%            | 38.38%           | ✓                |
|                      | \(\mu = 0, \sigma = 2\) | 15.71%           | 94.37%           | ✓                |
|                      | \(\mu = 0, \sigma = 4\) | 24.10%           | 97.73%           | ✓                |
|                      | \(\mu = 0, \sigma = 6\) | 28.48%           | 98.70%           | x                |
| Salt-and-pepper noise attack | 4%               | 1.99%            | 4.46%            | ✓                |
|                      | 10%              | 7.58%            | 33.20%           | ✓                |
|                      | 20%              | 14.48%           | 62.66%           | ✓                |
|                      | 30%              | 17.76%           | 86.32%           | ✓                |
|                      | 40%              | 27.67%           | 92.97%           | x                |
|                      | 80%              | 45.57%           | 98.83%           | x                |

Different attack intensities. The “tampering rate 2” is equal to 17% as the first threshold. If it is less than 17%, the images are valid. If it is greater than 17%, we then analyze the ratio of “tampering rate 1” and “tampering rate 2.” If “tampering rate 2” is three times or more than “tampering rate 1” and “tampering rate 1” is less than 18%, the image is valid and otherwise invalid.

Remark 9: An appropriate threshold of tampering rate of image attacks for double-layer detector is important to judge the validity of the images. Most of the existing threshold selection methods generally include theoretical derivation [49], statistical analysis [50], and machine learning [51]. According to the statistical results of real-world experiments, the thresholds of image attack tampering rate are determined. For NIPVCS shown in Fig. 8, the double thresholds achieve the appropriate division of the damage on the image under different attack intensities. The “tampering rate 2” is equal to 17% as the first threshold. If it is less than 17%, the images are valid. If it is greater than 17%, we then analyze the ratio of “tampering rate 1” and “tampering rate 2.” If “tampering rate 2” is three times or more than “tampering rate 1” and “tampering rate 1” is less than 18%, the image is valid and otherwise invalid.

Remark 10: When the system still remains stability under noise attacks, the tampering rate detected by Gaussian noise and salt-and-pepper noise demonstrates a large difference, so a uniform threshold cannot be obtained to classify them. This is due to the global characteristics of Gaussian noise, which will add different intensities of Gaussian interfere to each pixel, while the watermarking information is embedded in each bit of the pixel that it has a better detection effect. On the other hand, salt-and-pepper noise is selected a certain percentage of pixels to change its value to 0 or 255, and the watermarking information is also embedded at intervals: naturally, the detection probability of it will be lower. Therefore, the smaller tampering rate among them is selected as the second threshold value conservatively.

C. Co-Design Compensation and Real-Time Control Experiments

An experimental analysis is performed on NIPVCS to compare the proposed online compensation schemes step by step, and they are experimented under different network environments to analyze the factors affecting their performance.

1) Control Performance Comparison Under Different Compensation Schemes: Considering the invalidation of data equated to data loss, the frequency of data invalidation will be expressed as the loss rate \(\rho\). To verify the effectiveness of the prediction phase (without the update phase), the traditional method (deferring the previous data), single-step prediction (based on cubic spline interpolation), and multistep prediction are compared under the number of consecutive loss \(\tau = 4\). The performance of the above three prediction compensation methods is tested by gradually increasing \(\rho\), and the performance of the above three prediction methods is compared under the same \(\rho\), as shown in Figs. 10 and 11.

From Fig. 10, with \(\tau = 4\), it can be obtained that the tolerance to the loss rate is multistep prediction > single-step prediction > traditional method. From Fig. 11, under \(\rho = 15\%\), it can be obtained that the control curve fluctuation situation is multistep prediction < single-step prediction < traditional method. Multistep prediction performs best in both tolerance of loss rate and control stability.

Next, under \(\tau = 4\) and with multistep prediction phase, three update methods of nonupdate, single-step update, and multistep update were compared, and their performances are tested by gradually increasing \(\rho\), as shown in Figs. 10(c) and 12. It can be obtained that the tolerance to the loss rate is multistep update > single-step update > nonupdate.

Furthermore, the prediction error based on cubic spline interpolation will accumulate excessively after a period of time, which will affect the stability of NVCSs. Therefore, two updating methods (i.e., single-step update and multistep update) are used to reduce the prediction error in real-world experiments, which provides more accurate historical
data for the next prediction. The performance of five data compensation methods by prediction is compared under the same $\rho$ and $\tau$, as shown in Fig. 13. It can be obtained that the fluctuation of the control curve is multistep update with multistep prediction $<$ single-step update with multistep prediction $<$ multistep prediction $<$ single-step prediction $<$ traditional method, and a multistep update method based on historical prediction data has the best performance in loss rate tolerance and control stability again.

The prediction accuracy is evaluated by the root-mean-squared error (RMSE) between historical prediction data and real data, i.e., $PA = ((1/N_{inv}) \sum_{n=1}^{N_{inv}} (err(n))^2)^{1/2}$, where $N_{inv}$ represents the total number of invalid data and $err(n)$ represents the $n$th error between historical prediction and real data. When $PA$ is smaller, it indicates that the prediction accuracy is higher, i.e., the compensation performance is better. As shown in Fig. 14, under the same $\rho = 30\%$ and $\tau = 4$, the prediction error fluctuation based on multistep update with multistep prediction is smaller. Moreover, the prediction accuracies of five methods are calculated, as shown in Section I.H of Supplementary Material. Experimental results show that the proposed multistep update with multistep prediction has higher prediction accuracy in comparison with other approaches.

To summarize, multistep prediction compensation works best in the prediction stage, and multistep update works best in the update stage. The online compensation strategy based
on multistep prediction and multistep update can effectively compensate for the invalid data under network uncertainty of the control system.

2) Control Performance Comparison Under Different Network Environments: In fact, the variable network environment makes data loss random (e.g., random number of consecutive loss and random loss frequency), which affects the online date compensation and thus leads to different compensation effects of the proposed strategy. Therefore, control performance under a different number of consecutive loss $\tau$ and loss rate $\rho$ will be experimentally analyzed to further explore the impact of network environment on the proposed strategy.

First, the effect on the system control is observed by increasing $\tau$, as shown in Fig. 15. It can be seen that for the same $\rho$, the fluctuation of the pendulum angle keeps increasing as $\tau$ increases. Within a certain range of $\tau$, the control system at the lower $\rho$ fluctuates for a period of time after data loss, but it still can reach a stable state. Moreover, the inverted pendulum control system starts to lose stability with $\tau > 8$.

The absolute value of angular error is calculated for $\tau = 4, \ldots, 9$ under $\rho = 15\%$, as shown in Fig. 16. It can be seen that the prediction error increases with the increase of $\tau$ at the same $\rho$. The more distant the prediction data is from the valid data, the lower the prediction accuracy is, which leads to the continuous loss periods too close to each other on the time scale, which will lead to the accumulation of the error not being eliminated and accumulated to the next loss period. In this way, the prediction error will keep increasing, and then, the system gradually destabilizes over time.

V. CONCLUSION

In this article, a novel co-design secure control method based on image attack detection and data compensation for NVCSs is proposed to address the incomplete and untrue data caused by cyberattacks. First, a detector based on a double-layer detection mechanism of timeout strategy and digital watermarking has been designed for image real-time and integrity discrimination to achieve image information protection and integrity detection simultaneously. Then, based on the detection results, an online compensation scheme based on cubic spline interpolation has been proposed to improve the control performance. Finally, the feasibility and effectiveness of the proposed method are confirmed on a practical platform. Limited by high real-time requirement of system, the method proposed compensates for the data in the perspective of nonvisual information, and thus, future research will be devoted to the efficiency improvement of the recovery algorithm on the images.

REFERENCES

[1] S. S. Beauchemin, M. A. Bauer, T. Kowsari, and J. Cho, “Portable and scalable vision-based vehicular instrumentation for the analysis of driver intentionality,” IEEE Trans. Instrum. Meas., vol. 61, no. 2, pp. 391–401, Feb. 2012.
[2] S. Shirmohammadi and A. Ferrero, “Camera as the instrument: The rising trend of vision based measurement,” IEEE Instrum. Meas. Mag., vol. 17, no. 3, pp. 41–47, Jun. 2014.
[3] S. Yan, X. Tao, and D. Xu, “Image-based visual servoing system for components alignment using point and line features,” IEEE Trans. Instrum. Meas., vol. 71, pp. 1–11, 2022.
[4] R. C. Luo and C.-W. Kuo, “Intelligent seven-DoF robot with dynamic obstacle avoidance and 3-D object recognition for industrial cyber-physical systems in manufacturing automation,” Proc. IEEE, vol. 104, no. 5, pp. 1102–1113, May 2016.
[5] Y. Huang, M. Zhu, Z. Zheng, and K. H. Low, “Linear velocity-free visual servoing control for unmanned helicopter landing on a ship with visibility constraint,” IEEE Trans. Syst., Man, Cybern., Syst., vol. 52, no. 5, pp. 2979–2993, May 2022; doi: 10.1109/TSMC.2021.3062712.
[6] H. P. Wang, Y. Tian, and N. Christov, “Event-triggered observer based control of networked visual servoing control systems,” J. Control Eng. Appl. Infor., vol. 16, no. 1, pp. 22–30, 2014.
[7] D. Du, R. Chen, M. Fei, and K. Li, “A novel networked online recursive identification method for multivariable systems with incomplete measurement information,” IEEE Trans. Signal Inf. Process. Over Netw., vol. 3, no. 4, pp. 744–759, Dec. 2017.
[8] Y. Li and J. Zhou, “Fast and effective image copy-move forgery detection via hierarchical feature point matching,” IEEE Trans. Inf. Forensics Security, vol. 14, no. 5, pp. 1307–1322, May 2019.
[9] N. Sakr, N. D. Georganas, and J. Zhao, “Human perception-based data reduction for haptic communication in six-DoF telepersistence systems,” IEEE Trans. Instrum. Meas., vol. 60, no. 11, pp. 3534–3546, Nov. 2011.
[10] B. Liu, Q. Zhang, and J. Li, “Integrated sliding mode control and neural networks based packet disordering prediction for nonlinear networked control systems,” IEEE Trans. Neural Netw. Learn. Syst., vol. 30, no. 8, pp. 2324–2335, Aug. 2019.
[11] X. Jiang, G. Xia, Z. Feng, and Z. Jiang, “Consensus tracking of data-sampled nonlinear multi-agent systems with packet loss and communication delay,” IEEE Trans. Netw. Sci. Eng., vol. 8, no. 1, pp. 126–137, Jan. 2021.
A. T. S. Ho, X. Zhu, J. Shen, and P. Marziliano, “Fragile watermarking for localization and restoration of color images,” *IEEE Access*, vol. 8, pp. 200157–200169, 2020.

S. Bhalerao, I. A. Ansari, and A. Kumar, “A secure image watermarking for tamper detection and localization,” *J. Ambient. Intell. Humanized Comput.*, vol. 12, no. 1, pp. 1057–1068, Jan. 2021.

M. Zhang and C. Desrosiers, “High-quality image restoration using low-rank patch regularization and global structure sparsity,” *IEEE Trans. Image Process.*, vol. 28, no. 2, pp. 868–879, Feb. 2019.

T. Liu and X. Yuan, “Adaptive feature calculation and diagonal mapping for successive recovery of tampered regions,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 31, no. 7, pp. 2617–2630, Jul. 2021.

Z. Jin, M. Z. Iqbal, D. Bobkov, W. Zou, X. Li, and E. Steinbach, “A flexible deep CNN framework for image restoration,” *IEEE Trans. Multimedia*, vol. 22, no. 4, pp. 1055–1068, Apr. 2020.

D. Du et al., “Real-time H∞ control of networked inverted pendulum visual servo systems,” *IEEE Trans. Cybern.*, vol. 50, no. 12, pp. 5113–5126, Dec. 2020.

S. Kleinfelder, S. H. W. Chiang, W. Huang, A. Shah, and K. Kwaikowski, “High-speed, high dynamic-range optical sensors arrays,” *IEEE Trans. Nano. Sci.*, vol. 56, no. 3, pp. 1069–1075, Jun. 2009.

D. Du, C. Zhang, X. Li, M. Fei, T. Yang, and H. Zhou, “Secure control of networked control systems using dynamic watermarking,” *IEEE Trans. Cybern.*, early access, Sep. 20, 2021, doi: 10.1109/TCYB.2021.3110402.

C. Qu et al., “Retransmission methods to improve voltage control of distributed generation system,” *IEEE Commun. Lett.*, vol. 25, no. 6, pp. 1862–1866, Jun. 2021.

X. Meng, H. Yu, J. Zhang, and K. Yan, “Optimized control strategy based on EPCH and DBMP algorithms for quadruple-tank liquid level system,” *J. Process Control*, vol. 110, pp. 121–132, Feb. 2022.

T. Wang, H. Gao, and J. Qiu, “A combined adaptive neural network and nonlinear model predictive control for multirate networked industrial process control,” *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 2, pp. 416–425, Feb. 2016.

A.-A. Ahmadi, F. R. Salmasi, M. Noori-Manzar, and T. A. Najafabadi, “Speed sensorless and sensor-fault tolerant optimal PI regulator for networked DC motor system with unknown time-delay and packet dropout,” *IEEE Trans. Ind. Electron.*, vol. 61, no. 2, pp. 708–717, Feb. 2014.

M. Oikawa, T. Kusakabe, K. Kutsuzawa, S. Sakaino, and T. Tsuji, “Reinforcement learning for robotic assembly using non-diagonal stiffness matrix,” *IEEE Robot. Autom. Lett.*, vol. 6, no. 2, pp. 2737–2744, Apr. 2021.

S. Mellini, V. Rajput, I. A. Ansari, and C. W. Ahn, “A fast and efficient image watermarking scheme based on deep neural network,” *Pattern Recognit. Lett.*, vol. 151, pp. 222–228, Nov. 2021.

R. Li, Q. Liu, and L. Liu, “Novel image encryption algorithm based on improved logistic map,” *IET Image Process.*, vol. 13, no. 1, pp. 125–139, 2019.

K. Li, T.-Z. Huang, L. Li, and S. Lanteri, “Non-intrusive reduced-order modeling of parameterized electromagnetic scattering problems using cubic spline interpolation,” *J. Sci. Comput.*, vol. 87, no. 2, p. 52, May 2021.

Q. Su, S. Li, Y. Gao, X. Huang, and J. Li, “Observer-based detection and reconstruction of dynamic load altering attack in smart grid,” *J. Franklin Inst.*, vol. 358, no. 7, pp. 4013–4027, May 2021.

A. Kusiak, Z. Zhang, and A. Verma, “Prediction, operations, and condition monitoring in wind energy,” *Energy*, vol. 60, pp. 1–12, Oct. 2013.

M. Zhao, S. Zhong, X. Fu, B. Tang, and M. Pecht, “Deep residual shrinkage networks for fault diagnosis,” *IEEE Trans. Ind. Informat.*, vol. 16, no. 7, pp. 4681–4690, Jul. 2020. 

Dajun Du (Member, IEEE) received the B.Sc. degree in electrical technology and the M.Sc. degree in control theory and control engineering from Zhengzhou University, Zhengzhou, China, in 2002 and 2005, respectively, and the Ph.D. degree in control theory and control engineering from Shanghai University, Shanghai, China, in 2010. From September 2008 to September 2009, he was a Visiting Ph.D. Student with Queen’s University Belfast, U.K., where he was a Research Fellow from April 2011 to August 2012. He is currently a Professor with Shanghai University. His main research interests include system modeling and identification and networked control systems.
Lang Wu received the B.Sc. degree from Shanghai University, Shanghai, China, in 2019, where he is currently pursuing the M.Sc. degree.

His main research interests include secure control for networked control systems.

Changda Zhang received the B.Sc. and M.Sc. degrees from Shanghai University, Shanghai, China, in 2016 and 2019, respectively, where he is currently pursuing the Ph.D. degree.

His main research interests include secure control for networked control systems.

Zixiang Fei (Member, IEEE) received the bachelor’s degree from Liverpool John Moores University, Liverpool, U.K., in 2012, the master’s degree from the University of York, York, U.K., in 2014, and the Ph.D. degree from the University of Strathclyde, Glasgow, U.K., in 2020.

He is currently a Lecturer with Shanghai University, Shanghai, China. His major research interests include computer vision, machine learning, object recognition, and deep learning.

Lisi Yang received the B.Sc. and M.Sc. degrees from Shanghai University, Shanghai, China, in 2018 and 2021, respectively.

Her main research interests include secure control for networked visual control systems.

Minrui Fei received the B.S. and M.S. degrees in industrial automation from the Shanghai University of Technology, Shanghai, China, in 1984 and 1992, respectively, and the Ph.D. degree in control theory and control engineering from Shanghai University, Shanghai, in 1997.

Since 1998, he has been a Full Professor with Shanghai University. His research interests are in the areas of networked control systems, intelligent control, complex system modeling, hybrid network systems, and field control systems.

Dr. Fei is the Chairperson of the Embedded Instrument and System Sub-Society, the Standing Director of the China Instrument and Control Society, the Chairman of the Life System Modeling and Simulation Sub-Society, the Vice-Chairman of the Intelligent Control and Intelligent Management Sub-Society, and the Director of the Chinese Artificial Intelligence Association.

Huiyu Zhou received the B.Eng. degree in radio technology from the Huazhong University of Science and Technology, Wuhan, China, in 1990, the M.Sc. degree in biomedical engineering from the University of Dundee, Dundee, U.K., in 2002, and the Doctorate of Philosophy degree in computer vision from Heriot-Watt University, Edinburgh, U.K., in 2006.

He is currently a Full Professor with the School of Computing and Mathematical Sciences, University of Leicester, Leicester, U.K. He has authored or coauthored over 350 peer-reviewed articles in the field. His research work has been or is being supported by U.K. EPSRC, MRC, AHRC, ESRC, EU ICT, Royal Society, Innovate U.K., Leverhulme Trust, Invest NI, Puffin Trust, Alzheimer Research (U.K.), and industry.